

Symantec™ Advanced Threat Protection 2.0.2

Security Operations Guide



Documentation version: 2.0.2

Legal Notice

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
------------------------	--

Europe, Middle-East, and Africa	semea@symantec.com
---------------------------------	--

North America and Latin America	supportsolutions@symantec.com
---------------------------------	--

Contents

Technical Support	4
Chapter 1	About cybersecurity and threat protection 9
	About Symantec Advanced Threat Protection (ATP) 9
	How ATP fits into your cybersecurity framework 11
Chapter 2	Detecting threats in your environment 14
	About events, incidents, and entities 14
	How you can identify threats in your environment 15
	Delving through ATP Manager to investigate threats 17
	About searching for indicators of compromise (IOC) 18
	Searching the ATP database for IOCs 20
	Searching Symantec Endpoint Protection endpoints for IOCs 22
	Writing successful search expressions 23
	Viewing the events that occur in your environment 31
	The types of events that ATP detects 33
	How to analyze incidents 34
	How ATP creates and prioritizes incidents 36
	About analyzing the process behaviors that occurred on endpoints 38
	Analyzing the Dashboard 39
	About the Event Activity widget 40
	About the Network Event Activity widget 41
	About the Endpoint Event Activity widget 43
	About the Email Event Activity widget 45
	About the New and Unknown Threats widget 46
	About the Endpoints widget 46
Chapter 3	Acting on threats 48
	Isolating breached endpoints 48
	Remediating malicious files 49
	Reporting false positive and false negative file convictions 53
	Manually submitting files to Cynic for analysis 53

	Blacklisting suspicious domains, URLs, and IP addresses	54
	About policies	56
	Creating a Blacklist policy	56
	Creating a Whitelist policy	58
	Supported policy match values for IP addresses, domains, and URLs	60
	Managing policies	61
	Checking the status of an action	62
Chapter 4	Recovering after threats have been contained	65
	Recovery best practices	65
	About Reports	66
	Running and scheduling reports	69
	Viewing and deleting reports and report schedules	72
	How to use the Executive Report	75
Appendix A	About incident-related pages in the ATP Manager	77
	About the Incident Manager	77
	About Incident details	79
	About Endpoint details	84
	About File details	88
	About Process Behavior details	94
	About Domain details	97
	About Events	100
Index		102
Glossary		105

About cybersecurity and threat protection

This chapter includes the following topics:

- [About Symantec Advanced Threat Protection \(ATP\)](#)
- [How ATP fits into your cybersecurity framework](#)

About Symantec Advanced Threat Protection (ATP)

Symantec Advanced Threat Protection (ATP) performs the critical security tasks that detect, protect, and respond to threats to your network. ATP Platform is comprised of the following control points:

network	Processes the network stream passing it through various filters and detection engines. ATP can detect events on unmonitored endpoints as traffic passes through the scanner. Since ATP does not have Symantec Endpoint Protection agent's information, ATP is unable to provide all of the information about the endpoint, such as the user name, last check-in, or Symantec Endpoint Protection Manager group.
endpoint	Gathers information by proxying communications between Symantec Endpoint Protection clients and Symantec and by leveraging Symantec Endpoint Protection's Endpoint Detection and Response (EDR) functionality.
email	Integrates with Symantec Email Security.cloud to uncover the attacks that enter your organization through email.

ATP employs the following detection technologies:

Vantage	Vantage is a signature-based detection engine that finds threats in the network stream.
Insight	Insight accesses the world's largest reputation database and has reputation intelligence on over 8 billion files. Insight is a Symantec-owned reputation request service for Insight reputation queries. This service gathers information about the Windows executable files that are observed on endpoints.
Mobile Insight	Mobile Insight performs similar analyses for Android applications as Insight does for Windows executable files. In addition to tackling malware detection, Mobile Insight also detects privacy and performance issues in mobile apps.
Antivirus engine	The antivirus engine is a signature-based technology that detects malware.
Cynic	Cynic™ analysis and virtual execution detonates files in a cloud-based sandbox environment, analyzes, and reports each step of the observed behavior. Cynic uses machine-learning technology to compare the results to known bad attributes. It then correlates your data with real-world data provided by the Symantec Global Intelligence Network to determine if the files are malicious.
Blacklists and Whitelists	Symantec global blacklist and whitelist feeds, which are updated on ATP appliances regularly, accelerate detection and optimize performance. You can also create custom Blacklists and Whitelist that you maintain through ATP.
Synapse	<p>Synapse™ is a service that correlates ATP network event data with Symantec™ Email Security.cloud (Email Security.cloud) email event data and Symantec Endpoint Protection endpoint event data, integrating detection and protection across your network, email system, and endpoints.</p> <p>The Synapse correlation engine automatically matches events with Symantec Endpoint Protection, Email Security.cloud, and ATP to reduce the volume of security alerts. As incidents are detected, they are correlated with other incidents discovered on your network to show overall attack patterns and prioritize the most significant threats.</p>

SONAR

Symantec Endpoint Protection includes Symantec Online Network for Advanced Response (SONAR) technology for process behavior detection and remediation. However, Symantec Endpoint Protection provides no insight into these details. When you integrate ATP and Symantec Endpoint Protection, ATP can provide insight into SONAR detections, including the system changes that have occurred on your managed endpoints, the order that they occurred, and related file attributes. This information gives you greater visibility into the activity that occurs in your environment.

SONAR uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on Symantec Endpoint Protection endpoints to detect emerging threats. SONAR also detects changes or behavior on the endpoints that you should monitor. SONAR does not make detections on application type, but on how a process behaves.

See [“How ATP creates and prioritizes incidents”](#) on page 36.

How ATP fits into your cybersecurity framework

In February 2014, the Commerce Department's National Institute of Standards and Technology (NIST) created the *Framework for Improving Critical Infrastructure Cybersecurity 1.0* (the "Framework"). The Framework was designed to help organizations plan for and address cybersecurity threats. Whether or not you follow the Framework guidelines, [Table 1-1](#) describes how Symantec Advanced Threat Protection (ATP) can help your organization address some of the core functions that are involved in cybersecurity preparedness, detection, and response.

Table 1-1 Cybersecurity core functions

Function	Description
Identify	<p>Perform an internal assessment of your organization to identify your potential risks and security goals. Develop a risk management strategy based on your business needs.</p> <p>See Symantec's Disaster Recovery Planning Guide for more information.</p>

Table 1-1 Cybersecurity core functions (*continued*)

Function	Description
Protect	<p>ATP's network control point analyzes incoming data streams while they travel through the network before they reach your endpoints. ATP uses this information to create events and generate incidents to help you find potential threats in your environment. When you configure ATP to use the inline block operation mode, ATP blocks access to the files and external computers that it detects are malicious or are in your ATP Blacklist. You can further control what is blocked (or not blocked) through Blacklist and Whitelist policies.</p> <p>Note: ATP may be unable to block 100% of malicious detections, such FTP file downloads.</p> <p>See “The types of events that ATP detects” on page 33.</p> <p>See “About policies” on page 56.</p> <p>When you integrate ATP with Symantec Endpoint Protection, you not only have the protection that Symantec Endpoint Protection provides for your endpoint, but you can also perform remediation tasks through the ATP Manager (such as deleting infected files).</p> <p>See “About Symantec Advanced Threat Protection (ATP)” on page 9.</p>
Detect	<p>When you integrate the ATP network control point with Symantec Endpoint Protection and Email Security.cloud, the Synapse cloud service can correlate events from each product to give you a comprehensive picture of threats to your network, endpoints, and email system.</p> <p>ATP shows the threats that it detects on the Dashboard and the Incident Manager. And you can monitor all of the events that occur on your network for suspicious or malicious activity on the Events page.</p> <p>ATP helps you proactively search for indicators of compromise (IOC) using the Search.</p> <p>ATP can automatically send you notifications when incidents are created. It can also log events to syslog so that you can import them into your security information and event management (SIEM) system.</p> <p>See “How you can identify threats in your environment” on page 15.</p> <p>See “How ATP creates and prioritizes incidents” on page 36.</p>

Table 1-1 Cybersecurity core functions (*continued*)

Function	Description
Respond	<p>ATP provides one-click containment and remediation capability that works across endpoints, network, and email control points. For example, you can delete a malicious file from an endpoint or isolate a breached endpoint.</p> <p>See “Isolating breached endpoints” on page 48.</p> <p>See “Remediating malicious files” on page 49.</p> <p>See “Blacklisting suspicious domains, URLs, and IP addresses” on page 54.</p>
Recover	<p>After a threat has been contained, follow these best practices to analyze how the breach occurred and to prevent similar breaches in the future.</p> <p>See “Recovery best practices” on page 65.</p> <p>You can also run an Executive report, which is useful for analyzing the number and types of attacks that occurred in your environment.</p> <p>See “About Reports” on page 66.</p>

Additional resources

[NIST organization web site](#)

[Cybersecurity Framework 1.0](#)

[United State Computer Emergency Readiness Team \(US-CERT\)](#)

[Demystifying the NIST Cybersecurity Framework: What It Means for You by Symantec Corporation](#)

Detecting threats in your environment

This chapter includes the following topics:

- [About events, incidents, and entities](#)
- [How you can identify threats in your environment](#)
- [About searching for indicators of compromise \(IOC\)](#)
- [Viewing the events that occur in your environment](#)
- [How to analyze incidents](#)
- [About analyzing the process behaviors that occurred on endpoints](#)
- [Analyzing the Dashboard](#)

About events, incidents, and entities

An *event* is generated when ATP detects that an activity occurred, such as a malicious file is downloaded or a benign executable file is created. Not all events are malicious, such as a reputation request of a healthy file.

An *incident* is a collection of one or more events that represent a significant risk to the organization. Incidents include the events that Symantec Endpoint Protection has blocked, because even blocked events contribute to a more complete picture of the larger attack. What's more, not all malicious events are escalated to incidents.

For example, assume a user visits a spoofed website with a bad reputation. If there is no indication that the user's endpoint became infected or downloaded anything malicious, the event is not likely raised to an incident because it's not important

enough to bring to an incident responder's attention. However, the event is still logged on the Events page.

Examples of an event are as follows:

- An email with a file attachment that is deemed suspicious.
- An endpoint contacts a non-malicious IP address.
- Symantec Endpoint Protection detects a suspicious file.
- A malicious file is created.

Examples of an incident are as follows:

- A computer communicates with a command and control server.
- A malicious file is downloaded repeatedly on the same or on different endpoints.
- A network attack is repeatedly attempted against one or more endpoints.
- A file is detected that Symantec knows has been used in targeted attacks.

An *entity* is the component that is involved in an event. ATP monitors events on the following entities:



Domain

A domain, URL, or IP address not in your internal network.



Endpoint

Computers, servers, or mobile devices in your network.



File

Any file that resides on an endpoint, is attached to an email, or is downloaded from a domain.

See [“How ATP fits into your cybersecurity framework”](#) on page 11.

See [“The types of events that ATP detects”](#) on page 33.

How you can identify threats in your environment

[Table 2-1](#) describes how you can use Symantec Advanced Threat Protection (ATP) to identify potential threats to your environment.

Table 2-1 How to use ATP to detect threats

Description	Solution
Integrate ATP with your control points.	<p>You must integrate ATP with your control points to monitor and respond to threats in your environment. ATP supported control points are: network, endpoint, and email.</p> <p>See the <i>Symantec™ Advanced Threat Protection Administration Guide</i> for more information.</p>
Monitor and search your environment for indicators of compromise (IOC).	<ul style="list-style-type: none"> ■ When you learn of a potential threat, you can search for IOCs on the ATP database or on your managed endpoints. See “About searching for indicators of compromise (IOC)” on page 18. ■ You can review the events that occurred in your organization for suspicious or malicious behavior and trends. See “Viewing the events that occur in your environment” on page 31. See “About Events” on page 100.

Table 2-1 How to use ATP to detect threats (*continued*)

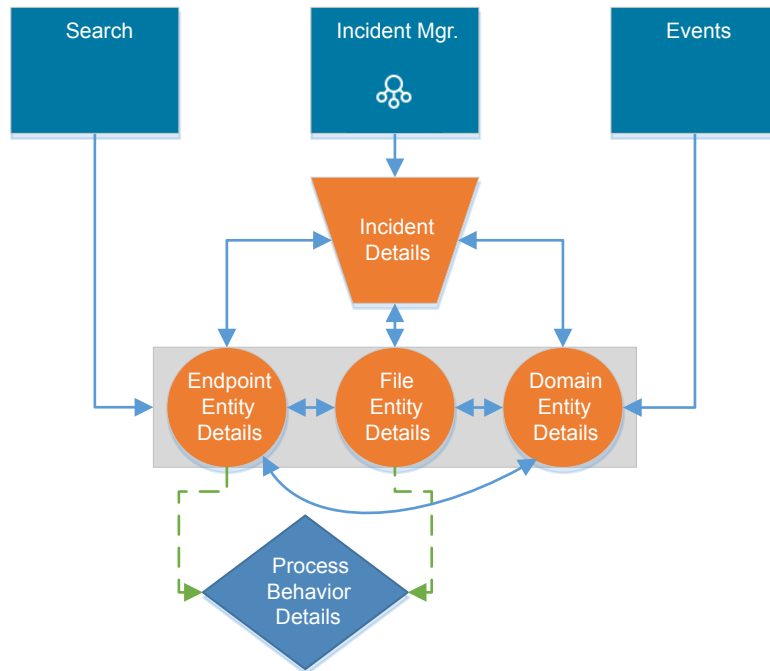
Description	Solution
Analyze the threats that ATP detects.	<p>ATP provides the following features to let you know that possible threats exist:</p> <ul style="list-style-type: none"> ■ Incident Manager ATP evaluates related events and aggregates them into incidents for your review and mitigation. Incidents are prioritized by severity and criticality so that you can quickly determine which ones need immediate attention. From this page, you can go to the Incident details page to view greater details about incidents and take actions to remediate them. You can also click on an entity node to go to that entity's details page to see more in-depth details about the entity and take actions. See "How to analyze incidents" on page 34. ■ Dashboard The dashboard provides a visual depiction of what's occurring in your environment. Click on any of the dashboard widgets for in-depth information. See "Analyzing the Dashboard" on page 39. ■ Email notifications ATP can notify you by email when an incident occurs. Email notifications contain a summary of the incident. ■ Syslog ATP can send incidents and notification messages to remote syslog servers using standard syslog forwarding. Logging to syslog lets you aggregate multiple management consoles and evaluate the data with your own sets of rules and data analysis, including aggregation from other systems into your security information and event management (SIEM) system.

Delving through ATP Manager to investigate threats

The following diagram shows how you can use hyperlinks within Symantec Advanced Threat Protection (ATP) Manager pages to more quickly and easily investigate threats and take actions.

Legend:

- ➔ The direction hyperlinks within those pages will take you
- Page is only available when there is a process behavior file/endpoint pairing
- Orange objects are pages on which you can take actions, such as isolating endpoint



About searching for indicators of compromise (IOC)

Symantec Advanced Threat Protection (ATP) lets you search its database and managed Symantec Endpoint Protection endpoints for artifacts that are *indicators of compromise (IOC)*s. For example, you may learn about malware activity through Cynic results or you may have become aware of a trending malicious threat through a news source. You can search for these artifacts in your environment and take the appropriate actions. There is no limit to the number of expressions that you can search for regardless of the type of search that you perform.

Table 2-2 describes the search types and provides information about what is supported for each.

See [“Searching Symantec Endpoint Protection endpoints for IOCs”](#) on page 22.

See [“Searching the ATP database for IOCs”](#) on page 20.

Table 2-2 Investigator search types

Details	Database Search	Endpoint Search
Description	<p>ATP collects information from the network, endpoint, and email sensors and aggregates them into a database. ATP also collects data from managed Symantec Endpoint Protection clients about events (such as convictions). You can search this database for artifacts.</p> <p>See “The types of events that ATP detects” on page 33.</p>	<p>ATP reaches out to managed endpoints and searches for artifacts. Endpoint searches provide visibility into conviction and non-conviction events.</p> <p>If you send a search request and a Symantec Endpoint Protection client is restarted before the search completes, that agent resumes the scan and returns results when the client comes back online.</p> <p>The minimum supported version of Symantec Endpoint Protection that you can use to perform endpoint searches is 12.1 RU5. The minimum Symantec Endpoint Protection Manager version is 12.1 RU6. If the client is using version 12.1 RU5, the following search features are not supported:</p> <ul style="list-style-type: none"> ■ File name searches ■ Use of wildcards in search expressions <p>Full Endpoint Detection and Response (EDR) functionality requires that the client endpoint runs Symantec Endpoint Protection version 12.1 RU6 MP3 or later.</p> <p>For more information about system requirements for ATP integration with Symantec Endpoint Protection Manager management interfaces and embedded databases, see the <i>Symantec Advanced Threat Protection Installation Guide</i>.</p>
Use case	<p>A database search lets you search on one or more fields and provides information about the artifacts that have been seen in your environment.</p> <p>Note: Registry key searches are not supported on database searches.</p>	<p>Endpoint searches reflect artifacts that currently are in your environment.</p> <p>Search for any supported field found in the ATP database plus the artifacts found on managed endpoints, such as registry searches.</p>

Table 2-2
 Investigator search types *(continued)*

Details	Database Search	Endpoint Search
Time to receive search results	ATP can quickly scan its database and return immediate results.	<p>The time to return search results depends on the Symantec Endpoint Protection Manager/Symantec Endpoint Protection configuration:</p> <ul style="list-style-type: none"> Pull mode When you make a search request, that request is immediately forwarded to Symantec Endpoint Protection Manager. However, the agent does not receive the request until the next heartbeat occurs when the Symantec Endpoint Protection client checks in with Symantec Endpoint Protection Manager and receives the request. The time to receive the request results depends on the heartbeat interval. Push mode When you make a search request, the time to receive the request results depends on the heartbeat interval. <p>Tip: The more specific you make your search, the quicker results are returned.</p>

See [“Writing successful search expressions”](#) on page 23.

Searching the ATP database for IOCs

Symantec Advanced Threat Protection (ATP) lets you search for events that have already occurred in your environment in the ATP database. You can specify the string that you want to search for in the search field. ATP parses individual strings to determine the field type (file name, hash, domain, etc.). However, if you want to perform more detailed searches, ATP supports expressions.

