What's New in DLP 15.5

Information Protection

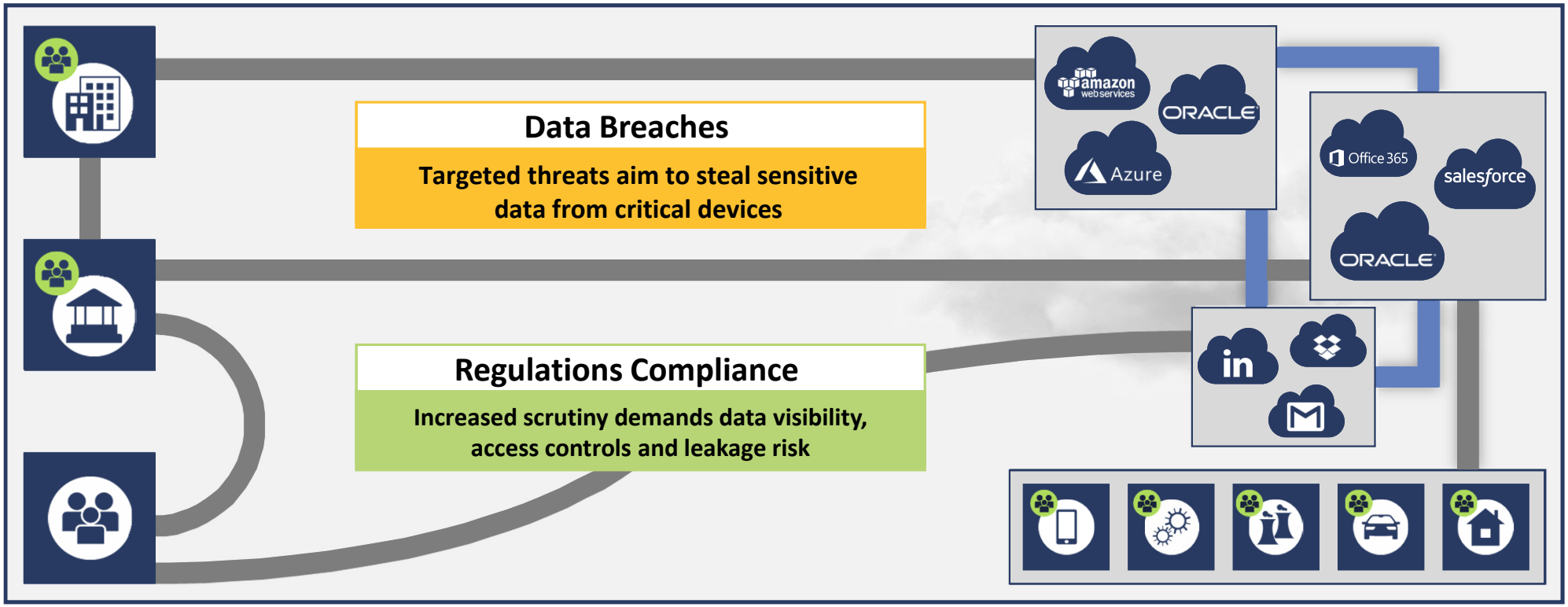
John Gruhn, CISSP

Symantec Data Loss Prevention SME

April 2019

Pressing Problems in Data Security

Changing usage models will mandate a platform architecture

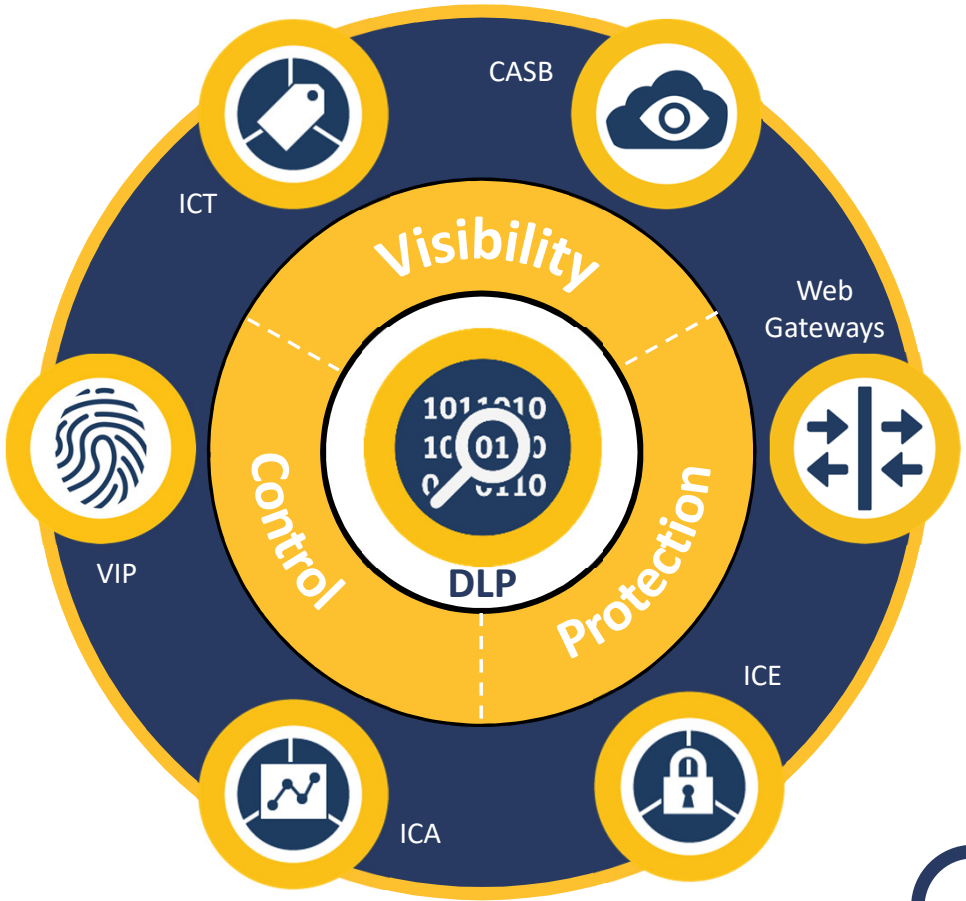


From DLP to An Integrated Data Security Platform

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…



