



What's New in DLP 15.5

Information Protection

John Gruhn, CISSP

Symantec Data Loss Prevention SME

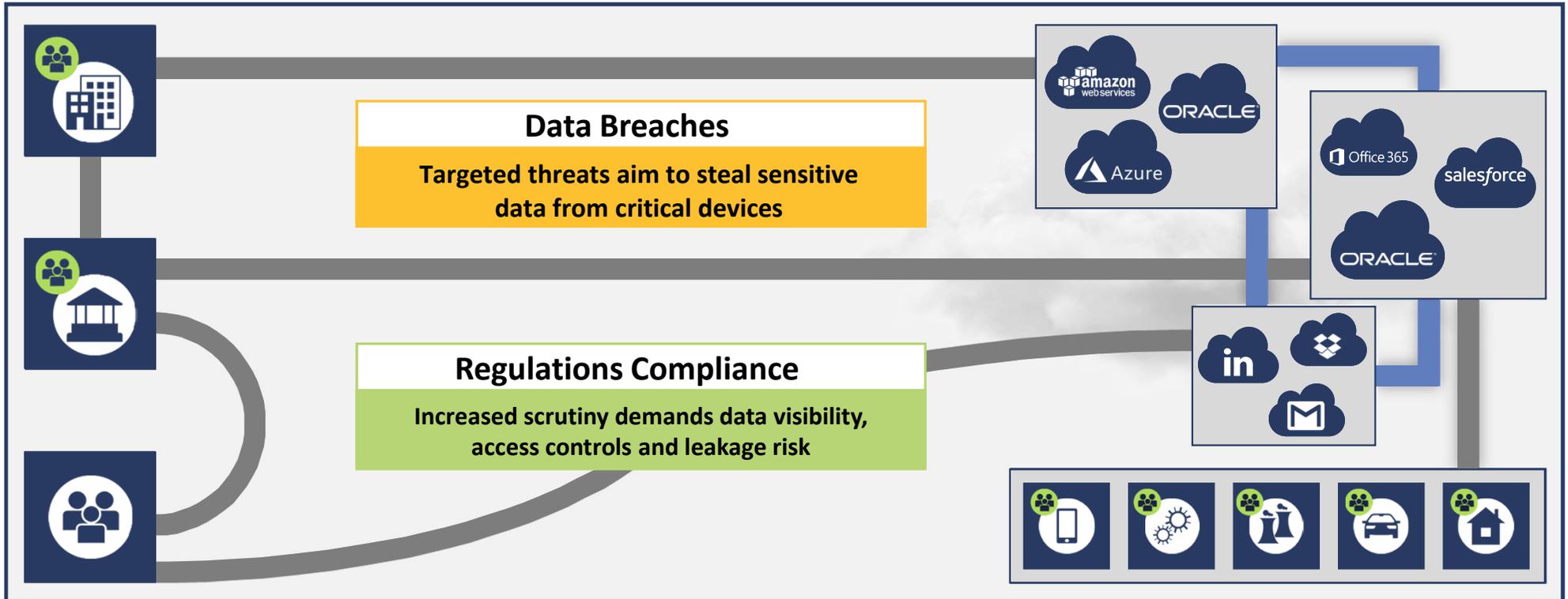
April 2019