ATP also lets you perform database searches using a Structured Threat Information Expression (STIX) file. Currently, ATP only supports searches of the ATP database using a STIX file (endpoint searches using a STIX file are unsupported). And only file hashes (SHA256 or MD5) within the Indicators or Reports tags are searchable. No other objects in the STIX file are queried.

See [“About searching for indicators of compromise \(IOC\)”](#) on page 18.

Tip: Search does not support searches by event type (such as file reputation requests). To view events by event type, go to the **Events** page. See [“About Events”](#) on page 100.

Note: Database search results cannot be saved or exported. If you navigate away from the search page and return, your search results no longer appear.

Any user role can search the ATP database for IOCs.

To search for IOCs in the ATP database

- 1 On the ATP Manager navigation pane, click **Search**.

Database Search is the default setting.

- 2 In the **Search** field, do any of the following:

To search for a string	<div>◆ Type the string that you want to search for.</div> <div>ATP parses the individual strings to determine the field type (file name, hash, domain, etc.). By default, ATP performs string searches using the "like" (starts with) conditional operator.</div>
To search for an expression	<div>◆ Type the expression that you want to search for.</div> <div>ATP supports expressions in the following format:</div> <div><Token> <Operator> <'Value'></div> <div>Important: You must separate each item in the expression with a space and the value must be in single or double quotes.</div> <div>By default, ATP performs searches using the "like" (starts with) conditional operator if no other conditional operator is specified. Click the following link to learn more about supported tokens, wildcards, and operators and to see examples.</div> <div>See “Writing successful search expressions” on page 23.</div>
To search using a STIX file	<div><div><div>1 Click the upload icon.</div><div>2 Browse to and select the STIX file that you want to search with.</div></div><div>The STIX file must be in .xml file format, and the file size cannot exceed 10 MB. The query size that is formed from the file hashes extracted from the STIX file cannot exceed 500 KB.</div></div>

3 Click **Search**.

Results should begin to appear immediately.

4 Optionally, in the search results, click on an entity to go to that entity's details page to learn more and remediate as needed.

The **Search Criteria** field shows the hash(es) included in the search. If you uploaded a STIX file, hover over the field to view a list of all of the hashes that are included in the search. The **Search Overview** indicates the date and time (in UTC) that the search started. The **Results Overview** indicates whether ATP found results for the search and the related entities that were found in the search results.

Tip: Double-click on any hash, right-click, and select **Copy** to copy the full hash to your Clipboard. You can then paste this value where needed.

Searching Symantec Endpoint Protection endpoints for IOCs

Users with the Admin role or Controller role can search Symantec Endpoint Protection endpoints for IOCs.

See “[About searching for indicators of compromise \(IOC\)](#)” on page 18.

Tip: Search does not support searches by event type. If you want to search for specific events, go to the **Events** page. See “[About Events](#)” on page 100.

Tip: Symantec Advanced Threat Protection (ATP) does not stop or fully display the status of all the searches. You can view the status of the search and stop full scan searches in Symantec Endpoint Protection Manager on the **Monitors > Command Status** page. For more information, see the Symantec Endpoint Protection Manager documentation.

https://support.symantec.com/en_US/endpoint-protection.54619.html

To search Symantec Endpoint Protection endpoints for IOCs

- 1 On the ATP Manager navigation pane, click **Search**.
- 2 Move the slider beside **Search** to the right to enable the **Endpoint Search**.
Database Search is the default setting.

- 3 In the **Search** field, type the string that you want to search for.

ATP parses the strings to determine the field type (i.e., file name, hash, domain, etc.). However, if you want to perform more detailed searches, ATP supports expressions in the following format:

<Token> <Operator> <'Value'>

Important: You must separate each item in the expression with a space and the value must be in single or double quotes.

By default, ATP performs searches using the "like" (starts with) conditional operator if no other conditional operator is specified. Click the following link to learn more about supported tokens, wildcards, and operators and to see examples.

See ["Writing successful search expressions"](#) on page 23.

- 4 In the **Filter Search By** fields, type a host name or IP address. Separate multiple host names or IP addresses with commas.
- 5 In the **SEPM Group Field**, specify the Symantec Endpoint Protection Manager group.

When you specify Symantec Endpoint Protection Manager group, all endpoints in subgroups are also searched.

When you begin typing a Symantec Endpoint Protection Manager group name, ATP auto-discovers similarly named groups from you select from.

- 6 Click **Search**.

Search results appear under **Active Endpoint Search**. The **Active Endpoint Search** table shows that the status of the search that is reflected by a progress bar, the search criteria, and when the search began. When the search completes, the search results appear in the **Search History** table.

To delete search results

- ◆ Under **Search History**, select the search that you want to delete and click **Clear Selected**.

Click on the entity node in the search results to go to that entity's details page to get more information and to take action on that entity.

Tip: Double-click on any hash, right-click, and select **Copy** to copy the full hash to your Clipboard. You can then paste this value where needed.

Writing successful search expressions

Symantec Advanced Threat Protection (ATP) parses individual strings to determine the string type (i.e., file name, hash, domain, etc.). For example, typing `test123`

into the search field returns any file whose name starts with "test123". Pasting 462EE52A6C5ABC4C547492B8B569B78A into the search field returns any file that contains this string in its name or any file that contains this hash value.

However, if you want to perform more detailed searches or perform faster searches, ATP supports search expressions written in the following format:

<Token> <Operator> <"Value">

Important: You must separate each item in the expression with a space, and the value must be in single or double quotes.

Click on any of the following links to learn more about writing successful expressions.

[Important information about endpoint searches](#) | [Tokens](#) | [Wildcards](#) | [Operators](#)

Important information about endpoint searches

ATP supports endpoint searches for Symantec Endpoint Protection clients that use Symantec Endpoint Protection 12.1 RU5 and later. ATP manages clients that use Symantec Endpoint Protection version 12.1 RU 6 MP3 or later with full EDR functionality. However, for the clients that use a version between Symantec Endpoint Protection 12.1 RU5 and 12.1 RU6 MP 3, some functionality may be limited depending upon the version of the client. These limitations are denoted where applicable in the tables below.

Because of the limited functionality of earlier versions of Symantec Endpoint Protection, performing searches in a mixed environment may not produce the desired results. Symantec recommends that as a best practice, you perform database searches first. Since ATP collects its information from the control point sensors, you're very likely to find the results that you're looking for. More importantly, database searches produce results very quickly. If you want to perform endpoint searches, Symantec recommends that you create Symantec Endpoint Protection client groups based on the Symantec Endpoint Protection version that those clients run. When you perform an endpoint search on that Symantec Endpoint Protection group, you can better understand what results you can expect.

Tokens

Table 2-3 Tokens

Token	Description and example	Database search support and supported operators ¹	Endpoint search support and supported operators ^{1, 2}
filename	<p>Searches for files by their name.</p> <p>Supported formats:</p> <ul style="list-style-type: none"> ■ Environmental variables ■ CSIDL paths ■ Supports user-specific file path <p>When searching for a file by its file name, if you don't type the file extension, ATP performs a partial search. For example, if you search <code>filename "a"</code>, ATP returns any file name that starts with an "a". However, if you search for file name using the <code>" ="</code> express, you must specify a file extension.</p> <p>EXAMPLE:</p> <pre>filename = "eicar.txt"</pre> <p>returns files that have the exact file name "eicar.txt".</p>	<p>Yes</p> <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	<p>Yes for Symantec Endpoint Protection 12.1 RU6 MP3 and higher</p> <ul style="list-style-type: none"> ■ The only conditional operators supported are <code>=</code>, <code>like</code>, and <code>match</code>. ■ The only logical operator supported is <code>OR</code>. <p>Important: Performing a file name search without specifying a directory location requires a search of the entire hard drive for all of the endpoints that you specify in your search criteria. This type of search is resource-intensive for client computers. As a best practice, limit the number of endpoints that you issue the search on.</p>
filehash	<p>Searches for executable files by their SHA256 or MD5 hashes.</p> <p>This search token does not currently support searches for non-PE file types, such as <code>.pdfs</code>.</p> <p>EXAMPLE:</p> <pre>filehash = "462EE52A6C5ABC4C547492B8B569B78"</pre> <p>returns files that have the exact hash value in the expression.</p>	<p>Yes</p> <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	<p>Yes</p> <ul style="list-style-type: none"> ■ The only conditional operator supported is <code>=</code>. ■ The only logical operator supported is <code>OR</code>.

Table 2-3 Tokens (*continued*)

Token	Description and example	Database search support and supported operators ¹	Endpoint search support and supported operators ^{1, 2}
filepath	Searches for a file based on the file path. EXAMPLE: <code>filepath = "c:/user/file.txt"</code> returns any file found in this directory by the name file.txt.	No	Yes <ul style="list-style-type: none"> ■ No conditional operators are supported. ■ No logical operators supported.
domainname	Searches for domains by domain name. EXAMPLE: <code>domainname like "testserver"</code> returns any domains whose names start with "testserver".	Yes <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	No
domainurl	Searches for domains by their URL. EXAMPLE: <code>domainurl match "SEP"</code> returns any domains that have "SEP" anywhere in their names.	Yes <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	No
domainip	Searches for a domain by its IP address. EXAMPLE: <code>domainip like "155.55"</code> returns any domain that whose address starts with "155.55".	Yes <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	No
hostname	Searches for endpoints by their host name. <code>hostname like "east coast"</code> returns any endpoint whose host name starts with "east coast".	Yes <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	No

Table 2-3 Tokens (*continued*)

Token	Description and example	Database search support and supported operators ¹	Endpoint search support and supported operators ^{1, 2}
hostip	Searches for endpoints by their IP address. EXAMPLE: <code>hostip match "155.55"</code> returns any endpoint whose IP address contains "155.55" in it.	Yes <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	No
username	Searches for endpoint users by their user name. EXAMPLE: <code>username = "John Doe"</code> returns all users with the user name "John Doe".	Yes <ul style="list-style-type: none"> ■ All conditional operators supported. ■ All logical operators supported. 	No
registry	Searches for the registry value. When you search for a registry key-value name, ATP returns any values it finds. However, ATP cannot search within the results of the value. If you search for the key only, ATP cannot return value names. Search expression should end with registry value name -- not the key. Alternatively, you can end the search with <code>"*"</code> . EXAMPLE: <code>registry = "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*"</code> returns all the values under this registry key.	No	Yes <ul style="list-style-type: none"> ■ The only conditional operator supported is <code>=</code>. ■ No logical operators are supported.

¹ See [Operators](#) for a description of the supported conditional and logical operators.

² When you perform a filename search, if the file name length (excluding the extension) is equal to or greater than 3 characters and it's partially matched with files under C:\Windows\SysWOW64 (for 64-bit) and C:\Windows\system32, ATP is unable to find match results. For example, assume that there is a file named

setup16.exe in the C:\Windows\SysWOW64 directory. When you search filename = "set.exe", ATP returns no results. However, if you search filename = "setup167.exe", ATP is able to return results. In this example, when you search for "set.exe", ATP actually searches for "set*.exe". Anything matching set*.exe in C:\Windows\System32 (32-bit OS) or C:\Windows\SysWOW64 (64-bit OS) will truncate the search and return no results. Symantec recommends in this scenario that you perform a filepath search instead of a filename search.

Wildcards

Table 2-4 Supported wildcards

Wildcard	Description	Example	Available on Database search	Available on Endpoint search ³
*	Any number of undefined characters.	registry = "HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows \CurrentVersion\Run*" returns all the values under this registry key.	No	Yes Supported for the filepath, filename, and registry tokens for Symantec Endpoint Protection 12.1 RU6 MP3 and higher, with partial results for 12.1 RU6 MP3 and full results for 12.1 RU6 MP4 and higher.
?	A single, undefined character.	filename match "?icar" returns any file that contains xicar". For example, aicar, bicar, dicar, etc.	No	Yes Supported for the filepath, filename, and registry tokens for Symantec Endpoint Protection 12.1 RU6 MP3 and higher only, with partial results for 12.1 RU6 MP3 and full results for 12.1 RU6 MP4 and higher.

Table 2-5 ³Supported endpoint search wildcards and substitutions by Symantec Endpoint Protection version

Field	Example	Symantec Endpoint Protection 12.1 RU6 MP2	Symantec Endpoint Protection 12.1 RU6 MP3 and higher
filepath	C:\Windows*\foo.exe	No	Yes
filename	C:\Windows\temp\foo*	No	Yes
CSIDL paths	CSIDL_APPDATA\antivirus\downloader	No	Yes
Environmental variable path	%APPDATA%\antivirus\downloader	Yes	Yes
Registry key	HKLM\Software\Symantec*\InstalledApps	No	Yes
Registry value	Key = HKLM\Software\Symantec Value = * Path	No	Yes
Registry data value search	N/A	No Value is returned in the search results	Yes

Operators

By default, ATP performs searches using the "like" (starts with) conditional operator if no other conditional operator is specified. ATP supports the following conditional operators ([Table 2-6](#)) and logical operators ([Table 2-7](#)) in search expressions.

Table 2-6 Conditional operators

Conditional operator	Description	Example	Database search support and supported tokens ⁴	Endpoint search support and supported tokens ⁴
=	Returns only the entities that contain exact matches of the value.	filehash = "462EE52A6C5ABC4C547492B8B569B78" returns files that have the exact hash value in the expression.	Yes Supported for all tokens.	Yes Supported for the filename, filehash, and registry tokens only.

Table 2-6 Conditional operators (*continued*)

Conditional operator	Description	Example	Database search support and supported tokens ⁴	Endpoint search support and supported tokens ⁴
match	Returns only the entities that have the value anywhere in the field.	<code>hostip match "155.55"</code> returns any endpoint whose IP address contains "155.55" anywhere in it.	Yes Supported for all tokens.	Yes Supported for the filename token only.
like	Returns only the entities that start with the value.	<code>domainname like "testserver"</code> returns any domains whose names start with "testserver".	Yes Supported for all tokens.	Yes Supported for the filename token only.
!=	Omits from the results any entity that exactly matches the value.	<code>filename like "eicar"</code> and <code>filename != "eicar.txt"</code> returns any file that has the name eicar in it except files named eicar.txt.	Yes Supported for all tokens.	No
not_match	Omits from the results any entity that has the value anywhere in the field.	<code>hostname match "ABJ"</code> AND <code>not_match "ABJK"</code> returns any endpoints that contains "ABJ" anywhere in their name but do not contain "ABJK" anywhere in their name.	Yes Supported for all tokens.	No
not_like	Omits from the search results any entities that start with the value.	<code>username like "Joh"</code> AND <code>not_like "Johnny"</code> returns all users whose names start with "Joh" but are not "Johnny".	Yes Supported for all tokens.	No

Table 2-7 Logical operators

Logical operator	Description	Example	Database search support and supported tokens ⁴	Endpoint search support and supported tokens ⁴
AND	Returns only those entities that match all of the values in the expression.	filename = "aaa" AND filehash = "462EE52A6C5ABC4C547492B8B569B78A" returns any file that has the name "aaa" and also has the hash that is indicated in the value.	Yes	No
OR	Returns artifacts that contain any of the values comprising the OR statement.	filename match "aaa" OR filename match "bbb" returns any file that has "aaa" in its name or any file that has "bbb" in its name.	Yes	Yes Supported for the filename and filehash tokens only.

⁴ See [Table 2-3](#) for the supported tokens.

See [“About searching for indicators of compromise \(IOC\)”](#) on page 18.

See [“Searching the ATP database for IOCs”](#) on page 20.

See [“Searching Symantec Endpoint Protection endpoints for IOCs”](#) on page 22.

Viewing the events that occur in your environment

You can view all of the events that have occurred in your environment chronologically. Or you can narrow your search by filtering and searching by event type and date range.

For example, filtering events by Blacklists provides insight into which endpoints attempted to access blacklisted sites. Repeated attempts from the same internal computer may be an indication that the endpoint is infected with malware and is attempting phone-home attempts.

See [“The types of events that ATP detects”](#) on page 33.

To view the events that occur in your environment

- 1 On the ATP Manager navigation pane, click **Events**.

By default, events are listed chronologically with the most recent event first.

- 2 To narrow the event list, click **Show Filters**. Do any of the following:

To filter by event type By default, all of the filter options are selected. Uncheck the options that you do not want to include in your filter criteria. Or click **Clear all** to uncheck all of the filter boxes, and select the options that you want to include in your filter criteria. Click **Hide Filters** to hide the filters view. ATP maintains your filter selections until you reset the filter criteria or refresh the page.

See [“The types of events that ATP detects”](#) on page 33.

To search for a specific event Type the event that you want to search on in the **Search** field.
 You can narrow filtered results to view just the following:

- IP address
- Domain name
- Host name
- File name
- File hash

Note: ATP lets you combine filtering and search to further narrow search results.

To narrow the search time range Specify a starting and ending date and time range.

To return to the default filter criteria Click **Reset all filters** to reset your filter criteria to the default setting (all boxes selected).

- 3 Optionally, click on any hyperlink (in blue) in the list of events to go to that entity's details page.

See [“How ATP creates and prioritizes incidents”](#) on page 36.

See [“About Events”](#) on page 100.

See [“About events, incidents, and entities”](#) on page 14.

See [“Reporting false positive and false negative file convictions”](#) on page 53.

The types of events that ATP detects

Analyzing the events that occur in your environment provides an overall view of your organization's security. Symantec Advanced Threat Protection (ATP) logs every event that it detects (whether the event appears malicious or not) in the ATP Manager on the **Events** page. Click the link below to learn more about the technologies that detect events.

See [“About Symantec Advanced Threat Protection \(ATP\)”](#) on page 9.

[Table 2-8](#) describes the types of events that ATP detects.

