



What's New in DLP 15.5

Information Protection

John Gruhn, CISSP

Symantec Data Loss Prevention SME

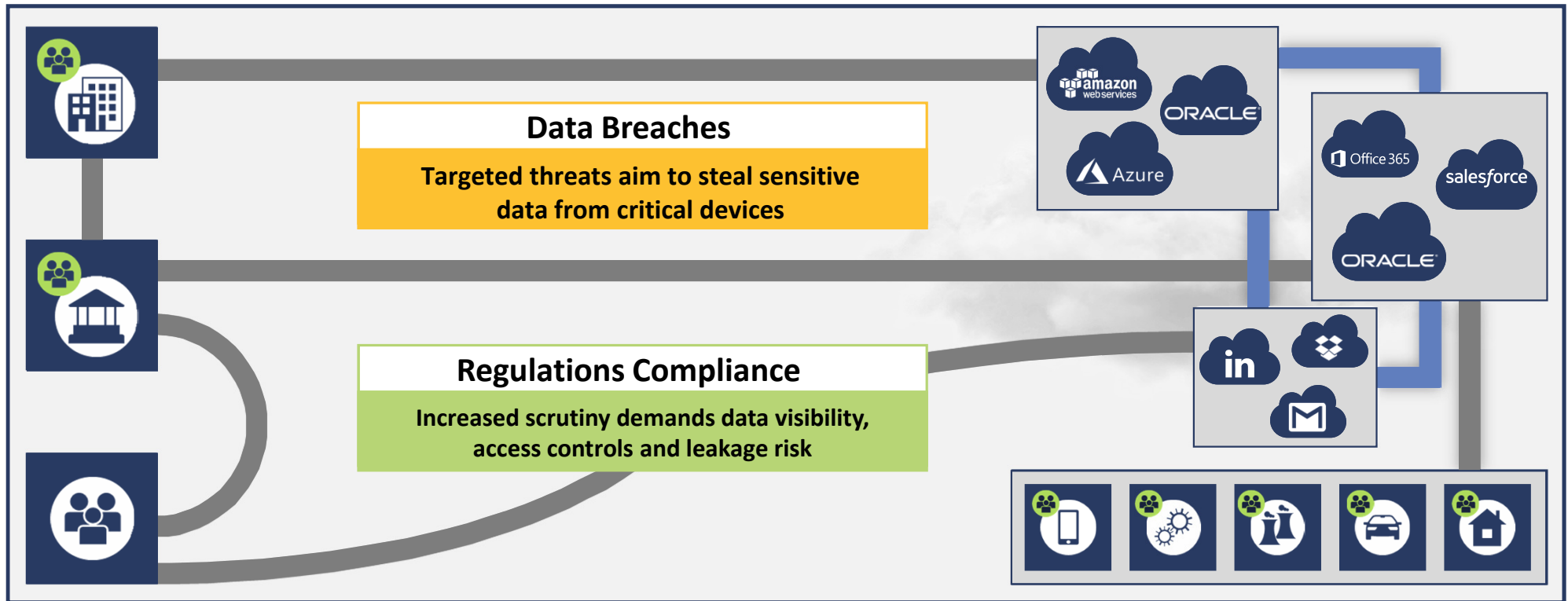
April 2019



Pressing Problems in Data Security



Changing usage models will mandate a platform architecture



From DLP to An Integrated Data Security Platform



Key products

Data Loss Prevention

Endpoint, Storage, Network, Cloud

Cloud Access Security Broker (CASB)

Digital Rights Management (ICE)

Data Classification (ICT)

User and Entity Behavior Analytics (ICA)

Identity and Access Management (VIP)

Web Gateways (ProxySG, WSS, Mobile)

Email Security, Encryption, SSLV, SEP, CCS...



Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY- LIMITED USE ONLY

Key Release Drivers for Data Loss Prevention 15.5



Issues in Data Protection



Data Breaches

How do I protect my sensitive data from malicious applications?

- Data is accessed by myriads of processes
- Critical data require threat awareness
- Not all sensitive data is protected



Regulations & Compliance

How do I ensure my sensitive data is protected on every channel?