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?

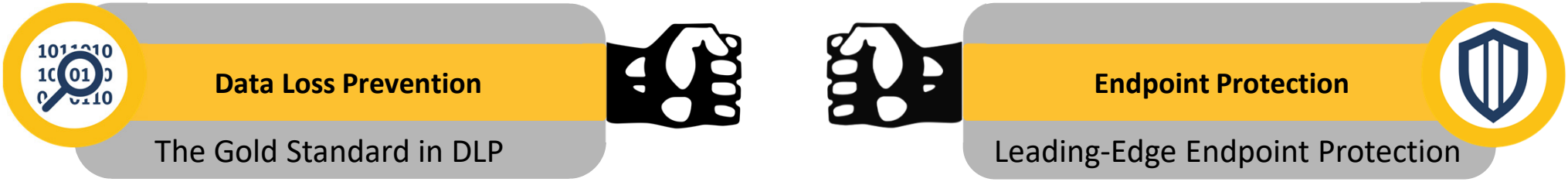
- Data residing and flowing everywhere
- Discovery of sensitive data is difficult
- Breach risk by insiders and 3rd parties

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

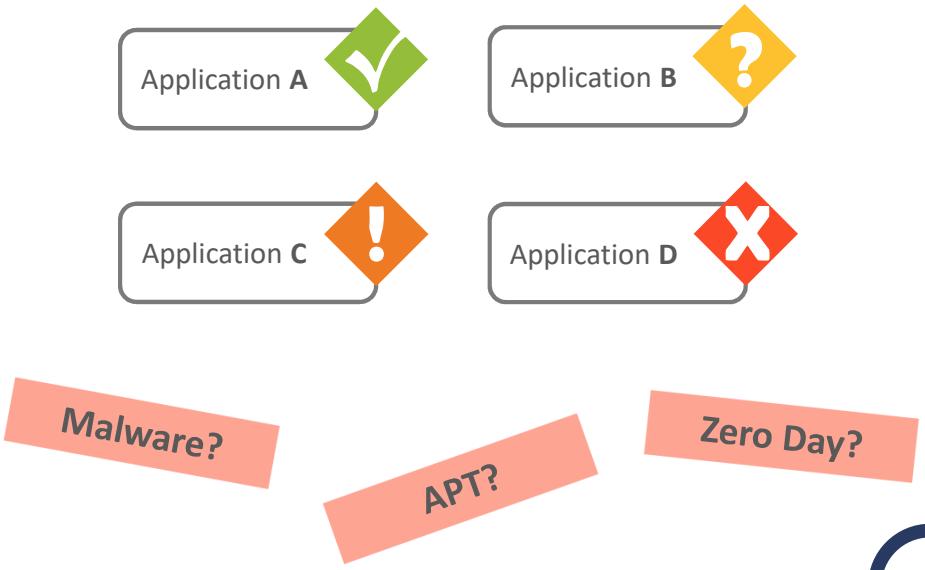
Cyber-threats lurk around the corner when untrusted apps touch sensitive data