Table 2-8 ATP event types

Event type	Description
Cynic file execution and analysis	Cynic observed a malicious file in your network.
Insight file detections	<p>Symantec Endpoint Protection has queried the file reputation server about a file on a managed endpoint or Insight detected malicious activity occurring in your network.</p> <p>Symantec Endpoint Protection clients can generate a large number of Insight events because Insight queries can be made on all types of files — good, bad, and unknown. The ability to filter Insight detections by type (for example, only bad files) is currently unsupported.</p>
Mobile Insight app analysis	Mobile Insight detected issues with an Android executable.
Blacklists	<p>A file has been detected that is in a Symantec-provided Blacklist or a file has been detected that is in the ATP Blacklist.</p> <p>See “Creating a Blacklist policy” on page 56.</p>
Vantage network intrusion prevention (IPS/NDC)	Vantage detected malicious activity on an endpoint or Vantage signature-based threats were found in the network stream.
Antivirus convictions	The antivirus engine convicted an infected file on an endpoint, and Symantec Endpoint Protection Manager submitted data about the conviction to Symantec for telemetry.

Note: ATP does not currently track file Process Behavior/SONAR submissions.

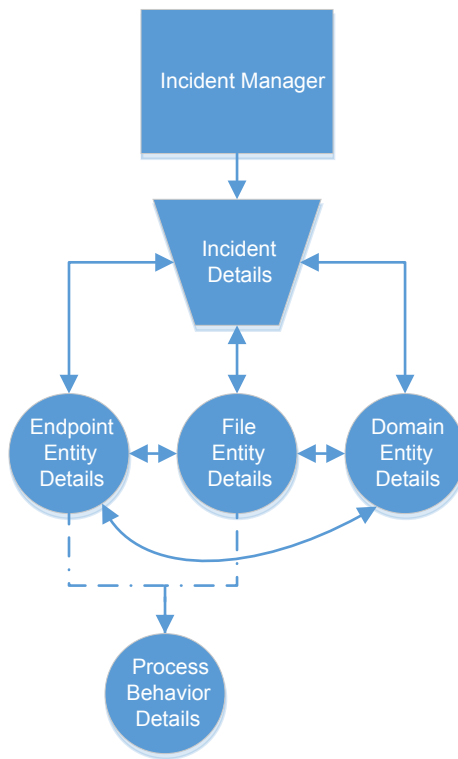
See [“About Process Behavior details”](#) on page 94.

See [“About Events”](#) on page 100.

See [“Viewing the events that occur in your environment”](#) on page 31.

How to analyze incidents

The following workflow explains how to analyze incidents at a high level and then drill-down to get greater details about the entities involved in the incident. As you drill down, Symantec Advanced Threat Protection (ATP) helps you determine how wide-spread the breach is and see what entities are affected. Hyperlinks make exploring related entities quick and easy. And you can perform remediation tasks as you progress in your investigation.



· — ➔ Page is only available when there is a process behavior file/endpoint pairing

Incident Manager Start your analysis in the Incident Manager.

The Incident Manager groups related events making it easier to spot overall patterns such as "Are we being attacked by this external entity over and over again?" "Are certain endpoints repeatedly being attacked?" "Are there multiple convictions because the same malicious file has been repeatedly downloaded, possibly by a Trojan horse or a downloader that infected multiple endpoints?"

Click on any incident in the list to go to that incident's details page for more information.

See ["About the Incident Manager"](#) on page 77.

Incident details Incident details page provides information about the events that comprise the incident and the relationship of the entities that are involved in the incident.

The First Seen date on the Incident details page is the date that the first event was detected in your environment. If the incident involves a possibly malicious file, check the Events table for the specific event that might indicate why the file was convicted.

Look for specific days and the times that convictions occur. If malicious activity is detected at very regular intervals, it is possible that malware is responsible for the downloads or server communications. In contrast, however, if malicious activities happen at irregular intervals during normal workdays, it is more likely that user behavior is the cause.

Right-click on any entity node in the Incident graph and select **Go to details**, or you can click on any hyperlink in the **Events** list to go to that entity's details page. You can also perform remediation tasks from this page.

See ["About Incident details"](#) on page 79.

Entity details The entity details page gives you the most comprehensive information about that entity and provides links to any related entities. You can click on any hyperlink on this page to go to related incidents or other entity details pages. And you can perform remediation tasks from this page.

When an endpoint contains a file that makes system changes to the endpoint that are deemed suspicious, a **Behavior** option appears on both the Endpoint details page (for the related file) and File details page (for the related endpoint). Click the **Behavior** option to go to the Process Behavior details.

See ["About File details"](#) on page 88.

See ["About Endpoint details"](#) on page 84.

See ["About Domain details"](#) on page 97.

Process Behavior details Process Behavior details page provides information about the system changes that were made by a file on an endpoint. These processes are listed in the ATP Manager in sequential order. ATP also provides the attributes that are associated with the system changes.

You cannot perform remediation tasks from this page, nor are there hyperlinks to related incident or entity details pages.

See [“About Process Behavior details”](#) on page 94.

How ATP creates and prioritizes incidents

Symantec Advanced Threat Protection (ATP) uses a rule engine to determine when it should create incidents based on the severity of related events. Incidents that consist of the events that Symantec knows are part of a targeted attack are prioritized higher than incidents without such events. Incidents with a high number of events are prioritized higher than incidents with fewer events. Incidents with events that occurred more recently are prioritized higher than older incidents.

[Table 2-9](#) lists the rules for how ATP generates incidents. Rules are listed in priority order.

Table 2-9 ATP incident rules

Incident description	ATP rule	Recommended actions
Malicious activity detected by {file name}.	ATP detected a file in your environment that is performing malicious acts, such as installing a key logger.	Isolate affected endpoints, delete the malicious file, and/or clean the system.
{Vantage signature name} detected.	Network or endpoint scanning has determined that a threat exists in your environment and is phoning home to a command and control server.	Ensure any related vulnerable software is patched. Blacklist the sites and delete the malicious files.

Table 2-9 ATP incident rules (*continued*)

Incident description	ATP rule	Recommended actions
{Virus signature name} detected.	ATP detected a Trojan that was not blocked by Symantec Endpoint Protection. Note: This rule only gets triggered when ATP does not get a block notification from Symantec Endpoint Protection. This can happen if Symantec Endpoint Protection isn't properly configured, has out of date definitions, or isn't installed.	Isolate breached endpoints, delete infected files, and/or clean the systems. Tip: Consider running Power Eraser on your endpoint.
Multiple attacks have been detected targeting {host name or IP address}.	More than five conviction events on an endpoint occurred within an hour.	Remove any software that keeps attempting malicious activity. Otherwise, consider communicating with users about their browsing choices.
Multiple attacks have been detected from {domain or IP address}.	More than five conviction events from an external computer occurred within an hour.	Review the SafeWeb evaluation for the site. Also, consider blacklisting the site at the firewall or adding the site to the DNS sinkhole if the site is not business critical.
Targeted attack detected.	ATP detected a file in your environment that is associated with a targeted attack.	Isolate affected endpoints, delete the malicious files, and/or clean the system.

ATP creates incidents and assigns them priorities based on the following criteria:

High	The incident could result in a business outage, loss of data, or have a severe impact on the business. The incident needs to be responded to immediately.
Medium	The incident may have an impact on the business, and the use of the computer in question might need to be limited while the incident is being addressed.

Low The incident does not affect critical business operation, and the computer can continue to function and provide normal service.

See [“About events, incidents, and entities”](#) on page 14.

About analyzing the process behaviors that occurred on endpoints

Symantec Endpoint Protection uses Symantec Online Network for Advanced Response (SONAR) technology for process behavior submission and remediation. However, Symantec Endpoint Protection provides no insight into the details of the SONAR submissions. When you integrate Symantec Advanced Threat Protection (ATP) 2.0.2 and later with Symantec Endpoint Protection, ATP can provide you with insight into the details of the SONAR submissions.

For more information about integrating ATP and Symantec Endpoint Protection, see the *Symantec Advanced Threat Protection (ATP) Administration Guide*.

ATP provides SONAR submission information based on an endpoint/file relationship (that is, a specific file makes system changes on a specific endpoint). This information is only available when there has been a Symantec Endpoint Protection SONAR submission. The information that appears in the ATP Manager is based on the information that ATP is able to extract from the Symantec Endpoint Protection submission information.

See the following topic to learn more about how process behavior analysis falls into your overall threat investigation workflow.

See [“Delving through ATP Manager to investigate threats”](#) on page 17.

ATP provides the following details based on SONAR submissions: [Process behaviors and dynamic file attributes](#) and [Static file attributes](#).

Process behaviors and dynamic file attributes

A process is created when a file is executed and is represented by a group of system changes. Behaviors refers to the system changes made by a process. For each event, ATP also provides the dynamic file attributes that are associated with the system change. These attributes are dynamic because the behaviors that are detected on one endpoint may differ from the behaviors that are detected on a different endpoint. Examples of process behaviors include: modifications to system policies; modifications to firewall policies; creating registry key paths.

Examples of dynamic file attributes include: SHA256; registry value data; process's parent.

Process behaviors and their dynamic file attributes appear on the Process Behavior details page. This page is only available when a file performs a process on a managed endpoint. You can navigate to this page in the following ways:

- From the Endpoint details page:
 A **Behavior** option appears in the **Malicious Files** row for the file that was involved in the process.
 See [“About File details”](#) on page 88.
- From the File details page:
 A **Behavior** option appears in the **Seen on Endpoints** row for the endpoint on which the process behavior occurred.
 See [“About Endpoint details”](#) on page 84.

See [“About Process Behavior details”](#) on page 94.

Static file attributes

These file attributes are considered static because they do not change regardless of the endpoint on which it appears. Examples of static file attributes include: the number of strings in a file's resource; the file imports only Kernel32 functions; the file has an embedded PE file.

Static file attributes appear on the File details page on the **Attributes** tab. The **Attributes** tab only appears when static file attributes are available.

See [“About File details”](#) on page 88.

See [“Remediating malicious files”](#) on page 49. See [“Remediating malicious files”](#).

Analyzing the Dashboard

The Dashboard provides a comprehensive visual representation of the threat activity in your network, endpoint, and email environment. The widgets on the Dashboard show the current patterns in threat detections. You can click through some of the charts on the widgets to find specific, filtered data for your area of interest, and then navigate to the Entity details page to perform actions against some of these threats.

The Dashboard contains the following widgets:

Event Activity

The **Event Activity** widget provides information about the malicious files that were detected in your network, endpoint, and email environments. This widget displays information from the Network, Endpoint, and Email widgets, which you can select individually to view additional information about each of those control points.

See [“About the Event Activity widget”](#) on page 40.

Network Event Activity	<p>The Network Event Activity widget provides information about the network traffic that flows through ATP when scanning is enabled on your appliance. This information appears in the form of an area chart that displays the total number of inspected IPv4 and IPv6 packets, as well as the conviction events created for traffic identified as malicious.</p> <p>See “About the Network Event Activity widget” on page 41.</p>
Endpoint Event Activity	<p>The Endpoint Event Activity widget provides information about both malicious and suspicious files that were detected on your endpoints. Malicious files are files that were blocked based on their detection as known threats. Suspicious files are files that were flagged based on their reputation score but were otherwise undetected as malicious. Suspicious files may be benign but may be worth investigating.</p> <p>See “About the Endpoint Event Activity widget” on page 43.</p>
Email Event Activity	<p>The Email Event Activity widget provides information about malicious files that were detected in email traffic from the endpoints in your environment. Malicious files are the files that were blocked based on their detection as known threats.</p> <p>See “About the Email Event Activity widget” on page 45.</p>
Endpoints	<p>The Endpoints widget lists the number of infected endpoints in your environment that executed a malicious file within the last 7 days. It also lists the total number of endpoints in your environment whether they are infected or not.</p> <p>See “About the Endpoints widget” on page 46.</p>
New and Unknown Threats	<p>The New and Unknown Threats widget lists the number of files that were detected as threats within your environment by the following Symantec technologies: Cynic, Insight, and Mobile Insight technologies.</p> <p>See “About the New and Unknown Threats widget” on page 46.</p>

About the Event Activity widget

The **Event Activity** widget provides information about the malicious files that were detected in your network, endpoint, and email environments. Malicious files are files that were flagged or blocked based on their detection as known threats.

When a file is detected as malicious, Symantec Endpoint Protection creates a conviction event that captures information about that event. The Event Activity widget provides information about these events based on their conviction type. As you filter through this widget, you can select one of these events to display its Entity

Details page. From there, you can take additional action against that entity, such as adding the malicious file to your Blacklist.

This widget displays information from the Network, Endpoint, and Email widgets, which you can select individually to view additional information about each of those control points.

The event activity appears in the form of a red area chart that depicts the total number of malicious events for each control point (network, endpoint, and email). You can click through various parts of the Event Activity widget to view additional information:

- Click **7d**, **1m**, **3m**, or **All** to view the information for the last 7 days, 1 month, 3 months, or all dates. The default is 7 days.
- Hover over the chart to display the total number of malicious events for each control point for a particular day.
- Click the dot within a control point to view a list of malicious events for that day.
- Click **Network**, **Endpoint**, or **Email** to view additional information about the malicious events for those control points.

See [“About the Network Event Activity widget”](#) on page 41.

See [“About the Endpoint Event Activity widget”](#) on page 43.

See [“About the Email Event Activity widget”](#) on page 45.

See [“About the New and Unknown Threats widget”](#) on page 46.

See [“About the Endpoints widget”](#) on page 46.

About the Network Event Activity widget

The **Network Event Activity** widget displays information about the network traffic that flows through ATP when scanning is enabled on your appliance. This information appears in the form of an area chart that displays the total number of inspected IPv4 and IPv6 packets, as well as the conviction events created for blocked traffic and traffic identified as malicious.

When traffic is blocked or identified as malicious, ATP creates a conviction event that captures information about that conviction. The Network Event Activity widget lists these events based on their conviction type. You can then select one of these events to display its Entity details page. From there, you can take action against that entity, such as isolating an endpoint or adding a file to your Blacklist.

You can click on various parts of the Network Event Activity widget to view the information you want:

- Click **7d**, **1m**, **3m**, or **All** to view the information for the last 7 days, 1 month, 3 months, or all dates.

The area chart that appears represents the total number of packets inspected for that time period. You can hover over the chart to display the total for an individual day within that period.

- Click **Packets Inspected** to view the total number of all packets inspected for that time period.

This information is represented by a blue area chart.

Click **Blocked** to display the total number of events that were blocked.

This information is represented by a light blue area chart.

- Click **Malicious** to display the total number of events identified as malicious. This information is represented by a red area chart.

You can hover over this chart to display the total number of malicious events for each day within that time period. You can then click on the dot to view the **Network Traffic** dialog box, which shows the number of blocked or malicious events for each conviction type. The conviction type corresponds to the Symantec technology that detected the malicious traffic.

You can select one of the following types:

Conviction Type:	Detects:
Blacklist	IPs, URLs, and domains that are blacklisted in ATP and the Symantec Global Intelligence Network
Vantage	Suspicious network traffic inside the network that is detected by Symantec's Intrusion Prevention System (IPS) technology
Insight	Files with bad reputations that are detected by Symantec's cloud-based reputation database
Mobile Insight	Malware and privacy and performance issues in mobile apps that are detected by Symantec's cloud-based reputation database
Cynic	Unknown malware and advanced threats from files that are executed in a virtual sandbox and then compared to real-world data in the Symantec Global Intelligence Network
AntiVirus	Viruses and malware that are detected by Symantec's signature-based technology

Based on the type that you select, a list of events appears with information about each event. You can then click on an event to display its Entity details page.

Note: **Packets Inspected**, **Blocked**, and **Malicious** are all selected by default, and the information for these packet types appear within the same chart. You can de-select one of these types to remove the information for that type.

See [“About the Endpoint Event Activity widget”](#) on page 43.

See [“About the Email Event Activity widget”](#) on page 45.

See [“About the New and Unknown Threats widget”](#) on page 46.

See [“About the Endpoints widget”](#) on page 46.

See [“About Endpoint details”](#) on page 84.

About the Endpoint Event Activity widget

The **Endpoint Event Activity** widget provides information about the traffic inspected on your endpoints, including malicious and suspicious files that were detected. Malicious files are files that were blocked based on their detection as known threats. Suspicious files are files that were flagged based on their reputation score but were otherwise undetected as malicious. Suspicious files may be benign but may be worth investigating.

When a file is detected as malicious or suspicious, Symantec Endpoint Protection creates a conviction event that captures information about that conviction. The Endpoint Event Activity widget provides information about these convictions based on their conviction type. You can then select one of these events to display its Entity details page. From there, you can take action against that entity, such as adding a file to your Blacklist.

This information appears in the form of an area chart that depicts the total number of all events, the number of malicious, and suspicious events.

You can click various parts of the Endpoint widget to view the information that you want:

- Click **7d**, **1m**, **3m**, or **All** to view the information for the last 7 days, 1 month, 3 months, or all dates.
The area chart that appears represents the total number of events for that time period. You can hover over the chart to display the total for an individual day within that period.
- Click **All** to view the number of events that occurred on a day-by-day basis within that period.
This information is represented by a light blue area chart.
As you hover over this chart, a line appears for each day within that period. Click the dot at the top of the line to view a list of all the events for that day. This list includes the name of the downloaded file, its publisher, the folder on the endpoint

to which it was downloaded, the domain from which it was downloaded, and the date the event was created.

- Click **Malicious** to display the number of malicious files that were blocked on a day-by-day basis within that period.

This information is represented by a dark red area chart.

As you hover over this chart, a line appears for each day within that period. Click the dot at the top of the line to display a dialog box with a drop-down menu that allows you select a conviction type. Based on the type you select, a list of events appears with information about each event.

You can select one of the following conviction types:

- **File**

This list includes the name of the blocked file, the host name, IP address, and user name associated with the endpoint, the folder on the endpoint to which it was downloaded, the action taken on it (for example, quarantined, cleaned, deleted), and the date the event was created.

- **Vantage**

This list includes the host name, IP address, and user name associated with the endpoint, the signature of the malicious file, the path on the endpoint from which the file was detected, the remote IP address related to the file, and the date the event was created.

- Click **Suspicious** to display the number of suspicious files that were flagged on a day-by-day basis within that period.

This information is represented by a light red area chart.

As you hover over this chart, a line appears for each day within that period. Click the dot at the top of the line to view a list of all the events for that day. This list includes the name of the downloaded file, its publisher, the folder on the endpoint to which it was downloaded, the host name and domain from which it was downloaded, and the date the event was created.

Note: **All**, **Malicious**, and **Suspicious** are checked by default, and the information for all their event types appear within the same chart. You can uncheck one to remove the information for that type.