- Data residing and flowing everywhere
- Discovery of sensitive data is difficult
- Breach risk by insiders and 3rd parties

User Story



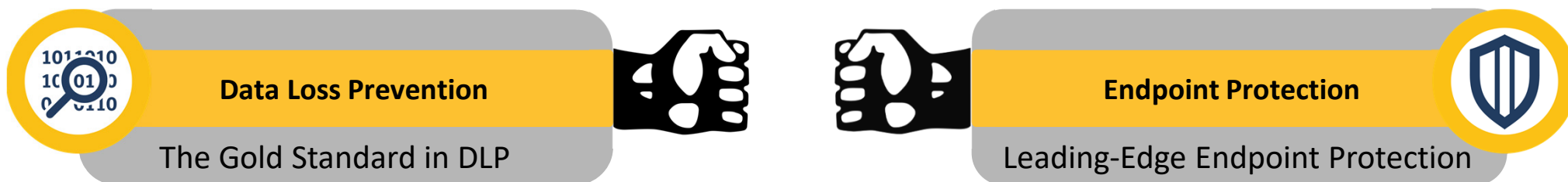
“How do I protect my sensitive data from malicious applications?”



SEP and DLP Together - The Ultimate Protection



Protecting sensitive data against cyber threats



Data Protection Based on Cyber Reputation

DLP leverages SEP application reputation to monitor applications running on endpoints that are suspicious or have unknown reputation.

DLP automatically prevents data exfiltration through those applications

Note: compatible with SEP 14.1 and newer versions

Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY- LIMITED USE ONLY

The Risk from User Installed Applications



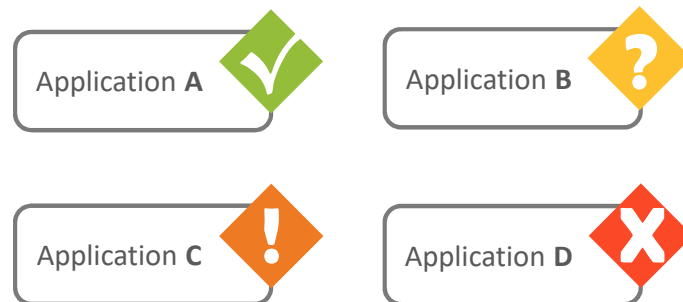
Cyber-threats lurk around the corner when untrusted apps touch sensitive data

Examples of non-corporate productivity application types that users install

- PDF mergers and splitting
- Image correction/enhancer
- Media downloading apps
- Media players
- Calculators
- Video capturing/editing tools
- Calendar
- Video/audio chatting apps
- To do lists
- File transfer apps
- Faxing

What do you trust?

The risk of data exfiltration is significant with **UNKNOWN**, **MALICIOUS** or **SUSPICIOUS** apps



Malware?

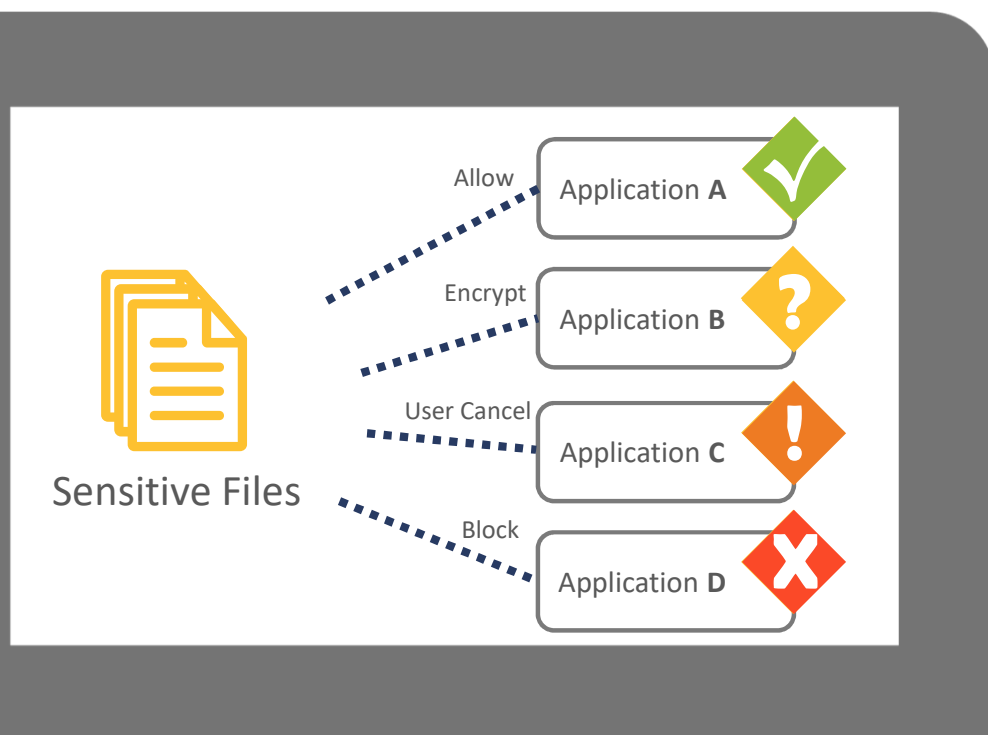
APT?