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

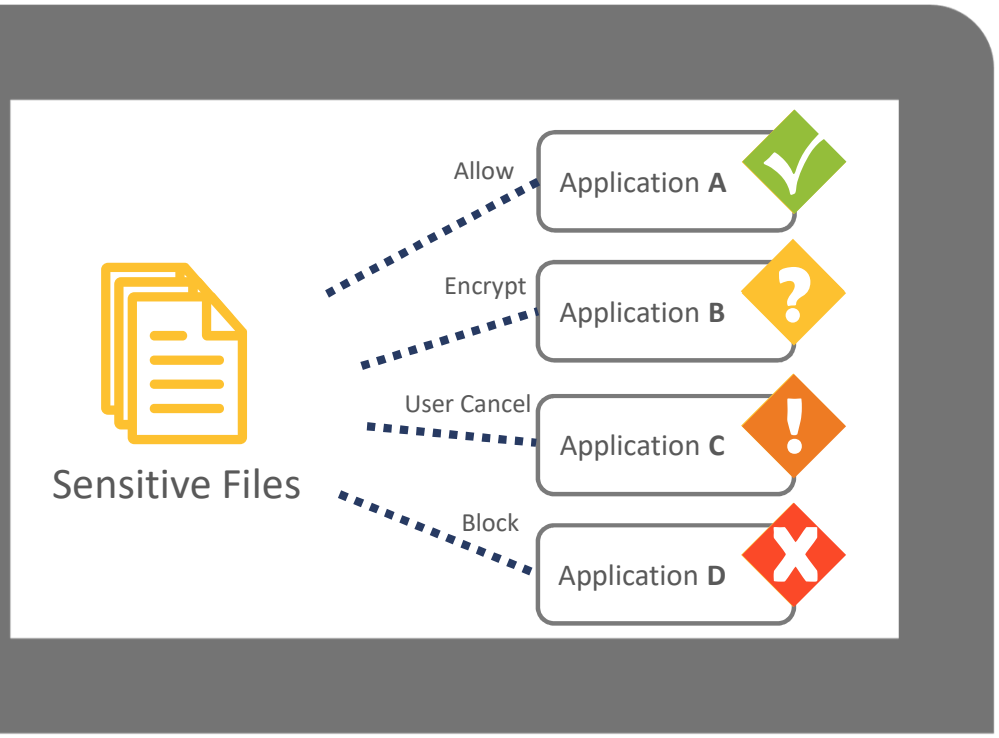
What do you trust?

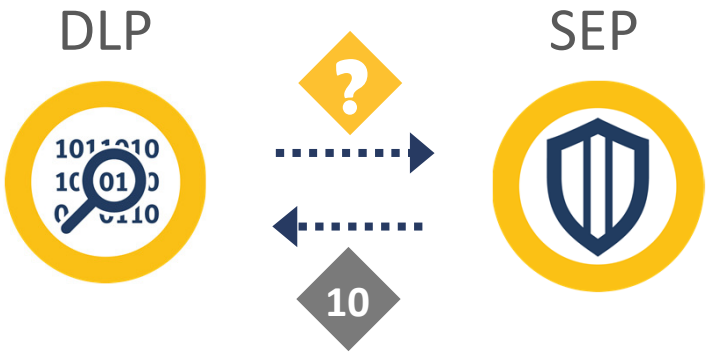
The risk of data exfiltration is significant with **UNKNOWN**, **MALICIOUS** or **SUSPICIOUS** apps