The Endpoint Event Activity widget requires that **Synapse Symantec Endpoint Protection Correlation** is enabled on your appliance.

See [“About the Network Event Activity widget”](#) on page 41.

See [“About the Email Event Activity widget”](#) on page 45.

See [“About the New and Unknown Threats widget”](#) on page 46.

See [“About the Endpoints widget”](#) on page 46.

See [“About the Incident Manager”](#) on page 77.

About the Email Event Activity widget

The **Email Event Activity** widget provides information about malicious files that were detected and blocked in attachments in the email traffic from your endpoints. Malicious files are files that were detected as known threats.

When an attachment is detected with a malicious file, ATP creates an event that captures information about that file, such as its name and the domain from where it was sent. The Email Event Activity widget lists these events, where you can then navigate to the Entity details page for that file or domain to take action against it.

You can click through various parts of the Email Event Activity widget to view the information you want:

- Click **7d**, **1m**, **3m**, or **All** to view the information for the last 7 days, 1 month, 3 months, or all dates.

The area chart that appears represents the total number of files blocked during that time period. You can hover over the chart to display the total for an individual day within that period.

- Click **Malicious** to display the total number of events identified as malicious. This information is represented by a red area chart. You can hover over this chart to display the total number of malicious events for each day within that time period. You can then click on the dot to display the **Email Traffic: Malicious** dialog box, which lists the malicious events. This list includes the name of the malicious file, the domain from which it was sent, the sender's email address, the email addresses of the recipients who received the file, the subject heading of the email, and the date the email was received.

The Email Event Activity widget requires that **Synapse Symantec Email Security.cloud Correlation** is enabled on your appliance.

See [“About the Network Event Activity widget”](#) on page 41.

See [“About the Endpoint Event Activity widget”](#) on page 43.

See [“About the New and Unknown Threats widget”](#) on page 46.

See [“About the Endpoints widget”](#) on page 46.

See [“About the Incident Manager”](#) on page 77.

About the New and Unknown Threats widget

The **New and Unknown Threats** widget lists the number of files that were detected as threats within your environment by the following Symantec technologies:

Cynic	Detects unknown malware and advanced threats from files that are executed in a virtual sandbox and then compared to real-world data in the Symantec Global Intelligence Network
Insight	Detects files with bad reputations using Symantec's cloud-based reputation database
Mobile Insight	Detects malware in mobile apps using Symantec's cloud-based reputation database

The outer arc in the widget represents the total number of detected threats. Each inner arc represents a specific technology and displays the percent of threats detected by that technology. You can hover over an arc to display the total number of threats detected by that technology.

See [“About the Endpoint Event Activity widget”](#) on page 43.

See [“About the Network Event Activity widget”](#) on page 41.

See [“About the Endpoints widget”](#) on page 46.

About the Endpoints widget

The **Endpoints** widget lists the number of infected endpoints in your environment that executed a malicious file within the last seven days. It also lists the total number of endpoints in your environment whether they are infected or not.

You can click on the number of **Actively Infected Endpoints** to view additional information about each endpoint. This information includes the endpoint's host name, IP address, and operating system; the last user to log onto the endpoints; and whether the endpoint is managed by Symantec Endpoint Protection.

From the **Actively Infected Endpoints** page, you can click on an endpoint's **Host Name** to view its Entity details page. From there, you can take action against that endpoint such as isolating it.

See [“About Endpoint details”](#) on page 84.

An infected endpoint with an active malicious file may be part of an active incident.

See [“How ATP creates and prioritizes incidents”](#) on page 36.

Note: The Endpoints widget requires a **Symantec Endpoint Protection Manager Controller Connection**.

See [“About the Endpoint Event Activity widget”](#) on page 43.

See [“About the Network Event Activity widget”](#) on page 41.

See [“About the New and Unknown Threats widget”](#) on page 46.

See [“About the New and Unknown Threats widget”](#) on page 46.

See [“About the Incident Manager”](#) on page 77.

Acting on threats

This chapter includes the following topics:

- [Isolating breached endpoints](#)
- [Remediating malicious files](#)
- [Blacklisting suspicious domains, URLs, and IP addresses](#)
- [About policies](#)
- [Checking the status of an action](#)

Isolating breached endpoints

When you find endpoints that have been compromised, you'll want to remove them from your network so that they can't contaminate other endpoints in your environment. Once the threat is resolved and the endpoint is healthy again, you can rejoin them to your network. ATP supports isolating endpoints on Symantec Endpoint Protection 12.1 RU6 and later.

Note: To isolate and rejoin endpoints from the ATP Manager, you must have a Quarantine Firewall policy in Symantec Endpoint Protection Manager and assigned it to a Host Integrity policy. This requirement is necessary to ensure that the endpoint is put into/taken out of quarantine in the event that your Host Integrity policy FAILS, regardless of what the THEN clause states. Click the following link to learn more about how to create Symantec Endpoint Protection Manager Host Integrity policies:

<http://www.symantec.com/docs/HOWTO101742>

ATP lets you isolate endpoints in several places in ATP Manager. How you perform the task depends on which page in ATP Manager you take the action. Only users with the Admin role or Controller role can isolate endpoints from the network or

rejoin them. These actions appear inactive in the ATP Manager if you do not have the appropriate role.

Table 3-1 To isolate breached endpoints

ATP Manager page	Description
Incident details page	<p>The Incident details page provides information about ATP's evaluation of the incident. It provides information about the events that comprise the incident.</p> <ul style="list-style-type: none">■ To take action from the Incident graph, right-click on the endpoint entity node that you want to take action on and select the action from the context menu.■ To take action from the Actions bar, click Isolate. A dialog box appears. By default, all of the endpoints that can be isolated are selected. Unselect the endpoints that you do not want to isolate, and click Isolate. <p>To rejoin an endpoint to the network, click Rejoin from the Actions bar, select the endpoints that you want to rejoin, and click Rejoin.</p> <p>See “About Incident details” on page 79.</p>
Endpoint details page	<p>The Endpoint details page provides information about all of the events that ATP detected has occurred with this endpoint. It shows the relationship of the endpoint with other entities.</p> <p>You isolate and rejoin endpoints from the Actions bar.</p> <p>See “About Endpoint details” on page 84.</p>

Tip: View the status of executed commands in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

See [Multiple endpoints appear in ATP for the same host/IP address](#).

Remediating malicious files

When you find infected files on your endpoints, you'll want to take action on them so that they don't pose any further harm to your network.

ATP lets you take the following actions on files:

Add to Blacklist	<p>Adds the file to the ATP Blacklist.</p> <p>ATP lets you add the following file hash values to the Blacklist:</p> <ul style="list-style-type: none"> ■ SHA256 ■ MD5 <p>See “Managing policies” on page 61.</p>
Add to Whitelist	<p>Adds the file to the ATP Whitelist.</p> <p>Whitelist the files that you know are not harmful or the files that ATP incorrectly flags as malicious (false positives).</p> <p>See “Reporting false positive and false negative file convictions” on page 53.</p>
Submit to Cynic	<p>Submits the file to Symantec for analysis.</p> <p>Cynic supports the following file types:</p> <ul style="list-style-type: none"> ■ 32- and 64-bit executable ■ Compressed (e.g., ZIP) ■ APK ■ JAR ■ PDF ■ Java ■ Microsoft Office documents <p>Note: You can only submit the files that Symantec has not already recognized as having a good reputation or a bad reputation.</p> <p>After Cynic has analyzed a file, you can view the results on the File details page under Cynic Observed File, Registry, System Changes and Cynic Observed Network Analysis.</p> <p>Note: This action is only supported on the clients that run Symantec Endpoint Protection 12.1 RU6 and later.</p>
Submit to VirusTotal	<p>Submits the file hash to VirusTotal and takes you to the VirusTotal website so that you can view the results.</p>

Copy to file store |
Download from file
store

Copies the file to the file store.

ATP stores the file in a compressed file and copies it to the ATP file store. After the compressed file is copied to the file store, the option changes to let you download the compressed file to your local computer. When you download the compressed file to the file store, you must assign a password for it.

You can open the compressed file on your local computer with the password that you assigned to it and analyze it in your own virtual environment. Or you can submit the file to Cynic.

Note: This action is only supported on the clients that use Symantec Endpoint Protection 12.1 RU6 and later.

Delete File

Deletes the file and the registry entries that point to that file.

Note: This action is only supported on the clients that use Symantec Endpoint Protection 12.1 RU6 and later.

This option remains active until the file is deleted from the endpoint through Symantec Endpoint Protection Manager. Then the option becomes inert for that file.

ATP lets you take action on files in several places in the ATP Manager. How you perform the task depends on which page you take action from. Only users with the Admin role or Controller role can perform any of these actions. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

Table 3-2 To remediate malicious files

ATP Manager page	Description
Incident details page	<p>The Incident details page provides information about ATP's evaluation of the incident. It provides information about the events that comprise the incident.</p> <ul style="list-style-type: none">■ To take action from the Incident graph, right-click on the file entity node that you want to take action on. Select the action that you want to take.■ To take action from the Actions bar, click the action that you want to take. A dialog box appears. By default, all of the files for which that action can be applied are selected. Unselect the files that you do not want to take action on, and click to confirm that you want to proceed with the action. Notes: You cannot submit a file to Cynic from the Incident details Actions bar. Also, when you delete a file from the Actions bar, the file and the registry entries that point to that file are deleted from all endpoints and not just the ones selected. If the file does not exist on an endpoint, then the extra commands show as in-progress in the Action Manager. Symantec recommends that you delete file from the Incident graph or from the File details page Actions bar. <p>See “About Incident details” on page 79.</p>
File details page	<p>The File details page provides information about all of the events that ATP detected has that occurred with this file. It shows the file's relationship with other entities, and it lets you perform containment and remediation tasks from the Actions bar.</p> <p>See “About File details” on page 88.</p>
Policies page	<p>You can create Whitelist and Blacklist policies from the Policies page. You can also view all of the files that you've already whitelisted and blacklisted and remove files from Whitelists and Blacklists.</p> <p>See “About policies” on page 56.</p> <p>See “Managing policies” on page 61.</p>

View the commands that you have executed commands in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

See [Multiple endpoints appear in ATP for the same host/IP address](#).

Reporting false positive and false negative file convictions

A false positive occurs when ATP incorrectly identifies that a file is infected. The criteria that Symantec products use to identify malicious code are constantly updated and revised in response to the newest emerging threats. In some cases, however, legitimate files have been mistakenly classified as a threat. Symantec definitions are continually refined and corrected to identify only malicious code.

Symantec recommends that you treat all files that a Symantec product identifies as being infected as malicious until Symantec Security Response verifies your suspicion of a false detection. If you believe that a legitimate file was identified in error, report the suspected false positive file conviction to Symantec at the following URL:

https://submit.symantec.com/false_positive/

To report a suspected false negative file conviction, contact Support.

https://support.symantec.com/en_US/contact-us.64123.64123.html

See “[About events, incidents, and entities](#)” on page 14.

Manually submitting files to Cynic for analysis

ATP lets you submit the files that it detects as suspicious or malicious to Cynic for analysis with a click of a button. However, you may have instances in which you want to submit files to Cynic manually. For example, you may have obtained a file on a USB that you want to analyze before you move it to your network. Or you learn in an intelligence feed about a file that is suspicious.

See “[Remediating malicious files](#)” on page 49.

Your ATP license lets you manually submit files or SHA256 file hashes to the Cynic portal for analysis (up to 20 submissions per day). Cynic supports the following file types:

- 32- and 64-bit executable
- Compressed (e.g., ZIP)
- APK
- JAR
- PDF
- Java
- Microsoft Office documents

You can download the results in .pdf format. The Cynic portal is supported on the following browsers: Internet Explorer 10 and later, Chrome, FireFox, and Safari.

You must first register as a user with the primary email address associated with your ATP account.

Note: If you have already used your email address to create a Managed Security Services (MSS) or DeepSight account, see the following knowledge base article for how to manually submit files to Cynic.

www.symantec.com/docs/TECH234660

To create a new user on the Cynic portal

- 1 Go to the following URL:
cynic.symantec.com
- 2 At the bottom of the page under the Symantec logo, click **Cynic License Upload Wizard**.
- 3 For step 1, click **Browse** and locate your ATP license and then click **Upload File**.
The license file must be in .slf format or be a .zip file that contains the .slf file.
- 4 Review the *Symantec Cynic Submission Portal Agreement*, and at the bottom click, **I accept the License agreement**. Click **Continue**.
- 5 For step 2, type your registration information and click **Continue**.
- 6 For step 3, confirm your information.
Symantec sends you an email confirming your email address and providing your temporary password. The first time that you log onto the Cynic portal, you must change your password.

To submit a file to Cynic for analysis

- 1 Go to the following URL:
cynic.symantec.com
- 2 Type your email address and password. Click **Login**.
- 3 Follow the on-screen navigation to submit a file or a SHA256 file hash.

Blacklisting suspicious domains, URLs, and IP addresses

When you determine that a domain, URL, or IP address (external computer) is malicious, you can blacklist it. Blacklisting an external computer in Symantec Advanced Threat Protection (ATP) does not block users from accessing it. However,

if you have the network control point integrated, it does generate an event. You can also whitelist the external computers that you know are not harmful.

ATP lets you add external computers to the Blacklist in several places in the ATP Manager. How you perform the task depends on from which page you take action. Only users with the Admin role or Controller role can blacklist external computers. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

Table 3-3

ATP Manager page	Description
Incident details page	<p>The Incident details page provides information about ATP's evaluation of the incident. It provides information about the events that comprise the incident.</p> <ul style="list-style-type: none"> ■ To take action from the Incident graph, right-click on the domain entity node that you want to take action on. Select the action that you want to take. ■ To take action from the Actions bar, click the action that you want to take. A dialog box appears. By default, all of the external computers for which that action can be applied are selected. Unselect the external computers that you do not want to take action on, and click to confirm that you want to proceed with the action. <p>See “About Incident details” on page 79.</p>
Domain details page	<p>The Domain details page provides information about all of the events that ATP detected has occurred with this external computer. It shows its relationship with other entities, and it lets you blacklist or whitelist the external computer from the Actions bar.</p> <p>See “About Domain details” on page 97.</p>
Policies page	<p>You can create Blacklist policies from the Policies page. You can also view all of the external computers that you've already whitelisted and blacklisted and remove domains from Whitelists and Blacklists.</p> <p>See “Blacklisting suspicious domains, URLs, and IP addresses” on page 54.</p> <p>See “Managing policies” on page 61.</p>

View the commands that you have executed commands in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

About policies

The **Policies** page lets you create Blacklist policies and Whitelist policies for files and external computers. This page is also where you can manage the policies that you created or that Symantec Advanced Threat Protection (ATP) creates when you take the Add to Blacklist or Add to Whitelist action when remediating incidents.

Only users with the Admin or Controller role can create Blacklist policies and Whitelist policies.

Table 3-4 Policy types

Policy	Description
Blacklist	<p>These are the files and external computers that ATP has not identified as a threat, but that you deem untrustworthy.</p> <p>If you run ATP in inline block mode, ATP blocks users from accessing the external computers or files that you specify in your Blacklist policies. If you run ATP in tap mode or inline monitor mode, users can access items in your Blacklist. ATP generates an event when users attempt to access items in Blacklist policies regardless of which operation mode you use.</p> <p>See “Viewing the events that occur in your environment” on page 31.</p>
Whitelist	<p>These are the files and external computers that you know are safe. ATP considers these items trustworthy and takes no action when endpoints access them.</p>

See [“Managing policies”](#) on page 61.

Creating a Blacklist policy

Symantec maintains a worldwide blacklist of external computers and files that is updated regularly and integrated with Symantec Advanced Threat Protection (ATP). You can supplement this list by creating Blacklist policies for external computers or files that you deem untrustworthy. For example, you may want to create a Blacklist policy for a file that recently appeared in your cybersecurity intelligence that Symantec has yet to identify as a threat.

Create a Blacklist policy to do any of the following:

Block or detect access to an external computer	<p>You can create a Blacklist policy for an external computer based on its IP address or subnet, domain, or URL.</p> <p>If you run ATP in inline block mode, ATP blocks access to external computers. When a user attempts to access a blacklisted external computer, a blocking page appears indicating why access is denied. If you run ATP in any other mode, ATP does not block access. ATP generates an event when users attempt to access items in Blacklist policies regardless of which operation mode you use.</p> <p>See “About Events” on page 100.</p>
Block or detect access to a file	<p>You can create a Blacklist policy for a file based on its hash value as follows:</p> <ul style="list-style-type: none">■ MD5 If ATP is integrated with Symantec Endpoint Protection, Symantec Endpoint Protection prevents blacklisted MD5 files (Windows executable files and MSI installers) that are on your endpoints from running. When you create a Blacklist policy for a file using its MD5 hash value, the hash value is added to the ATP blacklisted file on Symantec Endpoint Protection Manager. This file is added to the File Fingerprint Lists policy for all domains and all groups within those domains. If you add a new group to Symantec Endpoint Protection, the ATP blacklisted file is subsequently synchronized with that group as well. Additionally, if you edit the ATP blacklisted file on Symantec Endpoint Protection (for example, by removing an entry), Symantec Endpoint Protection overwrites your edits the next time that the file is synchronized. The ATP blacklisted file does not affect other fingerprint files that you create in Symantec Endpoint Protection.■ SHA256 If Symantec Endpoint Protection is configured to use your ATP proxy, Symantec Endpoint Protection immediately quarantines blacklisted SHA256 files when it detects them on your endpoints. <p>If you run ATP in inline block mode, ATP blocks access to blacklisted files. When a user attempts to access a blacklisted file, a blocking page appears. If you run ATP in any other mode, ATP does not block access. ATP generates an event when users attempt to access items in Blacklist policies regardless of which operation mode you use.</p>

You must have the Admin role or Controller role to create Blacklist policies.

To create a Blacklist policy

- 1 In the ATP Manager, click **Policies > + Add to Blacklist**.
- 2 In the **Add to Blacklist** dialog box, click the **Type** drop-down list and select one of the following:

- IP address
- Domain
- URL
- File Hash (SHA256)
The SHA256 hash value must be 64 characters with values ranging between 0 - 9 and a - f.
- File Hash (MD5)

Note: You cannot edit the **Type** or **Match Value** of a blacklisted item after you add it. However, you can delete it or edit the comment.