Zero Day?

How DLP-SEP Integration Works



SEP Intensive Protection delivers data exfiltration protection



- 1 A new user-installed application (UIA) is launched
- 2 DLP detects the app and sends an app info request to SEP
- 3 SEP returns a numeric risk score based on reputation
- 4 DLP maps an intensity level: **UNKNOWN-MALICIOUS-SUSPICIOUS**
- 5 DLP detects when these apps touch sensitive data
- 6 DLP applies a policy response based on reputation level

DLP Monitors Apps Using SEP Reputation



SEP Intensive Protection in DLP console

System > Agents > Agent Configuration

Save Cancel

Name * Agent 101 Configuration

Description

Channels Channel Filters Application Monitoring Device Control Settings Advanced Settings

☐ Enable different monitoring settings for endpoints located on and off the corporate network.

Enable Monitoring

Select the channels to monitor

Destinations

- ☒ Removable Storage
- ☐ CD/DVD
- ☐ Local drive
- ☒ Printer/Fax

Clipboard

- ☐ Copy
- ☐ Paste (configured applications only)

Email

- ☒ Outlook
- ☒ Lotus Notes

Configured Applications

- ☐ Application File Access
- ☒ Cloud Storage

Network Shares

- ☐ Copy to Local Drive
- ☒ Copy to Share

SEP Integration

- ☐ SEP Intensive Protection

Incident 00000035

Status: New Severity: High

SEP Intensive Protection

Key Info History Notes Correlations

Policy Matches

low-block [view policy]

r1 (Keyword Match)

Matches

2

Incident Details

Server or Detector EPS1

Agent Response Action Blocked

Occurred On 9/4/18 1:35 PM

Reported On 9/4/18 1:35 PM

Is Hidden No [Do Not Hide]

User AUTOMATIONPUNEuser1

User Education: "I did not know transferring this data was restricted."

Machine Name WIN10-PC-PK

Machine IP (Corporate) 10.210.178.232

Endpoint Location On the Corporate Network

Application forex_calculator.exe

SEP Intensity Malicious

Level

Application MD5 d399fcd5dcddeb5724ff47b7782ba72a

Hash

Application 68f6c25c9401429a87141669e52f9c88bcb45400eaf

SHA-256 Hash 9f586ad31ed5f4b564de [Open in SEP Console]

File Name test.txt

Source File Location D:\SEP_Integration\Sample\test.txt

Files

D:\SEP_Integration\Sample\test.txt

Data Owner [change]

Name [change]

Data Owner [change]

Email Address [change]

Matches (matches found in 1 component)

C:\Vendor_data\Customer_Info.docx (30 Matches):