How DLP-SEP Integration Works

SEP Intensive Protection delivers data exfiltration protection

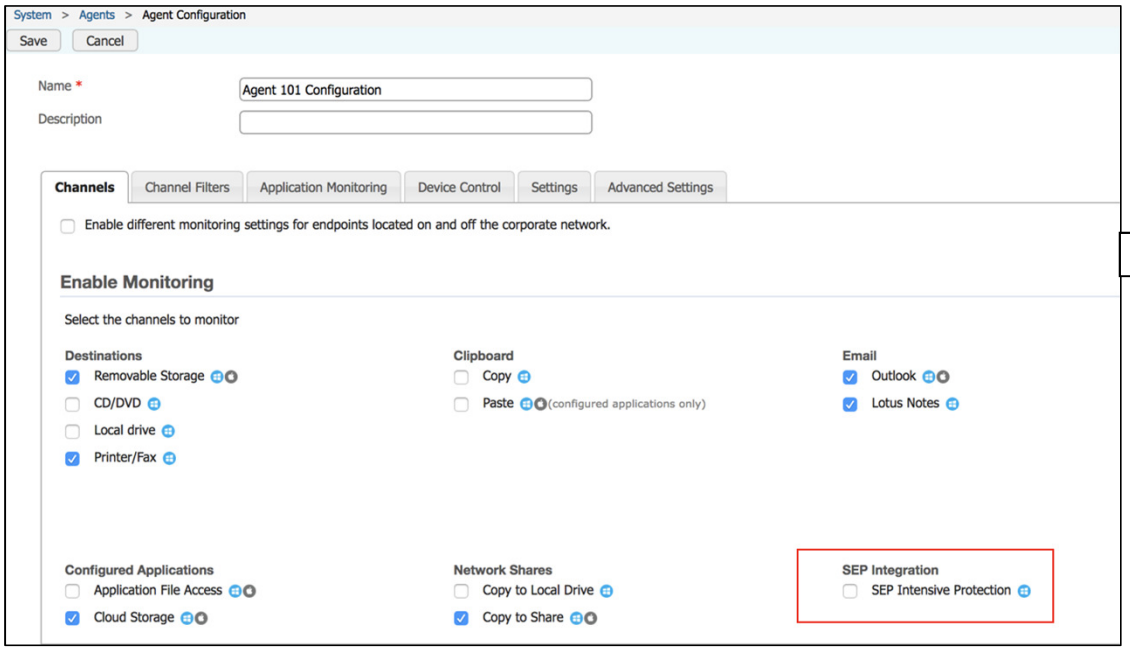


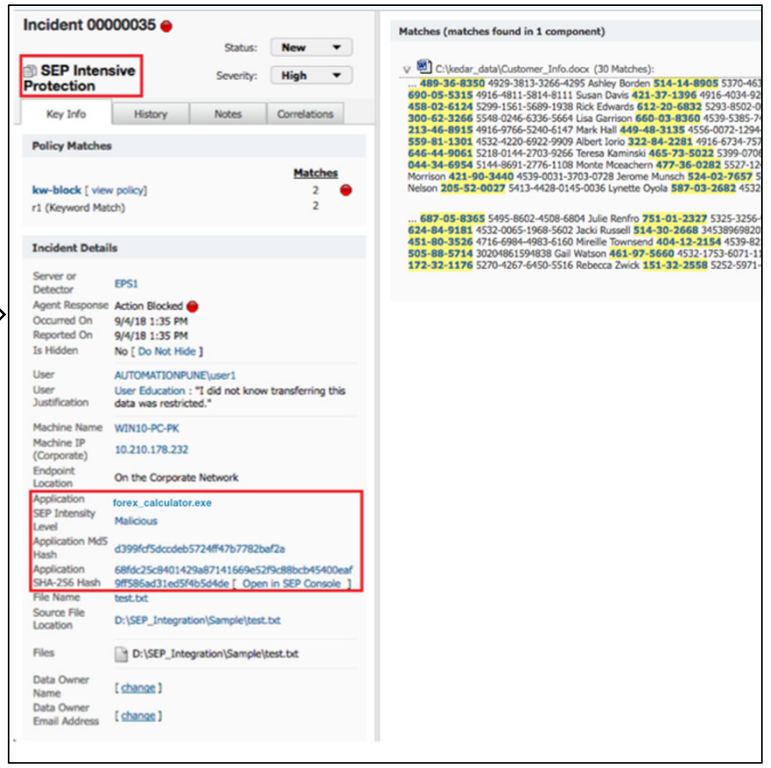


1. A new user-installed application (UIA) is launched
2. DLP detects the app and sends an app info request to SEP
3. SEP returns a numeric risk score based on reputation
4. DLP maps an intensity level: UNKNOWN-MALICIOUS-SUSPICIOUS
5. DLP detects when these apps touch sensitive data
6. DLP applies a policy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