Pressing Problems in Data Security



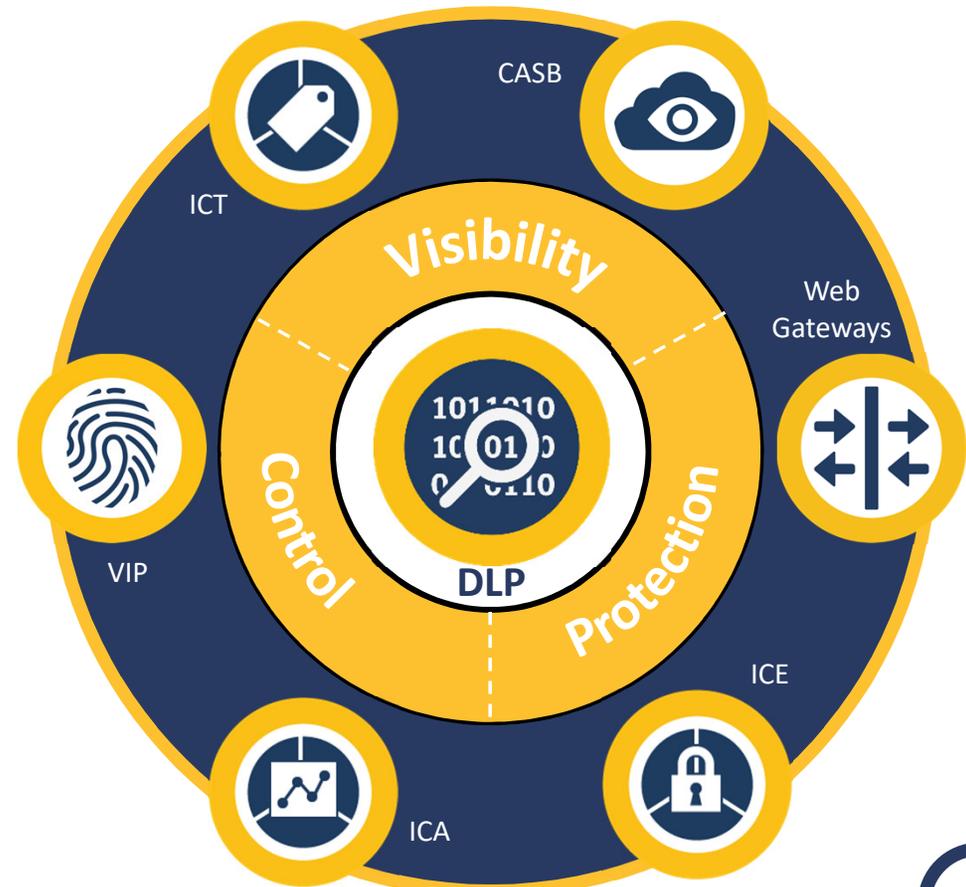
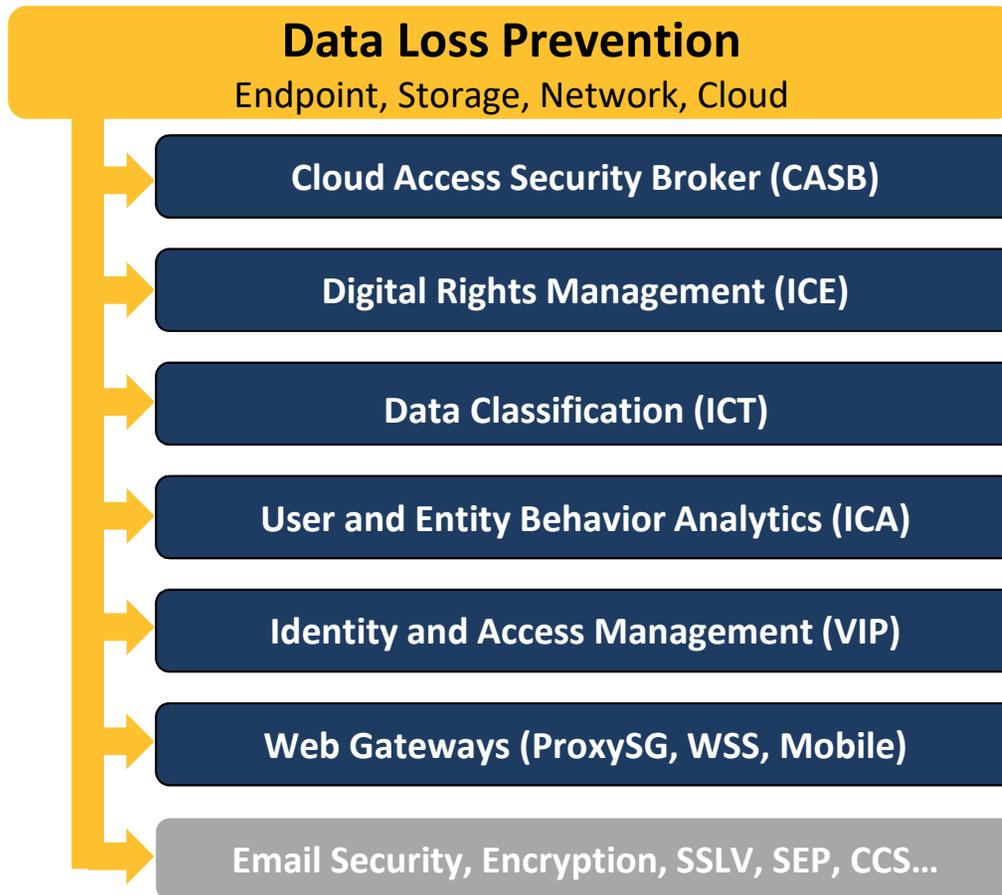
Changing usage models will mandate a platform architecture