489-36-8350 4929-3813-3266-4395 Ashley Borden 814-14-8995 5370-461

690-05-5315 4916-4811-5814-8111 Susan Davis 421-37-1396 4916-4034-92

458-02-6124 5299-1561-5689-1938 Rick Edwards 612-20-6832 5293-8502-0

300-62-3268 5248-0246-6336-5664 Lisa Garrison 660-03-8368 4579-5385-7

213-46-8918 4916-9766-5340-6147 Mark Hall 449-48-3135 4556-0072-1294

559-81-1301 4532-4220-6922-9909 Albert Iorio 322-84-2281 4916-6734-757

646-44-9061 5218-0144-2703-9266 Teresa Kaminski 465-73-5022 5399-0708

044-34-6954 5144-6691-2776-1108 Monte Mooschem 477-36-0282 5527-12

Morrison 421-90-3440 4539-0031-3703-0728 Jerome Munsch 524-02-7657 5

Nelson 205-52-0027 5413-4428-0145-0036 Lynette Oyola 887-03-2682 4532

687-05-8365 5495-8602-4508-6804 Julie Renfro 751-01-2327 5325-3256

824-84-9181 4532-0065-1968-5602 Jack Russell 514-30-2668 3453896820

451-80-3526 4716-6984-4983-6160 Mireille Townsend 404-12-2154 4539-62

505-88-5714 30204861594838 Gail Watson 461-97-5660 4532-1753-6071-11

172-32-1176 5270-4267-6450-5516 Rebecca Zwick 151-32-2558 5252-5971-

Easily enabled through Enforce console

DLP automatically prevents data exfiltration from applications with

UNKNOWN, MALICIOUS, SUSPICIOUS reputation

User Story



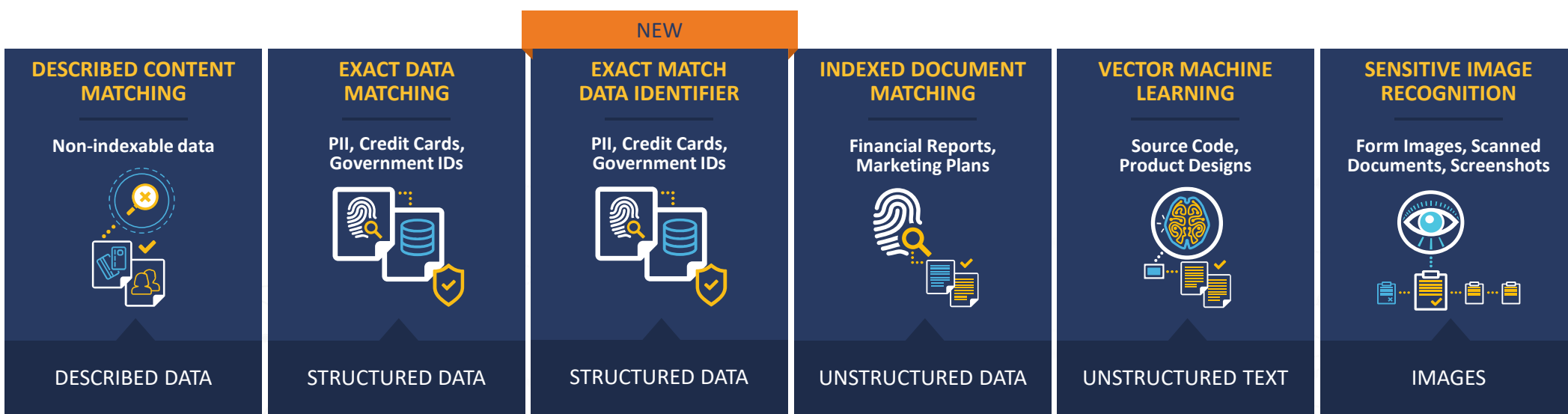
“How do I ensure my sensitive data is discovered and protected on every channel?”



Most Comprehensive Data Detection



Gives you the highest accuracy and minimizes false positives



“Symantec offers the most comprehensive sensitive data detection techniques in the market, with advanced functionality that can cover a wide breadth of data loss scenarios.”¹

¹ Source: Magic Quadrant for Data Loss Prevention, Gartner, January 2016

Exact Match Data Identifier (EMDI)



Fast, accurate detection of false positive-prone structured data

What is it?

- A new data fingerprinting technology
- Designed to work as an additional Data Identifier check against an indexed data store

Benefits

- Works on all DLP channels: detection servers, appliances, the cloud and agents
- Uses strict security to deploy profiles safely on endpoints
- Uses a much smaller memory footprint than EDM

9 Digit SSN

Direct Deposit Authorization Form
Please print and complete ALL the information below.

Name: Ariana Gates
Address: 424 Western Ave.
City, State, Zip: Redondo Beach, CA 90277
Social Security #: 476-93-3862

EXAMPLE

9 digit Routing Number: 123456789
Account Number (1-17 digits): 1234567890123456789
Check Number (do not include): 1234

Name of Bank: Bank of the South Bay
Account #: 3141592651
10-Digit Routing #: 2718281820
Amount: ☐ \$ ☐ % or ☒ Entire Paycheck
Type of Account: ☒ Checking ☐ Savings (Circle One)

Doorknob Depot LLC is hereby authorized to directly deposit my pay to the account listed above. This authorization will remain in effect until I modify or cancel it in writing.

9 Digit Invoice, Not SSN

Stefano Trading Company
INVOICE: 325333212

100 California St. Suite 1400
San Francisco, CA 94111

Bistro Nico
350 Ellis St.
Mountain View, CA 94043

BALANCE DUE
Upon Receipt
\$0.00

Notes

These are the finest quality truffles from Italy.