DLP Monitors Apps Using SEP Reputation

SEP Intensive Protection in DLP console

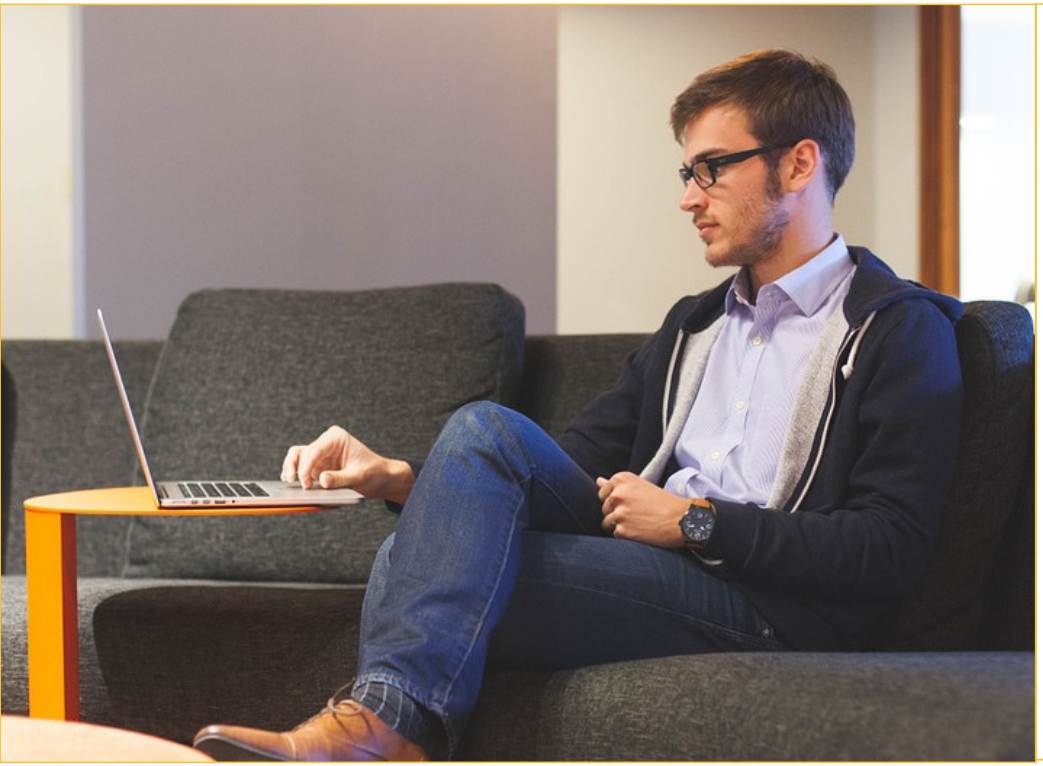




Easily enabled through Enforce console

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

NEW

DESCRIBED CONTENT MATCHING	EXACT DATA MATCHING	EXACT MATCH DATA IDENTIFIER	INDEXED DOCUMENT MATCHING	VECTOR MACHINE LEARNING	SENSITIVE IMAGE RECOGNITION
Non-indexable data	PII, Credit Cards, Government IDs	PII, Credit Cards, Government IDs	Financial Reports, Marketing Plans	Source Code, Product Designs	Form Images, Scanned Documents, Screenshots
					
DESCRIBED DATA	STRUCTURED DATA	STRUCTURED DATA	UNSTRUCTURED DATA	UNSTRUCTURED TEXT	IMAGES

"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

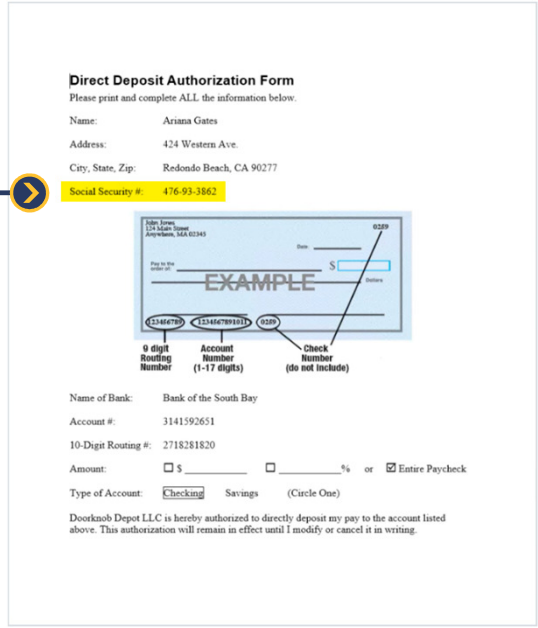
What is it?