See [“Managing policies”](#) on page 61.

- 3 In the **Match Value** field, type the value of the blacklisted item based on the type that you selected.

ATP validates the value based on its type. The **Match Value** appears in the **Blacklist policy** list as the **Rule Value**.

See [“Supported policy match values for IP addresses, domains, and URLs”](#) on page 60.

- 4 Optionally, type a comment in the **Comments** field.

For example, you may want to specify the file name for SHA256 hash.

- 5 Click **Save**.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

See [“Remediating malicious files”](#) on page 49.

Creating a Whitelist policy

You can create Whitelist policies for files and external computers so that Symantec Advanced Threat Protection (ATP) explicitly allows access to them regardless of their reputation. When you whitelist an item, ATP considers it "trusted" and takes no action on it. For example, if you whitelist a file, ATP does not inspect that file nor does it request a reputation score for it. Whitelisting trusted files and external computers can conserve scanning resources and reduce the number of events that ATP creates. It can also eliminate false negatives.

See [“Reporting false positive and false negative file convictions”](#) on page 53.

Create a Whitelist policy to do any of the following:

Allow explicit access to an external computer

When you whitelist an external computer, ATP considers it trustworthy and does not inspect traffic to or from it from your endpoints (even if it's blacklisted). You can whitelist an external computer based on its IP address or subnet, domain, or URL.

ATP allows access to whitelisted computers in the following ways:

- IP address and IP subnet
If you whitelist an IP address, ATP bypasses all traffic inspection to and from that IP address. However, it continues to inspect traffic associated with other IP addresses on the same subnet of that IP address.
- Domain
If you whitelist a domain, ATP allows access to any sub-domains and URLs associated with that domain.
- URL
If you whitelist a URL, ATP allows access to any sub-pages (including files) associated with that URL.

Allow explicit access to a file

You create a Whitelist policy for a file based on its SHA256 hash value or URL. If you whitelist a file based on its SHA256 hash value, ATP allows access to it on any external computer. If you whitelist a file based on its URL, ATP allows explicit access to it on that site only.

When you whitelist a file, ATP considers it trustworthy regardless of its identity as a known threat or its reputation. When an endpoint accesses a whitelisted file, ATP takes no action against it. For example, if Symantec Endpoint Protection is configured to use your ATP proxy, ATP does not block the file (even if it's blacklisted). If Symantec Endpoint Protection is not configured to use your ATP proxy, ATP does not generate a detection event.

You must have the Admin role or Controller role to create Whitelist policies.

To create a Whitelist policy

- 1 Click **Policies > + Add to Whitelist**.
- 2 In the **Add to Whitelist** dialog box, click the **Type** drop-down list and select one of the following:
 - IP address
 - Domain
 - URL
 - File Hash (SHA256)

The SHA256 hash value must be 64 characters with values ranging between 0 - 9 and a - f.

Note: You cannot edit the **Type** or **Match Value** of a whitelisted item after you add it. However, you can delete it or edit the comment.

See [“Managing policies”](#) on page 61.

- 3 In the **Match Value** field, type the value of the whitelisted item based on the type that you selected.

ATP validates the value based on its type. The **Match Value** appears in the **Whitelist policy** list as the **Rule Value**.

See [“Supported policy match values for IP addresses, domains, and URLs”](#) on page 60.

- 4 Optionally, type a comment in the **Comments** field.

For example, you may want to specify the file name for SHA256 hash.

- 5 Click **Save**.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

See [“About Domain details”](#) on page 97.

See [“Remediating malicious files”](#) on page 49.

See [“About File details”](#) on page 88.

Supported policy match values for IP addresses, domains, and URLs

Table 3-5

Type	Description	Example
Domain or URL	You can use special characters, such as international characters	http://gość.pl/a
	You can use full or partial domain names.	gov.ca/dmv .gov.ca Note: ATP looks for the most specific match when you have both Blacklist and Whitelist policies with similar domain names. For example, you can blacklist news.google.com and whitelist google.com.

Table 3-5 (continued)

Type	Description	Example
IP address or IP subnet	You can use both the IPv4 and IPv6 protocols	<p>10.10.10.0/24</p> <p>fe80::250:56ff:fe99:3903</p> <p>Note: ATP looks for the most specific match when you have both Blacklist and Whitelist policies with similar IP addresses. For example, you can blacklist an IP address that falls within a whitelisted IP subnet.</p> <p>Note: Unspecified addresses, zero subnet masks, and zero CIDR bit length/prefixes are not allowed.</p> <p>Examples:</p> <ul style="list-style-type: none"> ■ 0.0.0.0 ■ d.d.d.d/0.0.0.0 ■ d.d.d.d/0
	You can use dot-decimal notation for IPv4	<p>010.010.010.010</p> <p>Note: You can eliminate leading zeros. For example, you can represent 010.010.010.010 as 10.10.10.10.</p>
	You can use IPv4-compatible addresses for IPv6	<p>::w.x.y.z</p> <p>where w.x.y.z is an IPv4 public address assigned to an interface on the computer.</p>
	You can use colon-eliminated hex notation for IPv6	<p>For example, you can represent FF01:0:0:0:0:0:0:101 as FF01::101.</p>

See [“Creating a Whitelist policy”](#) on page 58.

See [“Creating a Blacklist policy”](#) on page 56.

See [“Managing policies”](#) on page 61.

Managing policies

Symantec Advanced Threat Protection (ATP) helps you manage the policies that you create either manually or that are created when you take the Add to Blacklist or Add to Whitelist action on the files and endpoints that you analyze.

See [“Creating a Blacklist policy”](#) on page 56.

See [“Creating a Whitelist policy”](#) on page 58.

See [“Remediating malicious files”](#) on page 49.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

You must have the Admin role or Controller role to add and remove Blacklist policies or Whitelist policies. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

Table 3-6 Manage policies

Task	Procedure
To view existing policies	On the ATP Manager navigation pane, click Policies . The Blacklist appears by default. Click the Whitelist tab to view Whitelist policies.
To view or modify a comment	<ol style="list-style-type: none">1 Hover over the policy for which you want to view, add, or update a comment. Options appear in the right column.2 Click the comment graphic.3 Write a new comment or modify the existing comment and click Update.
To move a policy to the other list	<ol style="list-style-type: none">1 Hover over the policy that you want to move. Options appear in the right column.2 Click the check box.3 Click OK to confirm that you want to move the policy to the other list.
To filter policies	Click Show Filters and select one or more policies that you want to filter on.
To search policies	Type the search value into the Search field. Matching values appear as soon as you start populating this field.
To delete a policy	<ol style="list-style-type: none">1 Hover over the policy that you want to delete. Options appear in the right column.2 Click the trash can graphic, and click OK in the confirmation dialog box.

See [“About policies”](#) on page 56.

Checking the status of an action

The Action Manager shows the status of the asynchronous actions that are taken on entities. If you take the same action on multiple entities, the Action Manager contains a line item for each individual action. For example, assume that you are

on the File details page and you see that a file is on Endpoint A, Endpoint B, and Endpoint C. ATP lets you delete the file from all three endpoints with a single click. When you navigate to the Action Manager table, you see an entry showing the status of deleting the file from Endpoint A, an entry showing the status of deleting the file from Endpoint B, and an entry showing the status of deleting the file from Endpoint C.

Note: The time it takes for an action to complete depends on the action that you are taking. Some actions may take several Symantec Endpoint Protection Manager heartbeat intervals to complete.

Tip: You can also log into Symantec Endpoint Protection Manager and look at the status of the commands that were issued from ATP on the Symantec Endpoint Protection Manager **Monitors** page.

To check the status of an action

- 1 On the ATP Manager navigation pane, click **Action Manager**.
- 2 To filter the incidents, click **Show Filters**. Select the **Start Date and Time** and **End Date and Time** (in UTC). Click **Reset all filters** to reset your filter criteria. Click **Hide Filters** to hide the filters view.

Table 3-7 provides information about the actions that are taken in ATP.

Table 3-7 Action Manager table

Column	Description
Action	<p>The action that was taken on an incident or event.</p> <p>Actions include the following:</p> <ul style="list-style-type: none">■ Get a file■ Submit to Cynic■ Delete a file■ Isolate endpoint■ Rejoin endpoint
Endpoint	<p>Any of the following:</p> <ul style="list-style-type: none">■ The endpoint that is being isolated or rejoined to the network■ The endpoint that contains the file or email that is being deleted■ The endpoint that contains the file that is being blacklisted, unblacklisted, whitelisted, unwhitelisted, submitted to Cynic, or downloaded■ The endpoint that accessed the domain that is being blacklisted, unblacklisted, whitelisted, unwhitelisted

Table 3-7 Action Manager table (*continued*)

Column	Description
Status	Statuses includes the following: <ul style="list-style-type: none">■ In progress■ Upload in progress■ Completed■ Clean/Malware This appears for items that are successfully submitted to Cynic.■ Error
Description	Provides a description of the action taken. In instances where a file is submitted to Cynic, the results from Cynic appear in the Description field.
Initiated By	The person who initiated the action.
Time	The time the action was initiated in UTC.

See [“About Incident details”](#) on page 79.

See [“About Endpoint details”](#) on page 84.

See [“About File details”](#) on page 88.

See [“About Domain details”](#) on page 97.

Recovering after threats have been contained

This chapter includes the following topics:

- [Recovery best practices](#)
- [About Reports](#)

Recovery best practices

After a threat has been contained and you have implemented your cybersecurity recovery plan, Symantec recommends that you do the following:

Analyze the incident. Consider the following about the security event:

- What was the overall scope of the breach?
- What events made up the breach?
- What happened as a result of the incident/events?
- What entities were affected by the breach?

You can use the Search, the Events page, Reports, and the Incident Manager to study what occurred and determine where your network was compromised.

See [“About searching for indicators of compromise \(IOC\)”](#) on page 18.

See [“About Events”](#) on page 100.

See [“About Reports”](#) on page 66.

See [“About the Incident Manager”](#) on page 77.

Take steps to prevent similar, future threats.	<p>Based on your analysis of how the breach occurred, the following are some suggestions on ways to prevent future attacks:</p> <ul style="list-style-type: none"> ■ Make sure that your endpoints are protected with the most recent version of Symantec Endpoint Protection. ■ Subscribe to a sharing community or indicator feeds to learn about new threats that you can proactively block. See “Managing policies” on page 61. ■ Communicate with employees your organization's IT best practices as well as your IT security policies and procedures.
Contact affected parties.	<p>Contact customers, business partners, and suppliers to let them know about the possible impact of the breach and the steps you're taking to recover. Also indicate how you intend to protect them.</p> <p>If the breach was the result of an action by a third party, re-evaluate your IT security policies to see how future threats can be thwarted.</p>
Report the incident.	Report a suspected or confirmed breach to the appropriate internal management entities and external oversight entities.
Update your cybersecurity plan.	Your cybersecurity plan should be a dynamic document that is continually updated and modified. You should also regularly test your cybersecurity plan.

About Reports

The Symantec Advanced Threat Protection (ATP) Reports option provides you with the Executive Report.

What is the Executive Report?

As an administrator or controller, you may need to provide your executive team with regular updates regarding your organization's threat activities. With its charts, lists, and summaries, you can use the Executive Report to provide monthly visibility into recently infected endpoints, the domains that targeted them, and open high and medium incidents. You can point out trends that occurred during this period based on your efforts to remediate threats, and then communicate any mitigation plans.

The Executive Report is available in PDF format. You can run the Executive Report on-demand, or you can create a schedule to run it at regular intervals. When you run or schedule the report, you can specify recipients (such as yourself and other members of your executive team) to whom you want it emailed. Recipients can also download it from ATP Manager.

Note: The Executive Report is designed to provide you with a trend analysis of your threat activity for the 30 days prior to its run date. Do not use it as a tool for identifying and responding to threats in real-time. For information on how to remediate threats, see:

Symantec Advanced Threat Protection Platform Security Operations Guide

What sections are included in the Executive Report?

[Table 4-1](#) lists the sections included in the Executive Report.

The Executive Report includes a cover page that lists the name of its schedule, the user who ran or scheduled it, and the date and time on which it ran. Each section includes a chart that displays daily activity for the 30 days prior to its run date.

For information on how to use the Executive Report, See [“How to use the Executive Report”](#) on page 75.

Table 4-1

Section	Description
Recently Infected Endpoints	<p>Charts and summarizes the number of endpoints that were infected based on whether the infections were:</p> <ul style="list-style-type: none">■ Detected on endpoints without SEP These endpoints are not protected by Symantec Endpoint Protection. The infected files on these endpoints are detected only by network-based threat detection technologies.■ Detected on endpoints with SEP These endpoints are protected by Symantec Endpoint Protection. The infected files on these endpoints are detected by both network and endpoint-based threat detection technologies.

Table 4-1 (continued)

Section	Description
Domains Showing Threat Behavior	<p>Charts and summarizes the number of malicious domains that targeted your endpoints based on the following types:</p> <ul style="list-style-type: none"> ■ Malware A virus that you download onto your computer that runs without your knowledge. It is designed to steal your personal information, or to use your computer to attack other computers. Vantage or IPS may trigger the following classes of malicious signature-based domains: <ul style="list-style-type: none"> ■ Web Attack: Fake Scan Webpage 16 ■ System Infected: Trojan.Cryptolocker.N Activity 3 detected ■ Botnet A type of malware on your computer that is controlled by an attacker. The attacker can send instructions to the bot to perform various tasks, such as collect data, or monitor your actions. ■ Fraud A fraudulent website hosted by an attacker that resembles a trustworthy website, such as Facebook. Vantage or IPS may trigger the following class of a malicious signature-based domain: <ul style="list-style-type: none"> ■ Web Attack: Facebook Manual Share 35 ■ Phishing An email that appears to come from a reliable source that includes a malicious link to a forged website. This site is designed to get you to reveal confidential information, such as your bank account number and password or credit card number. ■ Attack An attack that occurs when you visit a malicious website that deceives you into performing some action (such as updating your browser). Vantage or IPS may trigger the following class of a malicious signature-based domain: <ul style="list-style-type: none"> ■ Web Attack: Fake Scan Webpage 7 <p>Note: If a domain infected more than one asset on a given day, that domain is counted only once for that day.</p>

Table 4-1 (continued)

Section	Description
High and Medium Open Incidents	<p>Charts the number of high and medium incidents that are still open for the days on which they were opened. Also lists the 10 most recent incidents opened.</p> <p>High and medium incidents are defined as:</p> <ul style="list-style-type: none">■ High The incident could result in a business outage, loss of data, or have a severe impact on your business.■ Medium The incident may have an impact on the business, and the use of the system in question might need to be limited while the incident is being addressed. <p>Note: The incidents are listed based on their priority (High followed by Medium), and then by date on which they were created.</p>

Who can run a report and create a report schedule?

As an administrator or controller, you can:

- Create a schedule to run a report automatically on a daily, weekly, or monthly interval
See [“Running and scheduling reports”](#) on page 69.
- View and delete a report schedule
See [“Viewing and deleting reports and report schedules”](#) on page 72.
- View, download, and delete a completed report
See [“Viewing and deleting reports and report schedules”](#) on page 72.

As a user, you can:

- View and download a completed report
See [“Viewing and deleting reports and report schedules”](#) on page 72.

Running and scheduling reports

You can run a report on-demand, or you can schedule a report to run automatically on a regular interval.

When you run or schedule a report, you can choose to email a PDF copy of it to yourself and to other recipients. (These recipients only need a valid email address; they do not need to be part of your organization.) Recipients receive the report as an attachment to an email notification shortly after the report runs. This notification

includes a link to ATP Manager where recipients can view and download the report if there is a problem with the attachment.

You can view a list of previously completed reports in ATP Manager where you can download or delete them. You can also view previously scheduled reports in ATP Manager where you can delete them.

Running reports on-demand

As an administrator or controller, you can run a report on-demand.

To run a report on-demand

- 1 From ATP Manager, click **Reports**.
- 2 On the Reports screen, hover over the report you want to run, and then click **Run**.
- 3 On the report's dialog box, complete the following:

Report Name

Type a name for this report.

Recipients Email

Enter the email addresses of the recipients to whom you want to send a copy of the report. Separate multiple email addresses with a semicolon (;).

Note: Your email address automatically appears in this field. However, you can delete it if desired.

Note: Some SMTP servers limit the number of emails that a user can send per day and the number of recipients per message. As such, you may want to restrict the number of recipients, or use an email distribution list instead.

- 4 Click **Save**.

Scheduling reports

As an administrator or controller, you may need to run the same report on a regular basis and distribute it to one or more individuals. You can schedule a report to run automatically on a daily, weekly, or monthly interval.

You can schedule a report to run at any time. However, for performance reasons, it is recommended that you schedule a report to run in off-peak hours. You specify the time you want the report to run in Coordinated Universal Time (UTC). So, for

example, if you want the report to run at 1:00 A.M. EST, you specify 6:00 A.M. UTC (depending on Daylight Savings Time).

You can create more than one schedule for the same report as long as you specify a different name for each schedule. For example, as a controller, you may want to run the Executive Report for yourself on a weekly basis, but for a wider group of recipients on a monthly basis. In this example, you can name the first report Executive Report Weekly, and the second report Executive Report Monthly.

You can also schedule multiple reports to run at the same time. Reports that are scheduled to run at the same time are queued to run one at a time, so therefore may not run at the exact time specified.

Note: You cannot edit a report schedule after you create it. If you want to change an existing schedule, you must delete it and re-create it.