Item / Item Description	Qty / Hr Rate	Unit Cost	Total
White Alba Truffles - whole	100 gty.	\$120.00	\$12,000.00
		Subtotal	\$12,000.00
		Tax - 10%	\$1,200.00
		TOTAL	\$13,200.00

Exact Match Data Identifier (EMDI)



Fast, accurate detection of false positive-prone structured data

General

Rule Name: **SSN with EMDI**

Severity: **High**

Conditions

Content Matches Data Identifier

Data Identifier: US Social Security Number (SSN)

Breadth:

- ☒ **Wide** - Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
- ☐ **Medium** - Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, or periods. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
- ☐ **Narrow** - Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit. Also requires the presence of a Social Security-related keyword.

Optional Validators:

Optional Validators

Match Counting:

- ☐ Check for existence (don't count multiple matches)
- ☐ Count all matches
- ☒ **Count all unique matches**

Only report incidents with at least **1** matches

Match On:

- ☒ Envelope
- ☒ Subject
- ☒ Body
- ☒ Attachments

Also Match: **Match...** **Add**

Exact Match Data Identifier Check

Look up tokens around pattern for Exact Match Data Identifier index and validate pattern

Profile: **Customer Records**

Required: **SSN**

At least match: **1** other optional column(s)

Proximity: **50**

Match Counting:

- ☐ Check for existence (don't count multiple matches)
- ☒ Count all matches
- ☒ Count all unique matches

Only report incidents with at least **1** matches

Also Match: **Match...** **Add**

Enable EMDI in DLP Policy

Enhanced DLP Classification & Tagging



DLP Agent Reads Tags

General
Rule Name: Content is classified between Internal and Confidential

Severity
Default: High

Conditions
Content Matches Classification

☐ Content is classified
☐ Content is not classified
☒ Content matches

Is Greater Than: ACME ENG (2) Internal
OR
Is Less Than or Equal: ACME ENG (4) Confidential

Match On: ☒ Envelope ☐ Subject ☐ Body ☒ Attachments

Incident 00000016
Status: New
Severity: High

File System
Key Info History Notes Correlations

Policy Matches

Matches
Content is classified [view policy]
Content is classified (ICT)

NEW

DLP Agent Writes Tags

Symantec Data Loss Prevention Home Incidents Manage System

Manage > Policies > Response Rules > Configure Response Rule

Save Cancel

General
Rule Name:
Description:
Used in no active policies.