From DLP to An Integrated Data Security Platform



Key products



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

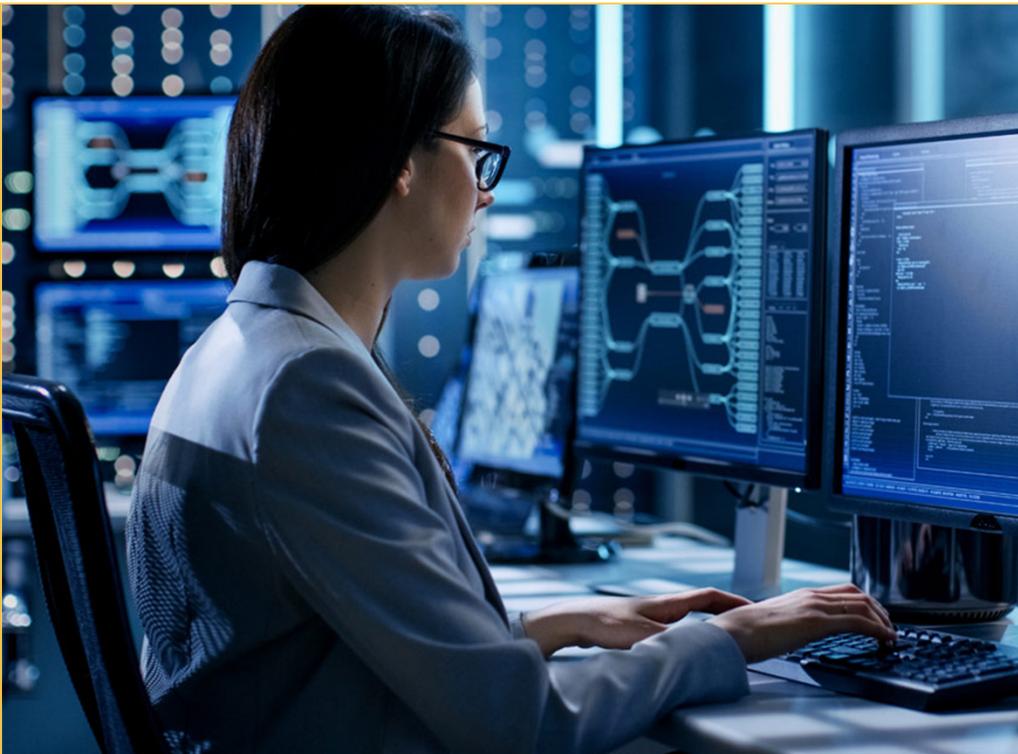


Regulations & Compliance

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



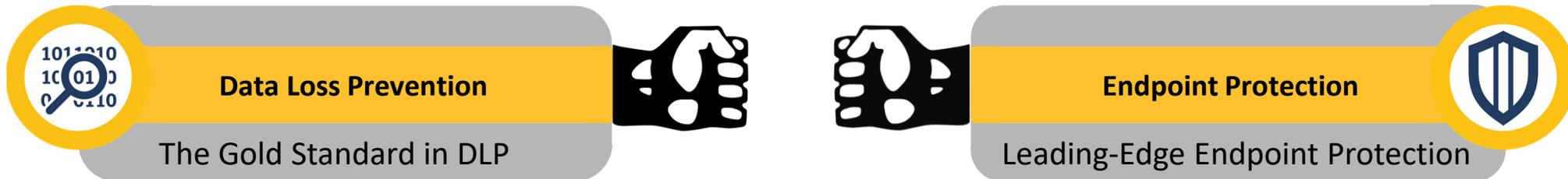
“How do I protect my sensitive data from malicious applications?”



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

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?