- 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 | Account Number (1-17 digits) | Check Number (do not include)

Name of Bank: Bank of the South Bay

Account #: 3141592651

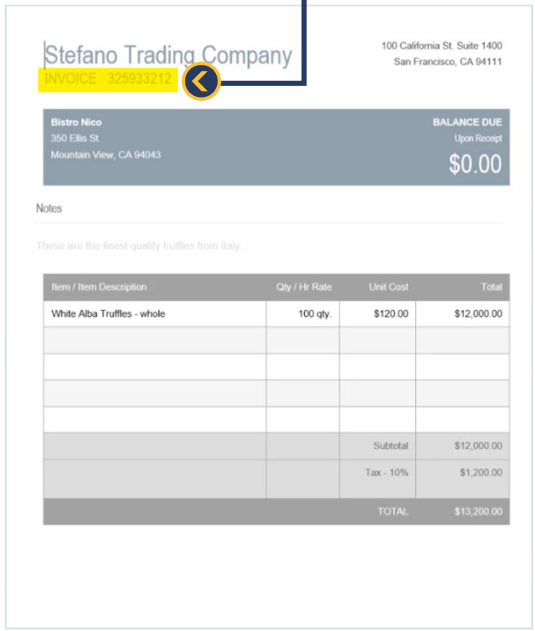
10-Digit Routing #: 2718281820

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 325933212