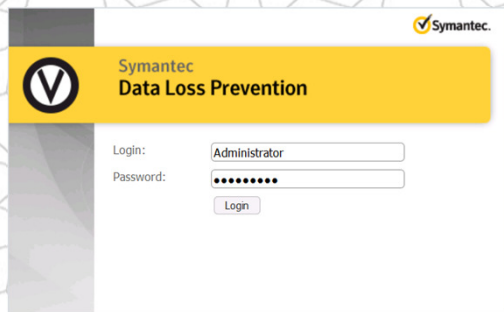
Conditions Add Condition

Actions <choose action type> Add Action

Response

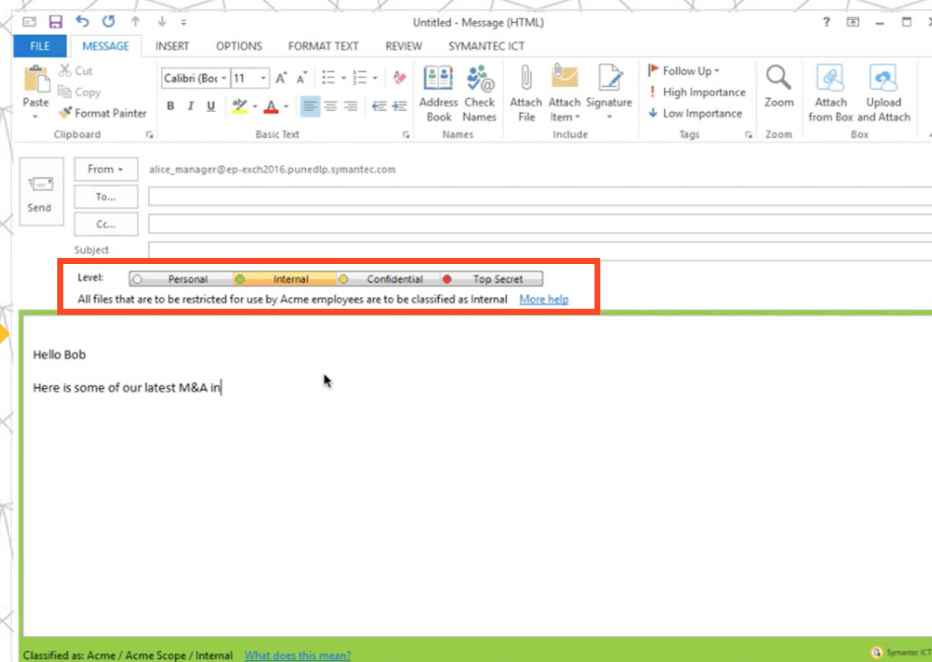
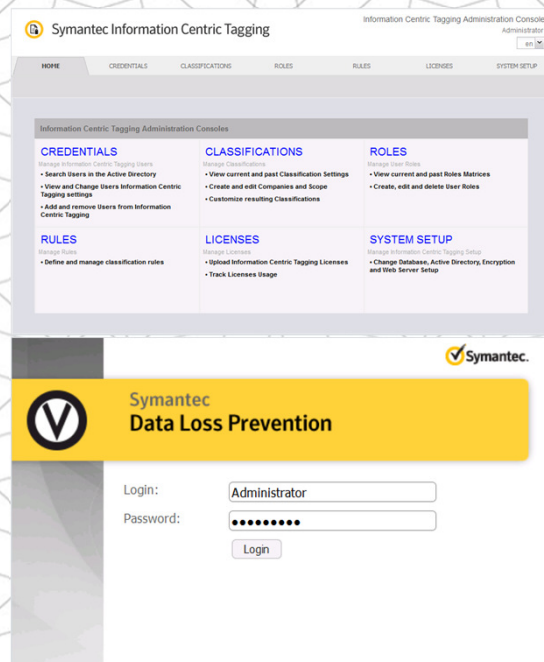
Endpoint
Discover: Quarantine File (Supported on Windows endpoints)
FlexResponse (Supported on Windows endpoints)
ICT Classification And Tagging
Information Centric Defence
Prevent: Block
Prevent: Encrypt
Prevent: Notify
Prevent: User Cancel (Supported on Windows endpoints)
Network Prevent

DLP Policy Drives Classification on Endpoints



DLP Endpoint Discover Scans and Classifies Existing Data on Endpoints

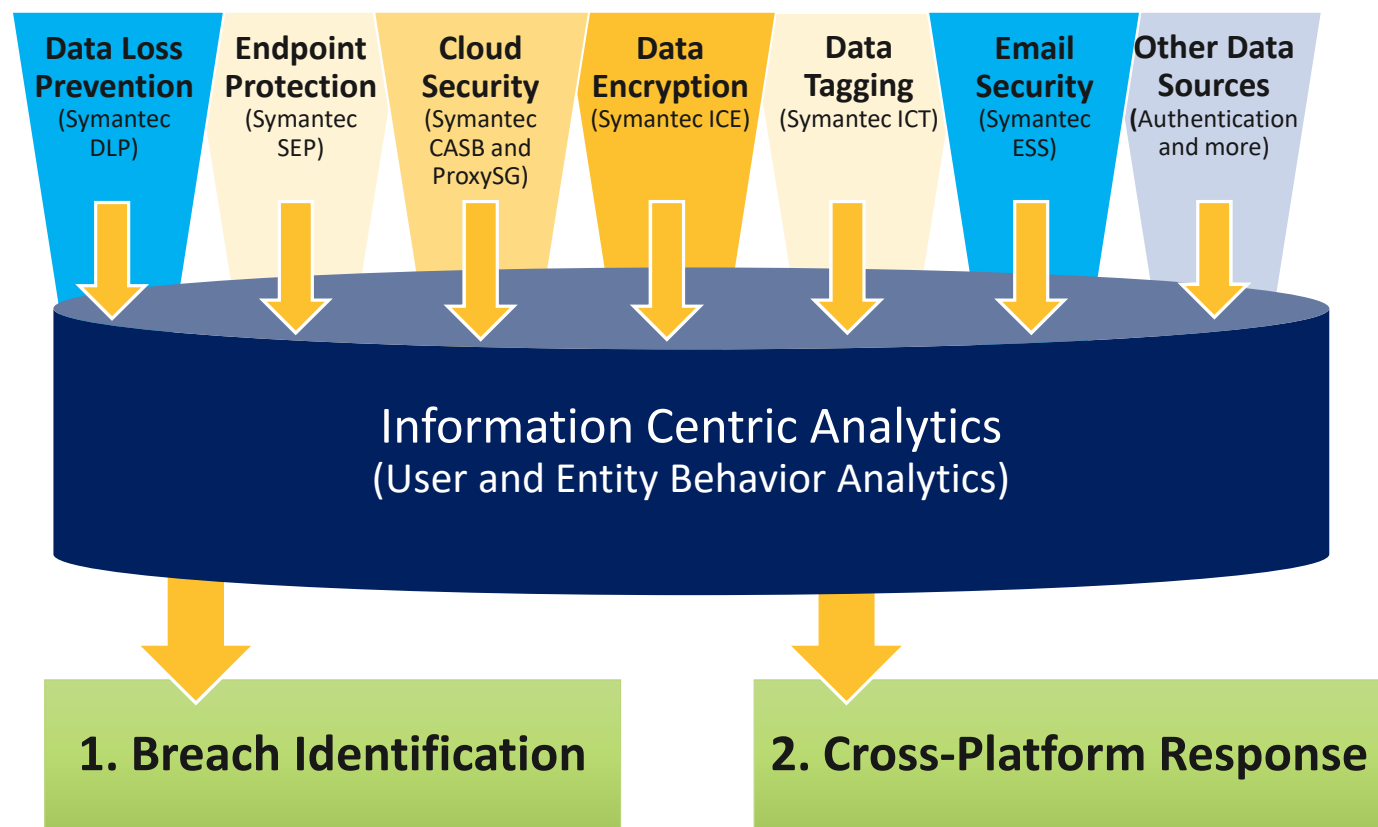
DLP Policy Suggests Classification to User