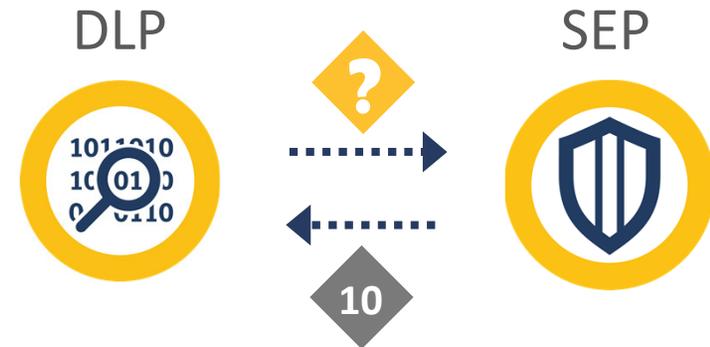
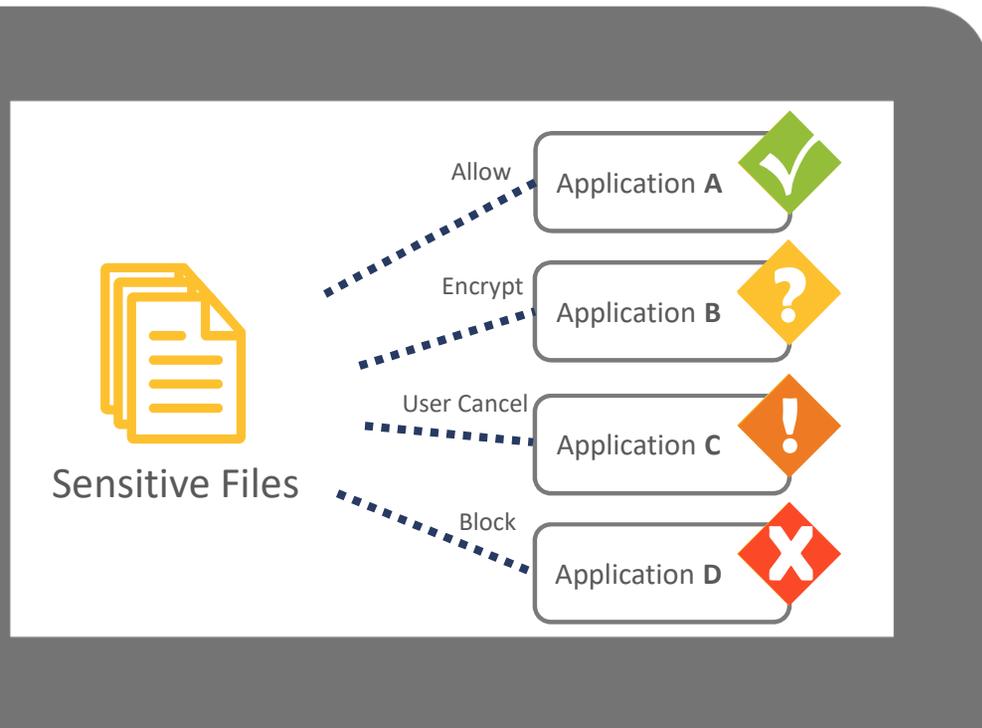
APT?

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

Name *

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

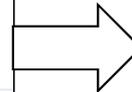
- Application File Access
- Cloud Storage

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

Policy	Matches
kw-block [view policy]	2
r1 (Keyword Match)	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: AUTOMATIONPUNE\User1

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 Level: Malicious

Application MD5: d399cf5dcccdeb5724ff47b7782ba72a

Hash: 68f4c25c9401429a87141669e52f9c88bc4540deaf

SHA-256 Hash: 9f586ad31ed5f465c4de [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 Name: [change]

Data Owner Email Address: [change]

Matches (matches found in 1 component)

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

- 489-36-8350 4928-3813-3266-4295 Ashley Borden 814-14-8995 5370-463
- 690-05-5318 4916-4811-5814-8111 Susan Davis 421-37-1398 4916-4034-92
- 458-02-6124 5299-1561-5689-1938 Rick Edwards 612-20-6832 5293-8502-0
- 300-62-3268 5548-0246-6336-5664 Lisa Garrison 660-83-8868 4539-5385-7
- 213-46-8918 4916-9766-5240-6147 Mark Hall 448-48-3138 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 5144-8691-2776-1108 Monte Mooschem 477-36-0282 5527-13
- 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
- 687-05-8369 5495-8602-4508-6804 Julie Renfro 751-01-2327 5325-3256-
- 824-84-9381 4532-0065-1968-5602 Jack Russell 534-30-2668 34538969200
- 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