Scheduling a report

- 1
- From ATP Manager, click **Reports**.
- 2
- On the Reports screen, hover over **Executive Report**, and then click **Schedule**.
- 3
- On the Executive Report screen, complete the following:

Schedule Name	Type a name for this schedule.
Repeats	<div>From the drop-down menu, select the frequency for which you want this report to run.</div> <div><div><div>■</div>Daily</div><div><div>■</div>Weekly</div><div><div>■</div>Monthly</div></div> <div><div>Select one or more days of the week on which you want this report to run.</div><div>Enter the day of the month on which you want this report to run.</div></div>
Time (UTC)	<div>From the drop-down menu, select the UTC time (listed in 15 minute intervals) at which you want this report to run.</div> <div>Note: This time is used for each day of the week that you specify when creating a weekly schedule.</div>

Recipients Email	<p>Enter the email addresses of the recipients to whom you want to send a copy of this report. Separate multiple email addresses with a semicolon (;).</p> <p>Note: Your email address automatically appears in this field. However, you can delete it if desired.</p> <p>Note: Some SMTP servers limit the number of emails that a user can send per day and the number of recipients per message. As such, you may want to restrict the number of recipients, or use a DL instead.</p>
------------------	--

- 4 Click **Save**.
- See [“About Reports”](#) on page 66.
- See [“Viewing and deleting reports and report schedules”](#) on page 72.

Viewing and deleting reports and report schedules

The Executive Report page has two sections. The **Schedules** section lets you view and delete report schedules. The **Reports** section lets you view, download, and delete completed reports. (Completed reports include those that you ran on-demand, and those that ran from a schedule.)

Your role determines which actions you can perform.

You can also create report schedules and run reports on-demand.

Schedules

The **Schedules** section lists the report schedules in the order in which you created them. It includes the following information:

Schedule Name	The name of the schedule
Created By	The individual who created the report schedule
Recurrence	The frequency (Monthly, Weekly, or Daily) and UTC time on which the schedule runs
Recipients	The email addresses of the recipients to whom the completed report is emailed. Multiple recipients are listed in a drop-down menu

As an administrator or controller, you can delete a report schedule. When you do so, its completed reports are not deleted with it. Additionally, the report will complete if it is currently running (or queued to run) at the time you delete its schedule.

Note: You cannot edit a report schedule after you create it. If you want to change an existing schedule, you must delete it and re-create it.

To delete a report schedule

- 1 From ATP Manager, click **Reports**.
- 2 On the Executive Report screen, under Schedules, hover over the schedule that you want to delete, and then click the **Delete** icon.

Reports

The Reports section lists the completed reports in the order in which they ran (whether on-demand or from a report schedule). It includes the following information:

Report Name	The name of the report
Created By	The individual who ran the report on-demand, or created the report schedule
Last Run Date/Time	The date and UTC time on which the report last ran
Scheduled	Whether or not (Yes or No) the report was generated from a report schedule If No, the report was run on-demand.

Status

The current execution state of the report.
These include:

- **Running**
The report is currently running.
- **Queue**
The report is in the queue to run. This typically means that multiple reports are scheduled to run at the same time, and that another report is currently running.
- **Failed**
The report encountered an error while running, and could not complete.
- **Completed with error**
The report completed but encountered one or more errors. The error(s) that the report encountered are listed in the report.
- **Completed**
The report completed with no errors.

As an administrator, controller, or user, you can download a report in PDF format to view it.

Reports are not deleted automatically; you must manually delete them when they are no longer needed. As an administrator or controller, you can delete reports.

- **Create a report schedule**
See [“Running and scheduling reports”](#) on page 69.

To delete or download a completed report

- 1 From ATP Manager, click **Reports**.
- 2 On the Executive Report page, under Reports, do one of the following:
 - Hover over the report that you want to delete, and then click the **Delete** icon.
 - Hover over the report that you want to download, and then click the **Download** icon.

Note: Your browser determines whether the report is saved to a default or specified location.

See [“About Reports”](#) on page 66.

How to use the Executive Report

The information that appears on the Executive Report is dependent on many factors, such as how you configured ATP, your organization's remediation policies, and the types of threats that target your users. As such, the best way to use this report is to validate whether its information adheres to your organization's processes for identifying and remediating threats, assessing your current threat level, and then adjusting your strategy to mitigate future attacks. Often, this is a collaborative effort that involves multiple parties which may take several iterations of month-over-month analysis.

In the short term, though, the Executive Report is designed to create a dialog between controllers and the executive team regarding your current threat level. As a controller, you may be required to provide answers to questions posed by the executive team based on the report's information. The following are examples of such questions:

Recently Infected Endpoints

- Why are there endpoints that are not protected by SEP?
Are they new endpoints or rogue endpoints?
- Are the same endpoints being detected month-over-month?
If so, who do these endpoints belong to?
- Are certain types of endpoints being detected; for example, a database server?
- Is the number of unprotected endpoints trending upwards or downwards month-over-month?

Domains Showing Threat Behavior

- What types of domains are targeting our endpoints the most?
If phishing, how can we increase detection on our endpoints at the network level?
If botnet, has malware taken control of one or more of our endpoints?
- Do we tend to see spikes in attacks based on certain times of the week, month, or year?
- Is the number of attacks for any given domains trending upwards or downwards month-over-month?

High and Medium Open Incidents

- Why is it taking so long to resolve high incidents?
Isn't our policy to resolve them in 3 days?
- What types of threats are associated with these incidents?

What is our plan to protect ourselves against these types of threats in the future?

- How do we plan on responding to the endpoints for which these incidents are open?

Has other malware been detected on these endpoints?

- Is the number of open incidents trending upwards or downwards month-over-month?

See [“About Reports”](#) on page 66.

See [“Running and scheduling reports”](#) on page 69.

See [“Viewing and deleting reports and report schedules”](#) on page 72.

About incident-related pages in the ATP Manager

This appendix includes the following topics:

- [About the Incident Manager](#)
- [About Incident details](#)
- [About Endpoint details](#)
- [About File details](#)
- [About Process Behavior details](#)
- [About Domain details](#)
- [About Events](#)

About the Incident Manager

The Incident Manager provides information about the incidents that ATP detects.

See [“About events, incidents, and entities”](#) on page 14.

To get to the Incident Manager, click the following graphic on the ATP Manager navigation pane.



Click on any of the following links to learn more about that section of the Incident Manager page.

[Incident Over Time Histogram](#) | [Incidents table](#)

Incident Over Time Histogram

The Incidents Over Time histogram lets you view the number of incidents that occurred over a set period of time. Hover your mouse over a data point in the histogram to see the number of incidents that occurred on that day.

To change the histogram time frame, under **Incidents Over Time**, click one of the pre-set time ranges (the last 7 days, the last month, the last 3 months, or all incidents).

Hover over data points in the histogram to reveal how many incidents were detected on that date.

Tip: Check specific days and the times that convictions occur. If malicious activity is detected at very regular intervals, it is possible that malware is responsible for the downloads or server communications. If malicious activities happen at irregular intervals during normal workdays, it is more likely that humans are the cause.

Incidents table

To filter the incidents by incident state (open or closed), click **Show Filters** and select the state that you want to filter on. Click **Hide Filters** to hide the filters view.

The Incident Manager table provides the following information about the incidents that ATP detects:

ID	A unique number that is assigned to the incident.
Description	<div>The reason that the collection of events is considered an incident.</div> <div>For example, ATP may report a new incident because there are repeated events from the same external IP address. It may report a new incident because there are repeated detections for the same internal IP address. Or it may report a new incident because multiple endpoints downloaded the same malicious file.</div>
Last updated	The date and time (in UTC) that the latest event occurred for this incident.

Priority	<p>The priority of the incident is determined based on Symantec's analysis of the severity of the incident.</p> <p>The priority can be one of the following:</p> <ul style="list-style-type: none"> ■ High - ATP detected a threat that Symantec classifies as malicious with high confidence. The threat was not blocked, possibly because the device operates in Tap mode. High priority incidents can result in outages, loss of data, or have a severe impact on the organization and needs to be responded to immediately. ■ Medium - The appliance detected a low-risk threat, such as unblocked adware. Medium priority incidents may have impact on the organization and the system in question. ■ Low - The incident is not deemed to be a serious threat at this time. Low priority incidents do not affect critical business operations. Systems can continue to function as normal.
Status	<p>The field shows the current status of the incident:</p> <ul style="list-style-type: none"> ■ Open - The incident is deemed to be a threat and has not been remediated. ■ Closed - The incident is remediated or deemed not to be a threat and has been closed.

To view the events that comprise the incident and to take remediation actions, click anywhere in the row for that incident to open an Incident details page.

See [“How ATP creates and prioritizes incidents”](#) on page 36.

See [“About Incident details”](#) on page 79.

About Incident details

Incident details provide information about the events that comprise the incident.

To get to the Incident details page, click **Incident Manager** on the ATP Manager navigation pane. In the Incident Manager, click on any incident to open the Incident details page.

Click on any of the following links to learn more about that section of the Incident details page.

[Summary](#) | [Incident graph](#) | [Actions](#) | [Events](#)

Summary

The unique incident number appears along with a description of the incident. Beneath the description is Symantec's recommended actions for how to address this incident.

The summary also provides the following information about the incident:

PRIORITY	<p>The priority that is assigned to this incident is based on Symantec Advanced Threat Protection (ATP)'s evaluation of the severity of the incident.</p> <p>Incidents that consist of the events that Symantec knows are part of a targeted attack are prioritized higher than incidents without such events. Incidents with a high number of events are prioritized higher than incidents with fewer events. Incidents with events that occurred more recently are prioritized higher than older incidents.</p> <p>The priorities are as follows:</p> <ul style="list-style-type: none"> ■ High - ATP detected a threat that Symantec classifies as malicious with high confidence. The threat was not blocked, possibly because the device operates in Tap mode. High priority incidents can result in outages, loss of data, or have a severe impact on the organization and needs to be responded to immediately. ■ Medium - The appliance detected a low-risk threat, such as unblocked adware. Medium priority incidents may have impact on the organization and the system in question. ■ Low - The incident is not deemed to be a serious threat at this time. Low priority incidents do not affect critical business operations. Systems can continue to function as normal.
TARGETED ATTACK	Whether ATP has evaluated the events constituting this incident and deems this threat to be targeted specifically at your organization or industry.
AFFECTED ENDPOINTS	The number of endpoints in your environment that are affected by this incident.
NETWORK SCANNER	<p>The ATP scanner that detected this incident.</p> <p>If multiple scanners detected the incident, the number of scanners appears. Hover over this field to view the names of all of the scanners that detected this incident.</p>
EVENT COUNT	<p>The number of events that comprise this incident.</p> <p>See the Events table below for a list of all of the events that comprise this incident.</p>
INCIDENT STATUS	<p>The current status of the incident.</p> <ul style="list-style-type: none"> ■ Open - The incident is deemed to be a threat and has not yet been remediated. ■ Closed - The incident is remediated or deemed not to be a threat and has been closed.

FIRST SEEN	The date and time that ATP detected the first event in this incident.
LAST SEEN	The date and time that ATP detected the latest event in this incident.
LAST UPDATED	The date the last event comprising the incident occurred.

Incident graph

The Incident graph is a visual display of the information that is found in the **Events** table below it. The Incident graph depicts entities' relationships to one another — it is not a causal depiction. The following graphic shows the entity nodes. Entity nodes are interactive graphics that represent the entities that are involved in incidents: domain, endpoint, email (that contains a file entity), and file, respectively.



Note: While the nodes are referred to as "entity" nodes, the email node is representative of a control point that contains a file entity, but the email itself is not an entity.

The colors of the circles around the entity nodes in the Incident graph indicate their health. For example, red indicates malicious; green means healthy. Gray means that the entity's inert. Entity nodes can also indicate the state of the entity. For example, the following graphic depicts an isolated endpoint.



Hover over the entity node to view details about it. For example, hovering over the domain entity node reveals the entity's domain name or IP address.

Right-click on an entity node to view a menu that lets you perform the tasks that are associated to that entity, such as going to the entity's details page or showing related entities.

Note: The actions to Copy to file store, Submit to Cynic, and Delete File are supported only for clients that use Symantec Endpoint Protection 12.1 RU6 and later.

The primary node initially appears in the center of the Incident graph. Nodes that are related to the incident appear slightly smaller than the primary node and are connected by a solid line. Expansions of a node that are not connected to the incident (such as when you right-click on a node and select to show, for example, the endpoints that accessed a domain) are indicated with dashed lines.

You can move around the Incident graph using the navigation keys. Or you can use your mouse wheel to expand or shrink the Incident graph view. Use your mouse pointer to move and rearrange the entity nodes. Double-click on any node to bring that node to the center of the Incident graph.

Note: If you refresh the page or go to another page and return, the Incident graph returns to its original state.

Note: If you have an endpoint under a workgroup with a name that exceeds 15 characters, the host name is reported twice: once with a short host name of 15 characters; the other with the full host name exceeding 15 characters. So the same endpoint may appear twice — once for each reported host name. This issue is a result of NetBIOS restrictions. Click the following link for more information:
<https://support.microsoft.com/en-us/kb/909264>

Actions

The Actions bar lets you take any of the following actions. If you have multiple Symantec Endpoint Protection Controllers, you can select on which managed endpoints you want to take the targeted action:

- Add to Blacklist
- Add to Whitelist
- Rejoin¹
Supported only for Symantec Endpoint Protection 12.1 RU6 and later.
- Isolate¹
Supported only for Symantec Endpoint Protection 12.1 RU6 and later.

- **Delete File**
Supported only for Symantec Endpoint Protection 12.1 RU6 and later.
When you delete a file from the Actions bar, it deletes the file and the registry entries that point to that file are deleted from all endpoints and not just the ones selected. If the file does not exist on an endpoint, then the extra commands show as in-progress in the Action Manager. Symantec recommends that you delete file from the Incident graph or from the File details page Actions bar. This option remains active until the file is deleted from the endpoint through Symantec Endpoint Protection Manager. Then the option becomes inert for that file.
- **Comment**
Maximum of 512 characters.
- **Close**
This option only appears if the incident is open. You must create a comment to close the incident.

See [“Remediating malicious files”](#) on page 49.

See [“Isolating breached endpoints”](#) on page 48.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

¹ To isolate and rejoin endpoints from the ATP Manager, you must have a Quarantine Firewall policy in Symantec Endpoint Protection Manager and assigned it to a Host Integrity policy. This requirement is necessary to ensure that the endpoint is put into/taken out of quarantine in the event that your Host Integrity policy FAILS, regardless of what the THEN clause states. Click the following link to learn more about how to create Symantec Endpoint Protection Manager Host Integrity policies: <http://www.symantec.com/docs/HOWTO101742>

When you select an action, a dialog box appears that lists all the entities that you can perform that action on. Unselect any entities in the dialog box that you don't want to perform this action on.

Only users with the Admin role or Controller role can perform actions. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

The time it takes for an action to complete depends on the action that you are taking. Some actions may take several Symantec Endpoint Protection Manager heartbeat intervals to complete. You can view the status of the commands that you executed in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

Events

Columns in the Events table show the node for the entity that contributed to the incident, when the event was first detected by ATP or Symantec Endpoint Protection Manager, and a description of the event. ATP also provides the host name or IP address of the computer (Affected Endpoint) involved in the event and domain or IP address (External Domain) that it communicated with. Click on any file, domain, or endpoint hyperlink (in blue) to open that entity's details page.

See [“About Events”](#) on page 100.

See [“About the Incident Manager”](#) on page 77.

See [“How ATP creates and prioritizes incidents”](#) on page 36.

See [“About File details”](#) on page 88.

See [“About Endpoint details”](#) on page 84.

See [“About Domain details”](#) on page 97.

About Endpoint details

Endpoint details provide information about the activity that ATP detected on this endpoint and its relationship to other affected entities. You can also perform containment from this page.

Navigate to the Endpoint details page in any of the following ways:

- On the ATP Manager navigation pane, click **Incident Manager**. In the Incident Manager, click on any incident to open the **Incident Details** page.
 - On the Incident details page in the Incident graph, right-click on the endpoint node and select **Go to details**.
 - On the Incident details page in the Events table, click on any endpoint hyperlink (in blue) to open its Endpoint details page.
- Click on the interactive endpoint node anywhere it appears in the ATP Manager to open that endpoint's details page.




See [“Delving through ATP Manager to investigate threats”](#) on page 17.

Click any of the following links to learn more about that section of the Endpoint details page.

[Summary](#) | [Actions](#) | [Related endpoint activity](#)

Summary

Beneath the name of the endpoint is a graphic that depicts the health of the endpoint.

		
Healthy	At Risk	Critical
The endpoint has not been involved in any recent incidents.	The endpoint is part of a low priority or medium priority incident that is less than 7 days old and is still open.	The endpoint is part of a high priority incident that is less than 7 days old and is still open.

The summary also provides the following information about the endpoint:

HOST NAME	The host name or, if unavailable, the IP address of the endpoint. ATP gathers endpoint information about Symantec Endpoint Protection endpoints from Symantec Endpoint Protection Manager. If you have the network control point, ATP also scans your network traffic. As such, ATP can detect events on unmonitored endpoints as traffic passes through the scanner. In these instances, ATP can only provide the host name or IP address. Since ATP does not have Symantec Endpoint Protection agent's information, it is unable to provide the user name, 64-bit, last check-in, or Symantec Endpoint Protection Manager group.
LAST IP ADDRESS	The last IP address for this endpoint that Symantec Endpoint Protection reported.
ATP LAST SEEN TIME	The last date and time that the endpoint checked in with Symantec Endpoint Protection Manager.
HOST DOMAIN / WORKGROUP INFO	This information only appears if Symantec Endpoint Protection collects the endpoint information.
MAC ADDRESS	The MAC address of the endpoint.
SEPM GROUP	The Symantec Endpoint Protection Manager group to which this endpoint belongs.
USER NAME	If available, the most recent user's name.
OPERATING SYSTEM	The endpoint's operating system.
64-BIT	Whether the endpoint is a 64-bit computer.

Actions

Isolate | Rejoin

When you isolate an endpoint, you cut off the connections that the endpoint has to internal networks and external networks. Isolating an endpoint keeps that computer from infecting any other computers. If the endpoint has already been isolated, the option **Rejoin** appears on the Actions bar so that you can remove it from isolation and re-establish network connections. ATP supports isolating endpoints on Symantec Endpoint Protection 12.1 RU6 and later.

See [“Isolating breached endpoints”](#) on page 48.