Extend DLP Policy Framework to All Control Points – ICT Leverages Advanced DLP Detection

Centralized Risk Management with ICA

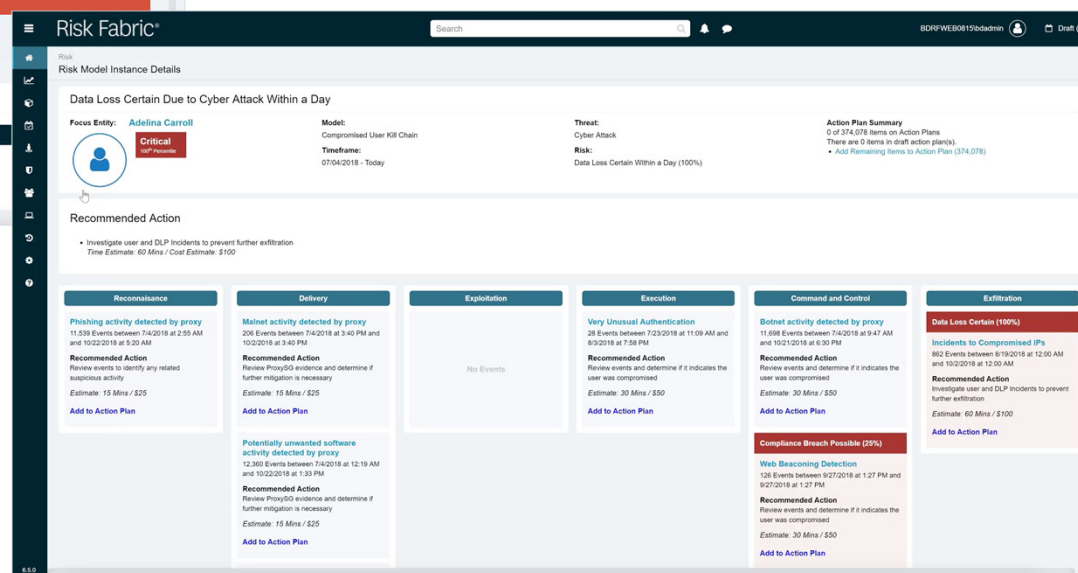
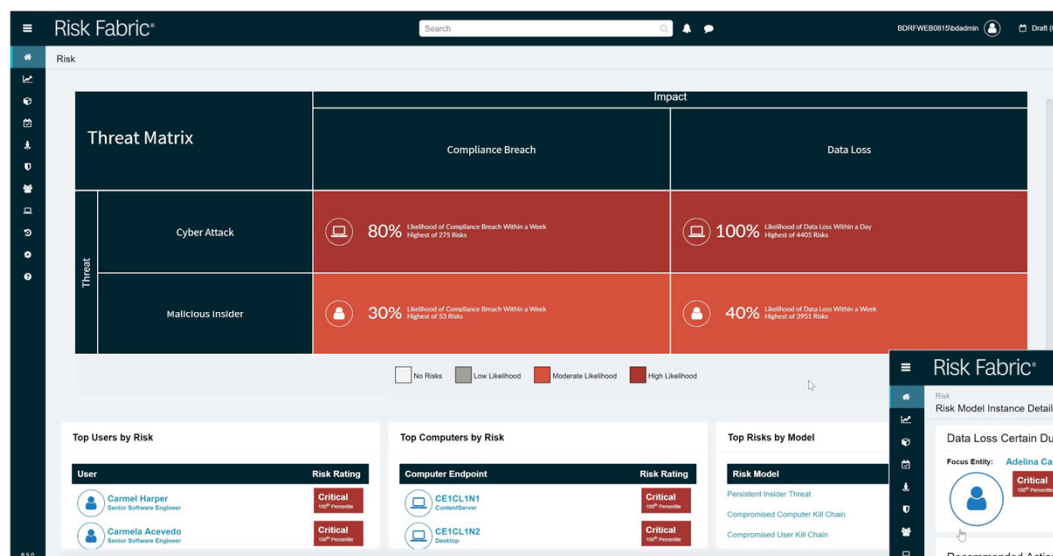
New Integration with Symantec Email Security