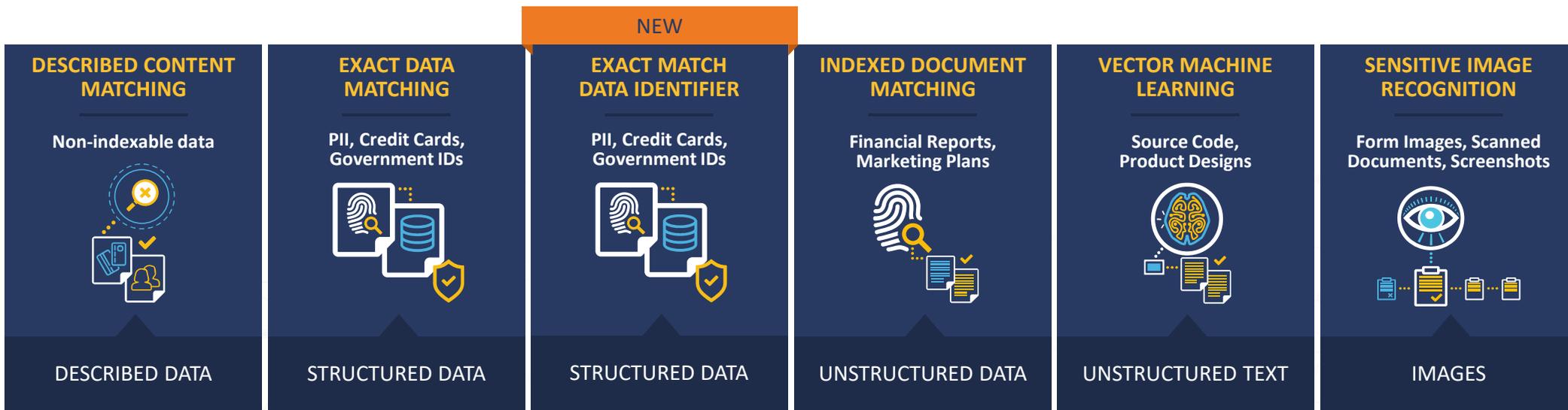
“How do I ensure my sensitive data is discovered and protected on every channel?”



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

Enable EMDI in DLP Policy

The image displays two screenshots of the Symantec Data Loss Prevention (DLP) configuration interface. The left screenshot shows the 'General' and 'Conditions' sections of a policy rule named 'SSN with EMDI'. The 'Conditions' section is expanded to show 'Standard Matches Data Identifier' with 'Data Identifier: US Social Security Number (SSN)'. The 'Optional Validators' section is highlighted with a yellow box and a blue arrow pointing to the 'Exact Match Data Identifier Check' option. The right screenshot shows the 'Exact Match Data Identifier Check' configuration, which is circled in blue. This configuration includes a dropdown for 'Profile' set to 'Customer Records', a dropdown for 'Required' set to 'SSN', and a dropdown for 'At least match' set to '1'. A blue box at the bottom left contains the text 'Enable EMDI in DLP Policy' with an arrow pointing to the 'Optional Validators' section in the left screenshot.

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
 Is Less Than or E 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	Count
Content is classified [view policy]	1
Content is classified (ICT)	1

Matches (matches found in 1 component)
acme_restricted.docx (1 Match):
Restricted(3), ENG, Symc

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

Actions <choose action type>

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



Information Centric Tagging Administration Console

HOME CREDENTIALS CLASSIFICATIONS ROLES RULES LICENSES SYSTEM SETUP

Information Centric Tagging Administration Console

CREDENTIALS Manage Information Centric Tagging Users • Search Users in the Active Directory • View and Change Users Information Centric Tagging settings • Add and remove Users from Information Centric Tagging	CLASSIFICATIONS Manage Classifications • View current and past Classification Settings • Create and edit Companies and Scope • Customize resulting Classifications	ROLES Manage User Roles • View current and past Role Matrices • Create, edit and delete User Roles
RULES Manage Rules • Define and manage classification rules	LICENSES Manage Licenses • Upload Information Centric Tagging Licenses • Track Licenses Usage	SYSTEM SETUP Manage Information Centric Tagging System • Change Database, Active Directory, Encryption and Web Server Setup

Symantec

Symantec Data Loss Prevention

Login:

Password:



Untitled - Message (HTML)