Only users with the Admin role or Controller role can perform actions. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

Note: To isolate and rejoin endpoints from the ATP Manager, you must have a Quarantine Firewall policy in Symantec Endpoint Protection Manager and assigned it to a Host Integrity policy. This requirement is necessary to ensure that the endpoint is put into/taken out of quarantine in the event that your Host Integrity policy FAILS, regardless of what the THEN clause states. Click the following link to learn more about how to create Symantec Endpoint Protection Manager Host Integrity policies:

<http://www.symantec.com/docs/HOWTO101742>

The time it takes for an action to complete depends on the action that you take. Some actions may take several Symantec Endpoint Protection Manager heartbeat intervals to complete. You can view the status of the commands that you executed in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

Related endpoint activity

The following describes the additional details about the endpoint. If more than five rows exist in a section, click {n} Total to view the entire list. Click on any hyperlink (in blue) to go to its entity details page.

Related Incidents

Other incidents in which this endpoint is associated. Click on a row to open that incident's details page.

Tip: You might want to evaluate other related incidents to see if they require similar remediation.

See [“About Incident details”](#) on page 79.

Related Events	<p>All of the events that ATP detected that are related to this entity. Upon investigation, related events may share multiple characteristics.</p> <p>Tip: You might want to evaluate other related events to see if they require similar remediation.</p> <p>See “About Events” on page 100.</p>
Malicious Files	<p>All of the convicted files based on network events, endpoint events, and Insight that originated from the endpoint. ATP shows the file name, path, certificate, and whether the file was blocked by ATP, Symantec Endpoint Protection, or not blocked. Click on a row to open that file's details page.</p> <p>When SONAR detects system changes on this endpoint relating to a file and the behavior is malicious, a Behavior option appears in the row for that file. Click the Behavior option to open the Process Behavior details page to view information about the system changes that occurred.</p> <p>See “About Process Behavior details” on page 94.</p> <p>Note: To view static file attributes (attributes that apply to a file regardless of any process behavior), go to the File details page and click the Attributes tab. See “About File details” on page 88.</p>
Malicious Connections	<p>Connections that left the endpoint and are deemed malicious (such as malware phone-home activity). This information also includes the Vantage detection evaluation. Click on a row to open that domain's details page.</p> <p>See “About Domain details” on page 97.</p>
Artifacts found in Endpoint Search	<p>The artifacts that were found in the most recent endpoint search. If no search has been conducted on this endpoint, this table is empty.</p> <p>See “Searching Symantec Endpoint Protection endpoints for IOCs” on page 22.</p>

Troubleshooting

See [Multiple endpoints appear in ATP for the same host/IP address](#).

About File details

File details provide information about the activity that ATP detected occurred with this file or email and its relationship with other entities in your environment. You can also perform remediation tasks from this page.

Navigate to the File details page in any of the following ways:

- On the ATP Manager navigation pane, click **Incident Manager**. In the Incident Manager, click on any incident to open the **Incident Details** page.
 - On the Incident details page in the Incident graph, right-click on the file node and select **Go to details**.
 - On the Incident details page in the Events table, click on any file hyperlink (in blue) to open its File details page.
- Click on the interactive file node anywhere it appears in the ATP Manager to open that File's details page.

See “[Delving through ATP Manager to investigate threats](#)” on page 17.

Click any of the following links to learn more about that section of the File details page.

[Summary](#) | [Actions](#) | [Details](#) | [Attributes](#)

Summary

Beneath the name of the file is a graphic that depicts the health of the file.



Good

The file is whitelisted or Symantec's reputation service indicates that the file is good.



Suspicious

The file is suspicious. Machine learning is used to identify the files that are likely to be malicious.



Bad

The file is blacklisted on ATP, Symantec Endpoint Protection has blocked the file, or a Symantec technology deems it to be malicious.

Beneath the graphic is the following information:

DISPOSITION

ATP's evaluation of the file.

AV SIGNATURE NAME	The antivirus signature that detected the file is suspicious or malicious.
TARGETED ATTACK	Whether ATP deems this file to be a part of a targeted attack on your organization.

To the right of the graphic is the following information:

SHA256	The file's 256-bit secure hash value. Click on this field to see the full hash value.
MD5	The MD5 hash that is associated with this file's SHA256 hash.
CERTIFICATE	The signor of the file certificate, if the file has been signed.
FILE TYPE	File type is the true file type, which may not necessarily match the file extension.

File Overview

RELATED EVENTS	<p>The number of events that are related to this file.</p> <p>To see a list of all of the related events that are associated with this file, see Related Events in the Details table.</p>
RELATED INCIDENTS	<p>The number of incidents that are related to this file.</p> <p>To see a list of all of the related incidents that are associated with this file, see Related Incidents in the Details table.</p>
EMAIL DETECTIONS	The number of emails that have this file as an attachment.
CYNIC MODIFICATIONS	<p>The number of file modifications that Cynic detects.</p> <p>When a file is submitted to Cynic, Cynic detonates the file in a sandbox. It then analyzes the results for the file modifications that are made.</p>
EXTERNAL DOMAINS ACCESSED	The number of external computers that the file has communicated with.

Global Reputation

FIRST SEEN	The first time that Insight saw this file worldwide.
PREVALENCE	The number of times a file reputation request has been made on this file worldwide.

Local Reputation

FIRST SEEN	The first time this file has been seen in your network.
------------	---

PREVALENCE	<p>The number of endpoints in your environment that have this file.</p> <p>To see a list of all of the endpoints that have this file, see Seen on Endpoints in the Details table.</p>
------------	--

Actions

The actions that you can perform on the File details page are as follows:

Add to Blacklist Revoke Blacklist	<p>Adds the file to or removes this file from your Blacklist.</p> <p>See "Remediating malicious files" on page 49.</p>
Add to Whitelist Revoke Whitelist	<p>Adds the file to or removes this file from your Whitelist.</p> <p>See "Managing policies" on page 61.</p> <p>See "Reporting false positive and false negative file convictions" on page 53.</p>

Submit to Cynic

Submits unknown files to Symantec (files not already recognized by Symantec as having a good reputation or a bad reputation) for analysis. Cynic detects unknown malware and advanced threats by executing files in virtual sandbox environments.

Only the files that are found by the endpoint control point can be submitted to Cynic. Files that are identified by the network control point or email control point cannot. **Tip:** In this scenario, consider running an endpoint search to locate the file on your endpoints. Copy them to the file store and then submit them to Cynic.

See [“Searching Symantec Endpoint Protection endpoints for IOCs”](#) on page 22.

Note: This action is only supported on the clients that use Symantec Endpoint Protection 12.1 RU6 and later.

Cynic supports the following file types:

- 32- and 64-bit executable
- Compressed (e.g., ZIP)
- APK
- JAR
- PDF
- Java
- Microsoft Office documents

Submit to VirusTotal

Submits the SHA256 hash to VirusTotal, then takes you to the VirusTotal website so that you can view the results.

Copy to file store | Download from file store

ATP stores the file in a compressed file and copies it to the ATP file store. When you copy the compressed file to the file store, you must assign a password for it. After the compressed file is copied to the file store, the option changes to let you download the compressed file to your local computer. You can open the compressed file on your local computer with the password that you assigned to it and analyze it in your own virtual environment. Or you can submit the downloaded file to Cynic.

Note: This action is only supported on the clients that use Symantec Endpoint Protection 12.1 RU6 and later.

Delete File

Deletes the selected file and the registry entries that point to that file from that endpoint.

Only the files that are found by the endpoint control point can be deleted. Files that are identified by the network control point or email control point cannot. **Tip:** In this scenario, consider running an endpoint search to locate the file on your endpoints and delete them from the Endpoint details page.

This option remains active until the file is deleted from the endpoint through Symantec Endpoint Protection Manager. Then the option becomes inert for that file.

Note: This action is only supported on the clients that use Symantec Endpoint Protection 12.1 RU6 and later.

Only users with the Admin role or Controller role can perform actions. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

The time it takes for an action to complete depends on the action that you take. Some actions may take several Symantec Endpoint Protection Manager heartbeat intervals to complete. You can view the status of the commands that you executed in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

Details

The following describes the additional information that appears on this page. If more than five rows exist in a section, click {n} Total to view the entire list. In the entire list dialog box, you can click on any hyperlink (in blue) to view its entity details page.

Related Incidents	<p>Other incidents in which this file entity is associated. Click on a row to open that incident's details page.</p> <p>Tip: You might want to evaluate other related incidents to see if they require similar remediation.</p> <p>See "About Incident details" on page 79.</p>
Related Events	<p>All of the events that ATP detected that are related to this entity. Upon investigation, related events may share multiple characteristics.</p> <p>Tip: You might want to evaluate other related events to see if they require similar remediation.</p> <p>See "About Events" on page 100.</p>
Seen on Endpoints	<p>All of the endpoints in your environment that contain this file. Click on a row to open that endpoint's details page.</p> <p>See "About Endpoint details" on page 84.</p> <p>When SONAR detects system changes on an endpoint relating to this file, a Behavior option appears in the row for the affected endpoint. Click the Behavior option to open the Process Behavior details page to view information about the system changes that occurred and their related attributes.</p> <p>See "About Process Behavior details" on page 94.</p>
File Download Origins	<p>The domain from which this file was downloaded. Click on a row to open that domain's details page.</p> <p>See "About Domain details" on page 97.</p>
File Instances	<p>Other instances of the SHA256 hash in your environment. If the malware polymorphed itself under different names, the different names appear in this row too. This row also shows whether the file was blocked by ATP, Symantec Endpoint Protection, or not blocked.</p>
Cynic Observed File, Registry, System Changes	<p>The Cynic results that were found for that particular file. Entries only appear if the file has been submitted to Cynic for analysis.</p> <p>Click on an item to show that file's details page.</p>

Cynic Observed Network Analysis Network connections that occurred during Cynic analysis (such as phone home attempts). Entries only appear if the file has been submitted to Cynic for analysis.

Click on a row to open that domain's details page.

See [“About Domain details”](#) on page 97.

Attributes

When SONAR detects system changes on an endpoint relating to this file, an **Attributes** tab appears on the File details page. The **Attributes** tab provides detailed information about that file's attributes (to the extent that this information is available). These attributes ("static file attributes") are the attributes that apply to a file and do not change regardless of what processes occur. Examples of file attributes are: file image size; the number of strings in a file's resource; that the file has a digital signature.

You view static file attributes on the File details page on the **Attributes** tab. ATP provides a description of the attributes and their values. Attributes are grouped as follows:

- Count of resources
- Imported functions
- Advanced file attributes

ATP lets you filter attributes so that you can narrow the results. Click **Show Filters** to reveal the filters. Select the attributes that you want to filter by. (Results immediately begin to appear.) Click **Hide Filters** to hide the filters view. ATP maintains your filter selections until you reset the filter criteria or refresh the page.

Note: To view a sequential list of the system changes that occurred on the endpoint, on the **Details** tab under **Seen on Endpoint**, click the **Behavior** option. The **Process Behavior** details page for that endpoint/file relationship appears.

See [“About Process Behavior details”](#) on page 94.

About Process Behavior details

Process Behavior details provide information about the file-executed system changes that occurred on an endpoint in sequential order. ATP also provides the attributes that are associated with each system change.

See [“About analyzing the process behaviors that occurred on endpoints”](#) on page 38.

A Process Behavior details page is only available when a process occurs on an endpoint and one or more events in the process are malicious. You can navigate to the Process Behavior details page in either of the following ways:

- From the Endpoint details page
A **Behavior** option appears in the **Malicious Files** row for the file that was involved in the process.
See [“About File details”](#) on page 88.
- From the File details page
A **Behavior** option appears in the **Seen on Endpoints** row for the endpoint on which the process behavior occurred.
See [“About Endpoint details”](#) on page 84.

See [“Delving through ATP Manager to investigate threats”](#) on page 17.

To the right of the graphic is the following information:

SHA256	The file's 256-bit secure hash value. Hover over this field to see the full hash value.
FILE NAME	The name of the file as it appears on the host computer.
MD5	The MD5 hash that is associated with this file's SHA256 hash.
HOST NAME	The host name of computer on which this file resides.
LAST IP ADDRESS	The last IP address for the endpoint that Symantec Endpoint Protection reported.

Process Behavior

A process is represented by a group of system changes. Each process has a separate date/time range. ATP shows the processes that were executed on the endpoint in sequential order. To view the attributes that are associated with the system change (the dynamic file attributes), click the down arrow to the right of the row. The dynamic file attribute data that appears is unique to that process. Different processes contain different attributes, depending the information that is available to ATP. To collapse the details, click the up arrow at the far right of the row.

ATP lets you filter processes so that you can narrow the list. Click **Show Filters** to reveal the filters. Select the process that you want to filter by. (Results immediately begin to appear.) Click **Hide Filters** to hide the filters view. ATP maintains your filter selections until you reset the filter criteria or refresh the page.

The Process Behavior table contains the following information:

Type Processes are grouped by the following types:

- Registry
- File
- Internet Explorer
- Windows Settings
- Process
- Loadpoint

Description The process description is written as follows:

<Actor> <Action> <Target>

where *<Actor>* is the object that is taking the action. This could be a file or a process. *<Action>* is the task that the actor is performing. Actions include: created, deleted, renamed, updated, disabled, loaded, executed, initiated, and modified. And *<Target>* is the object that has been acted upon.

Date The date and time of the event in UTC.

The following is an example of a process behavior as it would appear in the ATP Manager:

Type	Description	Date
Windows Settings	socar.exe modified firewall-authorized applications	2016-4-1 03:00 00:45 UTC
Process	socar.exe executed keylogger functions	2016-4-1 03:00 00:45 UTC
File	socar.exe created trustme.doc	2016-4-1 03:00 00:45 UTC

In this example, the first thing the file did was add an application to the firewall's allow list. This behavior can indicate that the application is malicious and attempting to bypass firewall blacklist policies. Next, the file executed a keylogger function, which monitors and logs users' keystrokes. And lastly, it created a new file called trustme.doc. For any of these events, you can click the down-arrow and view the associated dynamic file attributes to learn more.

Note: View static file attributes for this file (attributes that apply to the file regardless of any process behavior) on the File details page on the **Attributes** tab.

See [“About File details”](#) on page 88.

About Domain details

Domain details provide the information that you need to evaluate the external computer that might have been involved in a security incident and describes its relationship to other entities in your environment.

Navigate to the Domain details page in any of the following ways:

- On the ATP Manager navigation pane, click **Incident Manager**. In the Incident Manager, click on any incident to open the **Incident Details** page.
 - On the Incident details page in the Incident graph, right-click on the Domain node and select **Go to details**.
 - On the Incident details page in the Events table, click on any domain hyperlink (in blue) to open its Domain details page.
- Click on the interactive domain node anywhere it appears in the ATP Manager to open that Domain's details page.

See [“Delving through ATP Manager to investigate threats”](#) on page 17.

Click any of the following links to learn more about that section of the Domain details page.

[Summary](#) | [Actions](#) | [Related Domain activity](#)

Summary

The name that appears is the domain name (if available), URL, or the IP address of the external computer that is involved in the incident. The graphic beneath the endpoint name provides a visual depiction of the health of that domain.



Healthy

The domain or IP address is whitelisted.



At Risk

Malicious activity was detected from the domain or IP address more than a week ago. However, no malicious activity has been detected recently.



Critical

Malicious activity was detected from the domain or IP address within the last 24 hours.

Beneath the entity graphic is the following domain information based on DeepSight Intelligence scores:

REPUTATION	<p>The domain's reputation score.</p> <p>Values range from 1-10, with 10 being the worst reputation.</p>
HOSTILITY	<p>The hostility score is calculated based on the frequency of activity.</p> <p>Values range from 1-5, with 5 being the most malicious.</p>
CONFIDENCE	<p>Symantec's confidence in the information's validity.</p> <p>Values range from 1 - 5, with 5 being the highest confidence.</p>
BEHAVIOR	<p>The domain's behavior as observed by DeepSight. Behaviors include: Attack, Command and Control, Fraud, Phishing, and URL Malware.</p>

The summary details also provide the following information about the domain:

FIRST ACCESSED INTERNALLY	<p>The first time an endpoint in your environment accessed this external computer.</p>
LAST ACCESSED INTERNALLY	<p>The last time an endpoint in your environment accessed this external computer.</p>
ENDPOINTS THAT ACCESSED DOMAIN	<p>The number of endpoints in your environment that accessed this external computer. To see a list of all the endpoints that access this external computer, see Endpoints that Communicated with this External Machine in the Details table.</p>
NUMBER OF FILE DOWNLOADS	<p>The number of files that were downloaded from this external computer. To see a list of all the files that were downloaded from this external computer, see Files Downloaded in the Details table.</p>
LAST IP ASSOCIATED WITH DOMAIN	<p>The address of the last IP that was created that is associated with the site.</p> <p>An external computer can have many IP addresses associated with it. This field indicates the last IP address that was created.</p> <p>Tip: An IP address that has been very recently created may be suspicious.</p>

DeepSight Intelligence

CREATED DATE	<p>The date the domain was originally registered.</p>
UPDATED DATE	<p>The date the domain registration was last updated.</p>

PERSON	The organization that registered the domain and the administrator.
ORGANIZATION	The organization that registered the domain.
CITY	The city of the organization that registered the domain.
COUNTRY	The country of the organization that registered the domain.

Actions

You can take the following actions on external computers:

- Add to Whitelist | Revoke Whitelist
- Add to Blacklist | Revoke Blacklist

Only users with the Admin role or Controller role can perform actions. Actions that are not permitted based on your role appear in the ATP Manager as inactive.

The time it takes for an action to complete depends on the action that you are taking. Some actions may take several Symantec Endpoint Protection Manager heartbeat intervals to complete. You can view the status of the commands that you executed in the Action Manager.

See [“Checking the status of an action”](#) on page 62.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

See [“About policies”](#) on page 56.

See [“Managing policies”](#) on page 61.

Related Domain activity

The following describes the additional information that appears on this page. If more than five rows exist in a section, click {n} Total to view the entire list. In the entire list dialog box, you can click on any entity to view its entity details page.

Related Incidents	<p>Other incidents in which this external computer is associated. Click on a row to open that incident's details page.</p> <p>Tip: You might want to evaluate other related incidents to see if they require similar remediation.</p> <p>See “About Incident details” on page 79.</p>
Files Downloaded	<p>Files that were downloaded from the external computer and the endpoint it was downloaded on. This list includes files intentionally downloaded and drive-by downloads. Click on any hyperlink (in blue) to show that file's details page.</p> <p>See “About File details” on page 88.</p>

Endpoints that
Communicated with this
External Domain

Other endpoints in your organization that have visited this external computer. Click on a row to open that endpoint's details page.