Compromised User Kill Chain Risk Model

- **Identify Early Stages**
 - *Email phishing & emerging threats*
- **Map Vulnerable Assets and Entities**
 - *Rank exposed endpoints and data*
- **Correlate Exfiltration Attempts**
 - *Leverage DLP for data incidents*
- **Stop Potential Compromises**
 - *Visibility into risks and outcomes*

End-to-End View of Compromised User Kill Chain



What's New in Data Loss Prevention 15.5



ENDPOINT

DETECTION

DLP 15.5

CLOUD

ICT/ICE

DLP - SEP Integration

SEP Intensive Protection
Protection based on reputation

Automatic Classification

DLP classifies existing files

Added Securlets

Support for Amazon S3, Spark, and Slack
via CASB

EMDI

New fingerprinting technology
Accuracy, performance and security for
indexed data

DLP for Skype for Business

REST API Detection

Larger Inspection File

Support for larger file sizes

DLP Suggests Classification

DLP policy assists user for data
classification

ICE for Browser Channel

Apply DRM encryption to files uploaded
using HTTPS

Legal Disclaimer



Any information regarding pre-release Symantec offerings, future updates or other planned modifications is subject to ongoing evaluation by Symantec and therefore subject to change.

This information is provided without warranty of any kind, express or implied.

Customers who purchase Symantec offerings should make their purchase decision based upon features that are currently available.

STRATEGY: 2019 and Beyond Better Data Protection for More People



Product Outcome

Make DLP easier to Use



Expand Data Protection Beyond Company



Protect from Malicious Users and Processes



Info Protection Focus

SIMPLIFY DLP

Simplify DLP deployment

- Simpler install & upgrade
- Console UX improvements

Automatic policy/classification

- No policy required
- Template, index and ML
- Supervised learning

Simplify DLP remediation

- End use remediation
- Self Service
- Integrated with ServiceNow

Increased DLP speed & scale

- Larger Files
- Faster detection

DLP Cloud Service Availability

- 99.99% uptime SLA
- Multi-region support

DLP Cloud for WSS

- Policy improvements

DLP Cloud for CASB

- New Gatelets and Securlets
- Cisco Spark, S3, Splunk

FROM DLP TO DATA PROTECTION

Integrate DLP, Tagging, ICE

- Agent: Single installer
- Console: Auto Tagging in DLP Console

Integrate ICE with ESS, Fireglass

- Simple protection for cloud email
- Isolation based document protection

INSIDER RISK

DLP-SEP Integration

- Agent: Single installer
- Console: DLP in SEP evergreen
- DLP monitors suspicious process
- SEP protects PC with sensitive data

Activity Monitoring (DLP Agent)

- Record activities
- Discover anomalous behavior
- Investigate users



Thank you!

Copyright © 2019 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo 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 document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Copyright © 2019 Symantec Corporation | Confidential