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW SYMANTEC ICT

Calibri (Box) 11

From: alicc_manager@ep-exch2016.punedip.symantec.com

Level: Personal Internal Confidential Top Secret

All files that are to be restricted for use by Acme employees are to be classified as Internal [More help](#)

Hello Bob

Here is some of our latest M&A in|

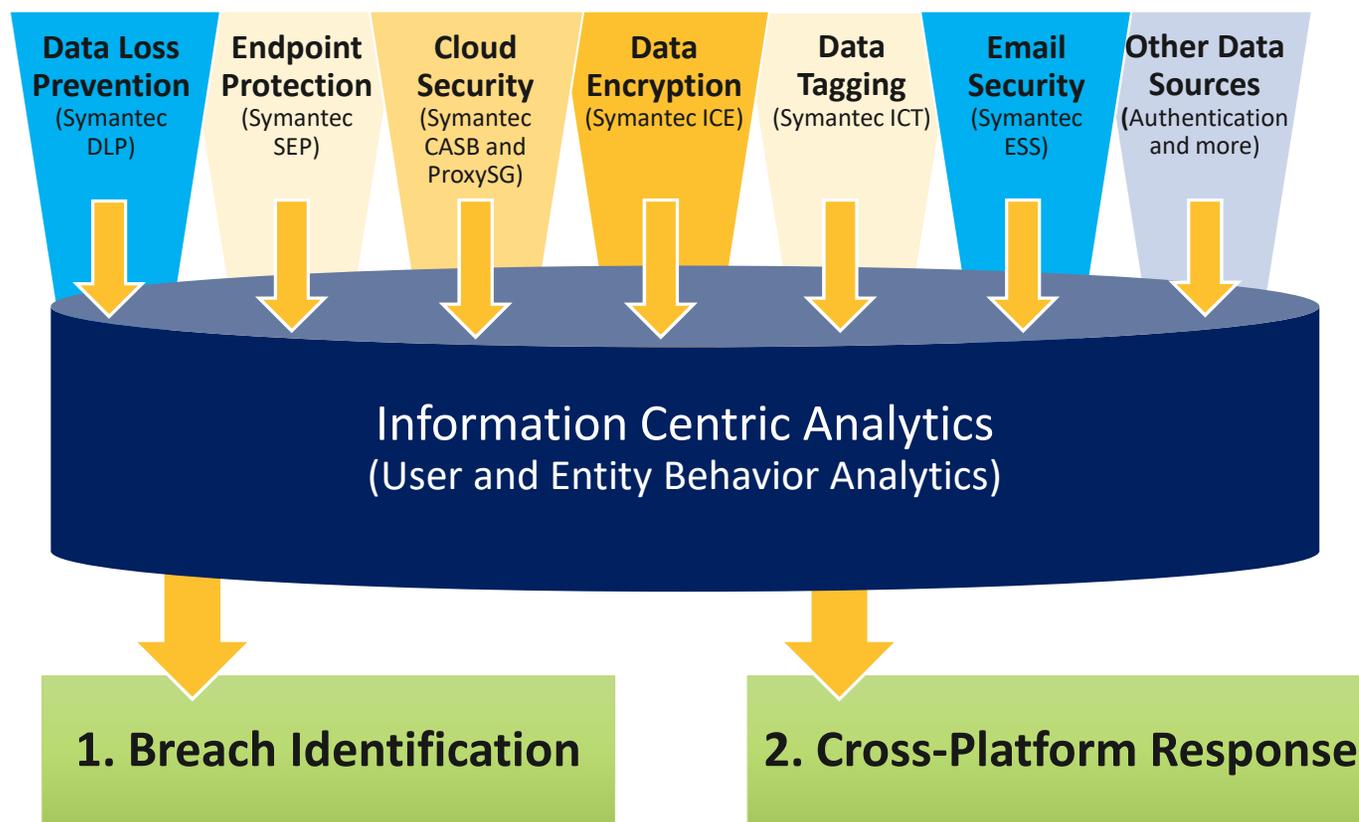
Classified as: Acme / Acme Scope / Internal [What does this mean?](#)