100 California St. Suite 1400
San Francisco, CA 94111

Bistro Nico
350 Ellis St.
Mountain View, CA 94043

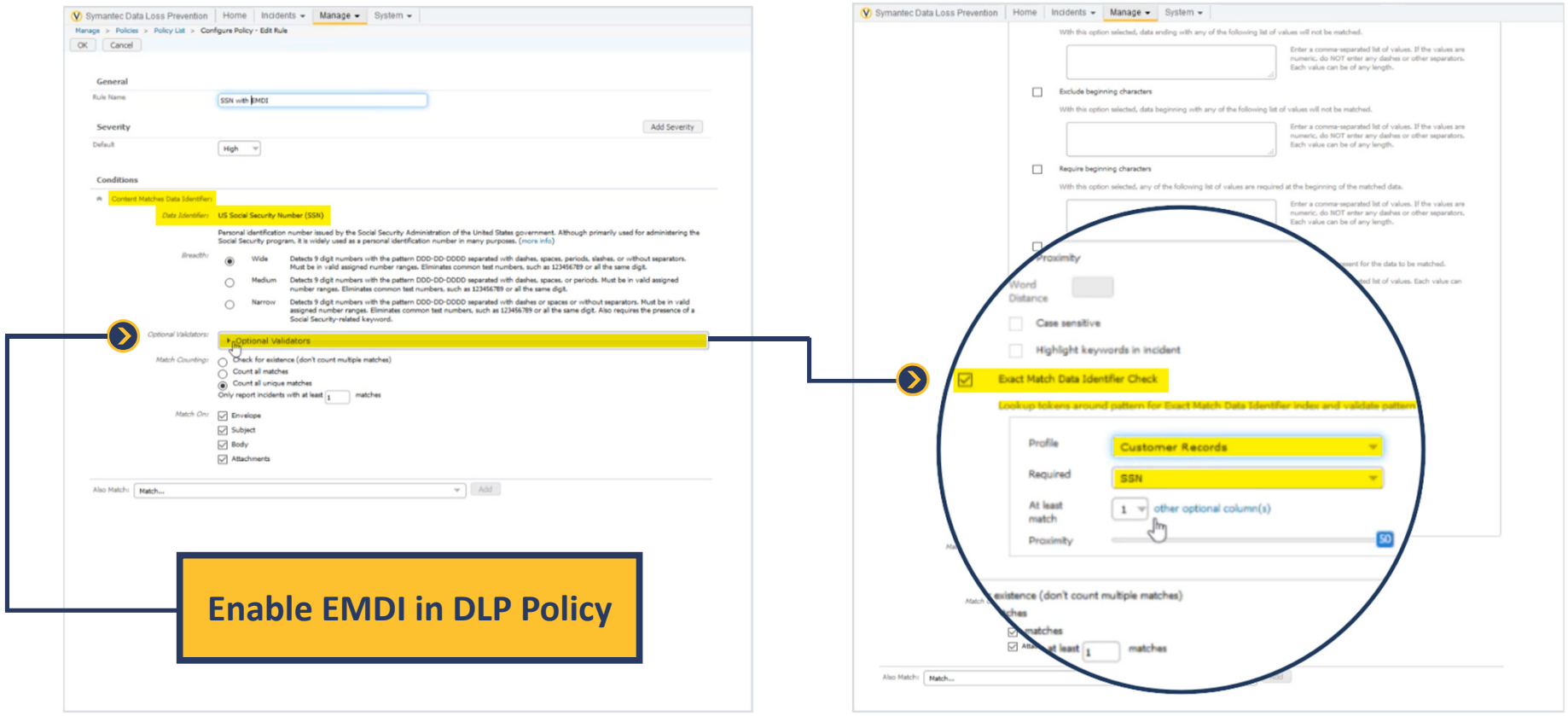
BALANCE DUE
Upon Receipt
$0.00

Notes

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

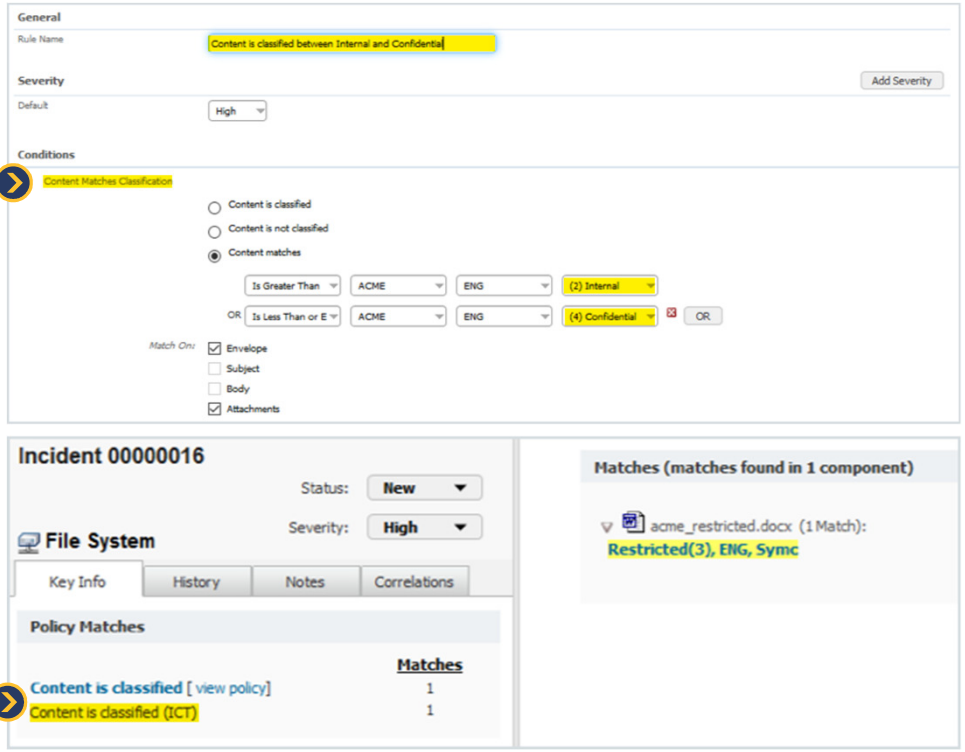
Exact Match Data Identifier (EMDI)