Tip: If you have concerns that these endpoints could infect your network, consider isolating these endpoints until you can remediate them or re-image them.

See [“About Endpoint details”](#) on page 84.

See [“About Domain details”](#) on page 97.

Emails Associated with this
Domain

Emails that were sent from this domain.

IPs Associated with this
Domain

The list of all of the IP addresses that have been associated with the external computer. Click on a row to open that external computer's details page.

Tip: You might want to blacklist these IP addresses if you deem them suspicious.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

Malicious URLs Associated
with this Domain

The list of all of the URLs that are associated with the external computer. Click on a row to open that external computer's details page.

Tip: You might want to blacklist these URLs if you deem them suspicious.

See [“Blacklisting suspicious domains, URLs, and IP addresses”](#) on page 54.

About Events

The Events page lists every event that ATP detects, whether or not the event is considered part of an incident.

See [“About events, incidents, and entities”](#) on page 14.

On the ATP Manager navigation pane, click **Events** to navigate to the Events page.



Click on any of the following links to learn more about that section of the Events page.

[Events Over Time Histogram](#) | [Events table](#)

Events Over Time Histogram

The Events Over Time histogram lets you view the number of events that occurred over a set period of time. Hover your mouse over a date to see the number of events that occurred on that date.

To change the histogram time frame, under Events Over Time, click one of the pre-set time ranges (the last 7 days, last month, last 3 months, or all events).

Events table

The Events table lists events in the order that they occurred with the most recent event first. Each row reflects when the event was detected or blocked by ATP or Symantec Endpoint Protection, and it contains a brief description of the event. The Internal column provides the endpoint in your organization that was affected. And the External column provides the external computer (e.g., domain, IP address, or URL) involved in the event (if any). Click on hyperlinks (in blue) to open that entity's details page for more information.

ATP lets you filter events so that you can view just the events that you want to see. Click **Show Filters** to reveal the filters. Select the events that you want to filter by. (Results immediately begin to appear.) You can click **Clear all** to uncheck all of the filter boxes. Click **Reset all filters** to reset your filter criteria to the default (all boxes selected). Click **Hide Filters** to hide the filters view. ATP maintains your filter selections until you reset the filter criteria or refresh the page.

See [“The types of events that ATP detects”](#) on page 33.

To search events, specify the event criteria in the box beside the filter and click the magnifying glass. ATP lets you combine filtering and search to further narrow search results.

See [“About File details”](#) on page 88.

See [“About Endpoint details”](#) on page 84.

See [“About Domain details”](#) on page 97.

See [“About Incident details”](#) on page 79.

Index

A

Action Manager 62

actions

- blacklisting 82, 90, 99
- closing incident 83
- commenting 83
- copying to file store 92
- deleting file 82–83, 92
- downloading from file store 92
- isolating endpoint 82, 86
- performing from Incident details 82
- performing from Incident graph 82
- performing on domains 99
- performing on endpoints 86
- performing on files 90
- rejoining endpoint 82, 86
- revoking blacklist 90, 99
- revoking whitelist 90, 99
- submitting to VirusTotal 91
- viewing in Action Manager 62
- whitelisting 82, 90, 99

antivirus 10, 33

ATP

- about 9
- creating and prioritizing incidents 36
- cybersecurity core functions 11

B

best practices, recovery 65

Blacklist 10, 33, 56, 60–61

C

control point 9, 12, 16, 55, 85, 91–92

cybersecurity 11

Cynic 10, 33, 50, 89, 91

D

Dashboard 17

Email Event Activity 45

Endpoint Event Activity 43

Dashboard *(continued)*

Endpoints 46

Event Activity widget 40

Network Event Activity 41

New and Unknown Threats 46

details

domain 97

endpoint 84

file 88

incident 35, 79

process behavior 94

disaster and recovery planning 11

domain

actions 99

blacklisting 54, 61

entity node 97

whitelisting 54, 61

E

email 12, 19, 88–89, 91–92, 100–101

endpoint

actions 86

entity node 84

isolating 48

process behavior 87

troubleshooting 87

Endpoint Detection and Response (EDR) 9

entity

about 15

details 35

domain 15, 97

endpoint 15, 84

file 15, 88

health 81

entity node

about 81

domain 97

endpoint 84

file 88

events 14, 16, 31, 33, 100

external computer. *See* domain

F

false negatives 53
 false positives 53
 See also file
 See also Whitelist
 file 53
 See also false negatives
 See also false positives
 actions 90
 blacklisting 49, 61
 copying to file store 49
 deleting 49
 details 88
 downloading from file store 49
 dynamic attributes 38, 94
 email 88
 entity node 88
 remediating 49
 static attributes 39, 94
 submitting to Cynic 49
 submitting to VirusTotal 49
 whitelisting 49, 61
 file hash. *See* MD5. *See* SHA256

H

Host Integrity policy 48, 83, 86

I

Incident graph
 about 81
 navigating 82
 performing actions from 82
 Incident Manager 17, 35, 77
 incidents
 about 14
 analyzing 34
 details 79
 priority 36, 79
 rules 37
 viewing in Incident Manager 77
 indicator of compromise. *See* IOC
 inline block mode 12
 Insight 10, 33
 IOC 16, 18, 20, 22–23
 isolate 48, 82, 86

M

MD5 89

Mobile Insight 10, 33

N

NIST (National Institute of Standards and Technology) 11
 notification 17

O

operators
 conditional 29
 logical 30
 using in search expressions 24

P

policies
 Blacklist 56
 managing Blacklist 61
 managing Whitelist 61
 supported match values 60
 Whitelist 56, 58
 process behaviors 36, 38, 87, 93–94
 See also endpoint
 See also file
 See also file: dynamic attributes
 See also file: static attributes

Q

quarantine. *See* isolate
 Quarantine Firewall policy 48, 83, 86
 See also Symantec Endpoint Protection

R

rejoin 48, 82, 86
 See also isolate
 reports
 about 66
 deleting 72
 Domains Showing Threat Behavior 66, 75
 downloading 72
 Executive Report 66, 75
 High and Medium Open Incidents 66, 75
 Recently Infected Endpoints 66, 75
 schedules
 deleting 72
 viewing 72
 scheduling 69
 viewing 72

S

SafeWeb 37

search

- about 16, 18, 23

- database 18, 20, 23

- endpoint 18, 22–23

- STIX 20

- writing expressions 23

SEP. *See* Symantec Endpoint Protection

SHA256 89

SIEM (security information and event management) 12, 17

SONAR 11, 38, 94

STIX 20

Structured Threat Information Expression file. *See* STIX

Symantec Advanced Threat Protection. *See* ATP

Symantec Email Security.cloud 9

Symantec Endpoint Protection 9, 20, 27–31, 48

Symantec Online Network for Advance Response. *See* SONAR

Synapse 10, 12

syslog 17

T

threat 15

- See also* events

- See also* incidents

token

- using in search expressions 24

V

value 24

Vantage 10, 33, 36

VirusTotal 49–50, 91

W

Whitelist 10, 58, 60–61

wildcards 27

Glossary

all-in-one	<p>A configuration in which the appliance performs all system functions: acting as a management server, scanning network traffic, and EDR (Endpoint Detection and Response) functionality.</p> <p>See also: EDR.</p>
antivirus	<p>Software that is used to detect malicious computer applications, prevent them from infecting a system, and clean files or applications that are infected with computer viruses.</p>
artifact	<p>Any item that can be detected in your environment that may be an indicator of compromise (for example, a file hash).</p> <p>See also: indicator of compromise.</p>
Blacklist (noun)	<p>A list of domains, IP addresses, URLs, or files to which access is automatically blocked.</p> <p>See also: blacklist (verb) and Whitelist.</p>
blacklist (verb)	<p>The act of adding domains, IP addresses, URLs, or files to the ATP Blacklist.</p> <p>See also: Blacklist and Whitelist.</p>
client	<p>A computer that has Symantec Endpoint Protection installed on it.</p> <p>See also: controlled endpoint, endpoint, and managed endpoint.</p>
closed incident	<p>An incident that has been investigated, remediated, and requires no further action.</p> <p>See also: open incident.</p>
controlled endpoint	<p>Endpoints that have Symantec Endpoint Protection installed.</p> <p>See also: client, endpoint, and managed endpoint.</p>
control point	<p>The items that ATP monitors and can take actions on, consisting of: network, endpoint, and email.</p> <p>See also: Symantec Endpoint Protection and Symantec Email Security.cloud.</p>
Cynic™	<p>A Symantec technology that examines files in a cloud-based sandbox environment, analyzes, and reports each step of the behavior. Cynic uses machine-learning technology to compare the results to known bad attributes. It then correlates your data with real-world data provided by the Symantec Global Intelligence Network to determine if the files are malicious.</p> <p>See also: Global Intelligence Network.</p>

DeepSight™ Intelligence	A Symantec technology that uses a global warning threat detection system to aggregate threat information into a central database.
dynamic file attributes	The file attributes related to a specific process on an endpoint, which may differ from endpoint to endpoint.
EDR (Endpoint Detection and Response)	A category of tools and solutions that focus on detecting and investigating suspicious activities and issues on endpoints. See also: endpoint.
endpoint	A computer or device at the termination or origination of network traffic. Devices can include laptops, desktop computers, mobile devices, and servers. See also: client, controlled endpoint, and managed endpoint.
enterprise proxy	The proxy server in your network that connects to the Internet. When ATP is located on the internal network behind the enterprise proxy server, communication from protected endpoints to the proxy server is considered internal communication. ATP does not monitor that internal communication. You specify the enterprise proxy in your ATP configuration so that traffic between internal clients and the enterprise proxy server is inspected. See also: client, endpoint, and internal network.
entity	An artifact that ATP monitors and can take actions on. Entities include: endpoint, domain, or file.
event	A record of activity, such as a malicious file is downloaded or a benign executable file is created. See also: incident.
external computer	Any computer or server that is not part of your internal network. See also: internal network.
external network	Any computers, IP addresses, and devices that are not part of your internal network and are not considered protected assets. See also: internal network.
Global Intelligence Network	A Symantec technology that has global visibility into the threat landscape through big data that is accumulated from one of the largest collection of sensors in the industry, an extensive anti-fraud community of enterprises and security vendors, and more than 8 billion emails per month from 5 million decoy accounts. The Global Intelligence Network provides proactive protection to Symantec products, including the DeepSight Intelligence. See also: DeepSight Intelligence.
iDRAC (integrated Dell Remote Access Controller)	A device that is shipped with the ATP physical appliance that provides console access to the appliance. The iDRAC, though integrated, is a separate device that requires its own network address to function.

incident	<p>A collection of one or more events that ATP considers important enough to highlight to an incident responder.</p> <p>See also: event.</p>
Incident graph	<p>An interactive graph that appears on the Incident details page that shows the entities that are involved in an incident and their relationship to one another. It also visually depicts the health of the entities and any actions that are taken on entities (such as being isolated).</p> <p>See also: incident and entity.</p>
indicator of compromise (IOC)	<p>Artifacts that are observed on a network that might indicate a security breach. Examples of IOCs include IP addresses, file hashes, and URLs.</p>
inline block mode	<p>An installation configuration for the network scanner in which network traffic passes through the appliance between the endpoints and the Internet. ATP blocks file downloads, websites, and the traffic that it considers malicious.</p> <p>Note: This mode is only supported in ATP 2.0.2 and later.</p> <p>See also: endpoint, inline monitor mode, and tap mode.</p>
inline monitor mode	<p>An installation configuration for the network scanner in which network traffic passes through the appliance between the endpoints and the Internet. Malicious files, websites, and traffic are logged for visibility but are not blocked.</p> <p>Note: This mode is only supported in ATP 2.0.2 and later.</p> <p>See also: inline block mode, and tap mode.</p>
Insight	<p>A Symantec reputation database that has reputation intelligence on over 8 billion files. Insight is the world's largest reputation request service for Insight reputation queries. This service gathers information about Windows executable files.</p> <p>See also: Mobile Insight.</p>
internal network	<p>A group of computers, IP ranges, and devices within your organization that are connected by communications facilities (both hardware and software) and represent your protected assets. ATP does not scan traffic between protected assets on your internal network.</p> <p>See also: external network.</p>
IOC	<p>See <i>indicator of compromise (IOC)</i>.</p>
isolate	<p>Separating a computer from internal and external networks to prevent it from infecting other computers.</p> <p>See also: rejoin.</p>
malicious	<ol style="list-style-type: none"> 1. Symantec technology deems an entity to be a threat. 2. The entity was involved in an incident less than 7 days ago. <p>See also: entity and threat.</p>

managed endpoint	<p>An endpoint that has Symantec Endpoint Protection installed.</p> <p>See also: controlled endpoint and endpoint.</p>
management platform	<p>A configuration in which the appliance hosts the ATP Manager, centralizes management functions, stores all detection incidents and convicted files, and communicates administrative actions.</p>
Mobile Insight	<p>Mobile Insight analyzes Android applications. In addition to tackling malware detection, Mobile Insight also detects privacy and performance issues in mobile apps.</p> <p>See also: Insight.</p>
network proxy	<p>The proxy server that ATP uses for communications to the Internet. For example, ATP communicates through the network proxy server to Symantec for Synapse analysis and updated virus definitions.</p> <p>See also: enterprise proxy.</p>
network scanner	<p>The scanner that monitors network traffic.</p>
new threat	<p>A threat that has been detected in the last 24 hours.</p> <p>See also: threat.</p>
open incident	<p>An incident that is newly detected or one that is still in investigation.</p>
Power Eraser	<p>A Symantec technology that eliminates deeply embedded and difficult to remove the crimeware that traditional virus scanning doesn't always detect.</p>
process behavior	<p>The system changes made by a file on an endpoint.</p> <p>See also: dynamic file attributes and static file attributes.</p>
reputation request	<p>A request that is made to a service (Insight and Mobile Insight) for information about the reputation of a file.</p> <p>See also: Insight and Mobile Insight.</p>
rejoin	<p>Returning an isolated computer to internal networks and external networks.</p> <p>See also: isolate.</p>
resource	<p>When used in ATP, references to a resource refer to an endpoint.</p> <p>See also: endpoint.</p>
rule engine	<p>A technology that determines when an incident should be created based on the severity of related events.</p> <p>See also: event and incident.</p>

SONAR (Symantec Online Network for Advanced Response)	A Symantec technology that uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on your client computers to detect emerging threats. SONAR also detects changes or behavior on your client computers that you should monitor.
static file attributes	The attributes that are related to a specific file, which are the same regardless of on which endpoint the file resides.
STIX™ (Structured Threat Information Expression)	A structured language that contains cybersecurity threat information. Typically stored in XML format, the STIX standard lets users share, store, and analyze content relating to security threats in a consistent manner.
suspicious	<ol style="list-style-type: none"> 1. A file has characteristics similar to other malicious files but was not known to be bad by Symantec or the Administrator (i.e., is not in the Blacklist). 2. An endpoint has been involved in at least one low to medium priority incident over the last 7 days. 3. A domain has appeared in the DeepSight Intelligence feed in the last 24 hours to 7 days. <p>See also: threat.</p>
Symantec Email Security.cloud	<ol style="list-style-type: none"> 1. A cloud email security service that filters unwanted messages and protects on-premises and hosted mailbox services from targeted attacks. It also provides encryption and data loss prevention to protect sensitive data. 2. A solution that ATP leverages for its email control point to detect email-based threats. <p>See also: control point.</p>
Symantec Endpoint Protection	<ol style="list-style-type: none"> 1. A client-server solution that protects laptops, desktops, and servers (endpoints) in your network against malware, risks, and vulnerabilities. 2. A solution that ATP leverages to detect endpoint-based threats. <p>See also: Symantec Endpoint Protection client and Symantec Endpoint Protection Manager.</p>
Symantec Endpoint Protection client	<p>Any computer that runs Symantec Endpoint Protection and communicates with Symantec Endpoint Protection Manager.</p> <p>See also: control point, endpoint, managed endpoint, Symantec Endpoint Protection, and Symantec Endpoint Protection Manager.</p>
Symantec Endpoint Protection Manager	<ol style="list-style-type: none"> 1. The Symantec Endpoint Protection management server that communicates with Symantec Endpoint Protection clients. 2. The console that lets administrators manage Symantec Endpoint Protection clients. <p>See also: Symantec Endpoint Protection and Symantec Endpoint Protection client.</p>
Synapse™	<p>A Symantec service that correlates ATP event data between control points.</p> <p>See also: control point.</p>

tap mode	<p>A configuration mode in which the network appliance connects to a Tap or Span port on a switch. The appliance monitors a copy of the traffic between the endpoints and the Internet.</p> <p>See also: endpoint, inline block mode, and inline monitor mode.</p>
targeted attack	<p>A malicious attack that is directed at a specific organization, industry, or individual intended to (but not limited to): exploit data, steal or extort funds, covertly spy, disrupt business activities, invoke fear, provoke reaction, or make a political or social statement.</p>
threat	<p>A circumstance, event, or person with the potential to cause harm to a system or organization in the form of destruction, disclosure, modification of data, or denial of service.</p> <p>See also: event, incident.</p>
unknown threat	<p>A new threat with no known signature that has not yet been fully analyzed and whose impact is not yet fully been assessed. Also known as zero-day exploits, which are exploits in the software that attackers take advantage of before they're known and fixed.</p> <p>See also: threat and zero-day.</p>
Vantage	<p>A Symantec detection engine that finds threats in the network stream.</p>
Whitelist (noun)	<p>A list of domains, IP address, URLs, or files that are trusted. Access is automatically granted to whitelisted items regardless of reputation.</p> <p>See also: Blacklist and whitelist (verb).</p>
whitelist (verb)	<p>The act of adding domains, IP addresses, URLs, or files to the ATP Whitelist.</p> <p>See also: Blacklist and Whitelist.</p>
zero-day	<p>The day a security researcher reports the discovery of a new vulnerability to either the technology manufacturer, a security newsgroup, or both. This starts the "time to exploit clock" which tracks the number of days between the discovery of the vulnerability and the exploitation of it.</p> <p>See also: Insight and unknown threat.</p>