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

Centralized Risk Management with ICA



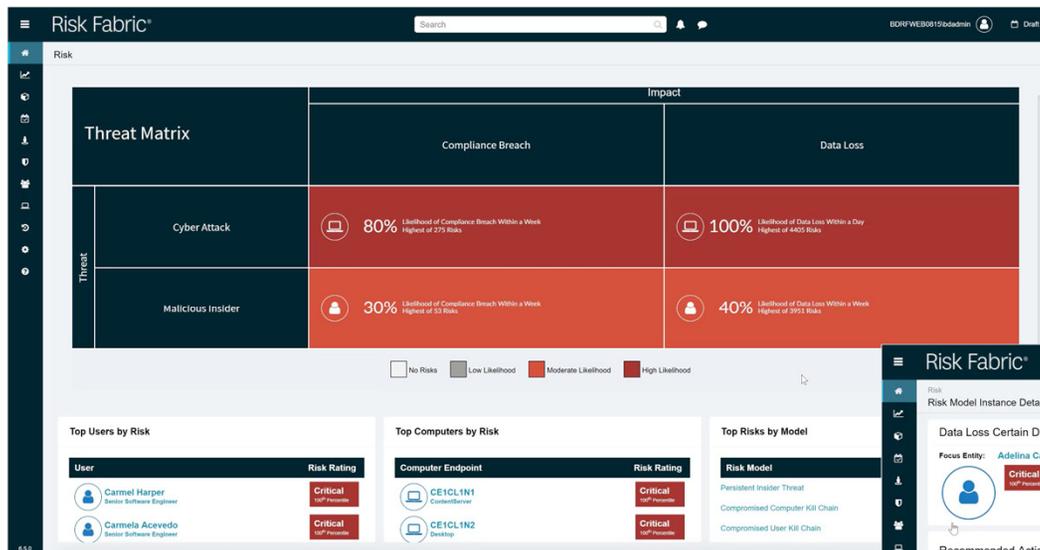
New Integration with Symantec Email Security



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



Top Users by Risk

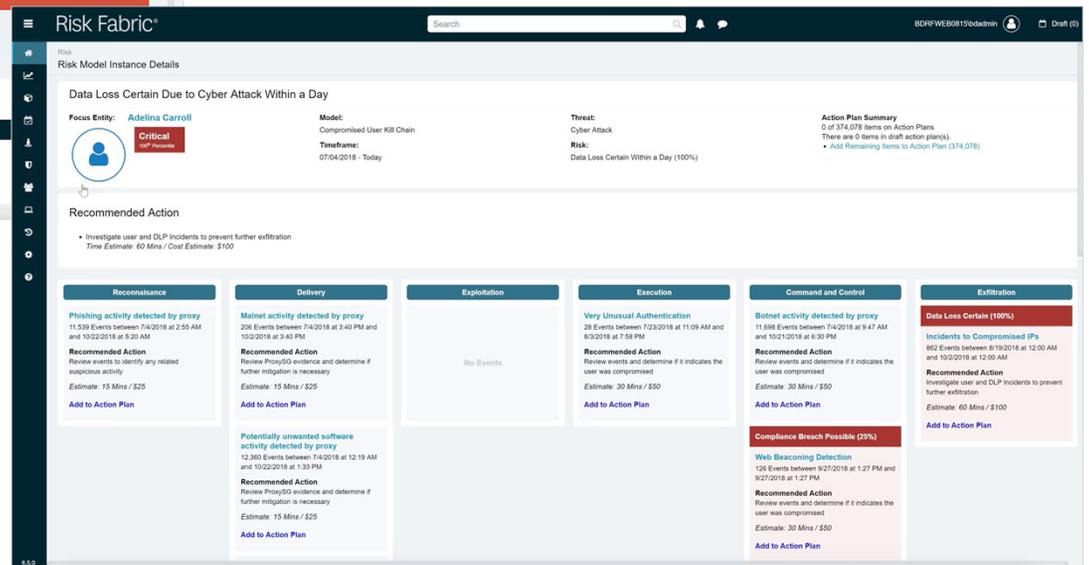
User	Risk Rating
Carmel Harper Senior Software Engineer	Critical 100% Penetration
Carmela Acevedo Senior Software Engineer	Critical 100% Penetration

Top Computers by Risk

Computer Endpoint	Risk Rating
CE1CLIN1 CustomerServer	Critical 100% Penetration
CE1CLIN2 Desktop	Critical 100% Penetration

Top Risks by Model

Risk Model
Persistent Insider Threat
Compromised Computer Kill Chain
Compromised User Kill Chain



What's New in Data Loss Prevention 15.5



ENDPOINT

DETECTION

CLOUD

ICT/ICE

DLP 15.5

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