Fast, accurate detection of false positive-prone structured data



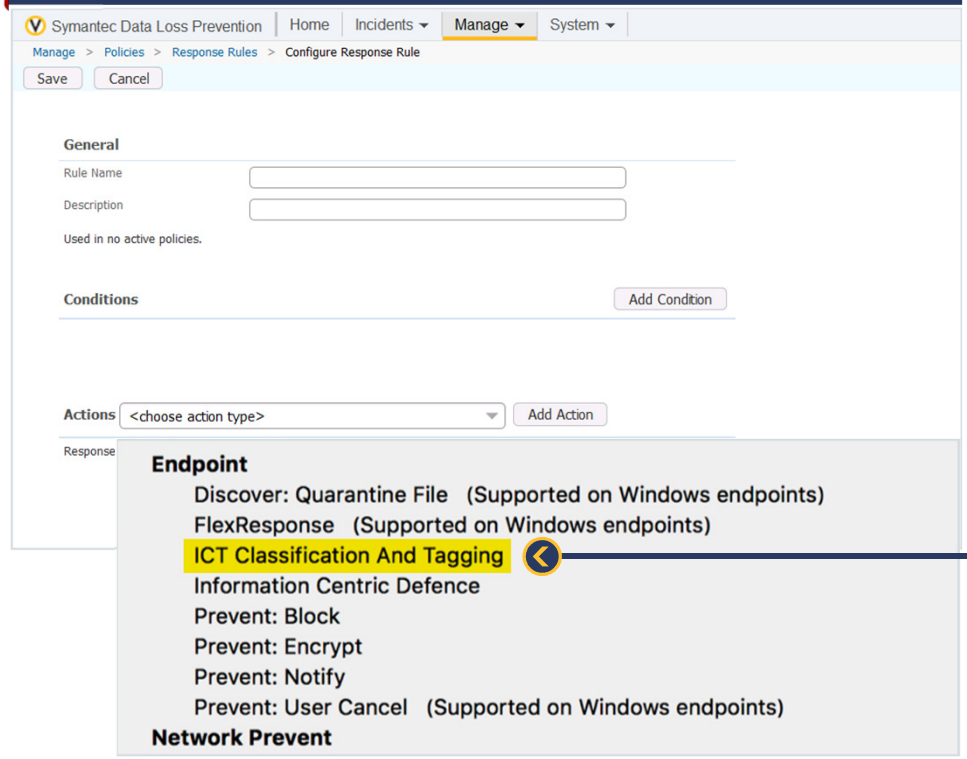
Enhanced DLP Classification & Tagging

DLP Agent Reads Tags



DLP Agent Writes Tags

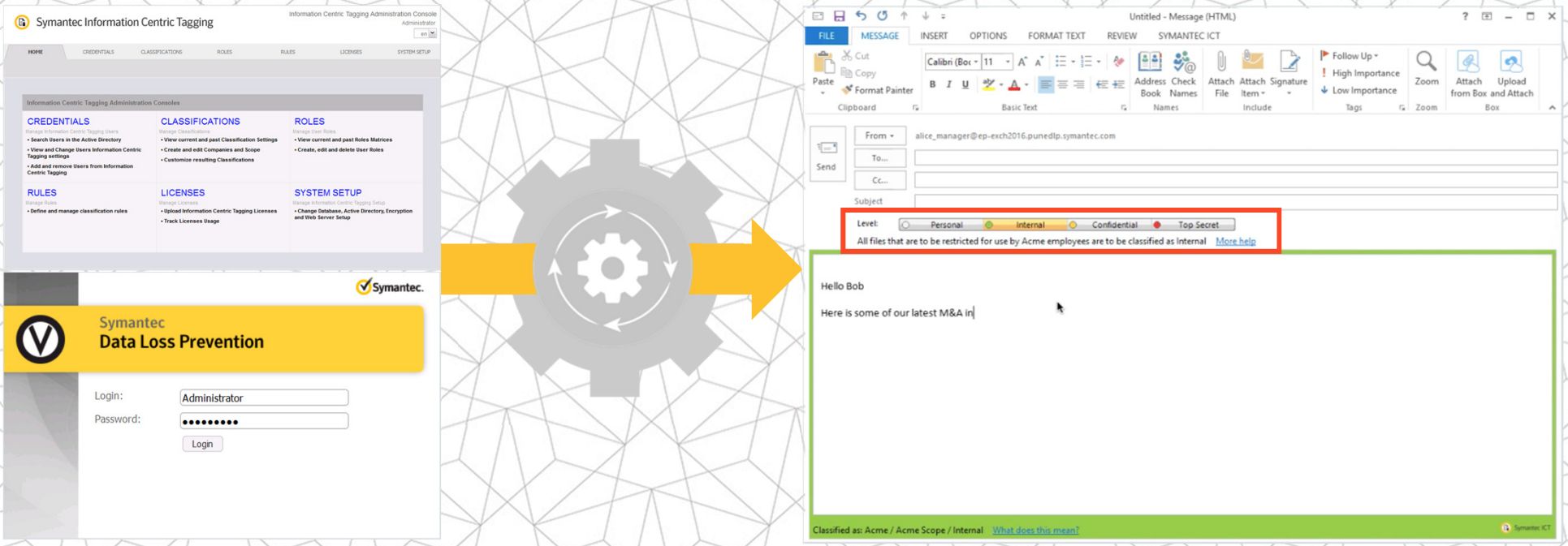
NEW



DLP Policy Drives Classification on Endpoints

DLP Endpoint Discover Scans and Classifies Existing Data on Endpoints

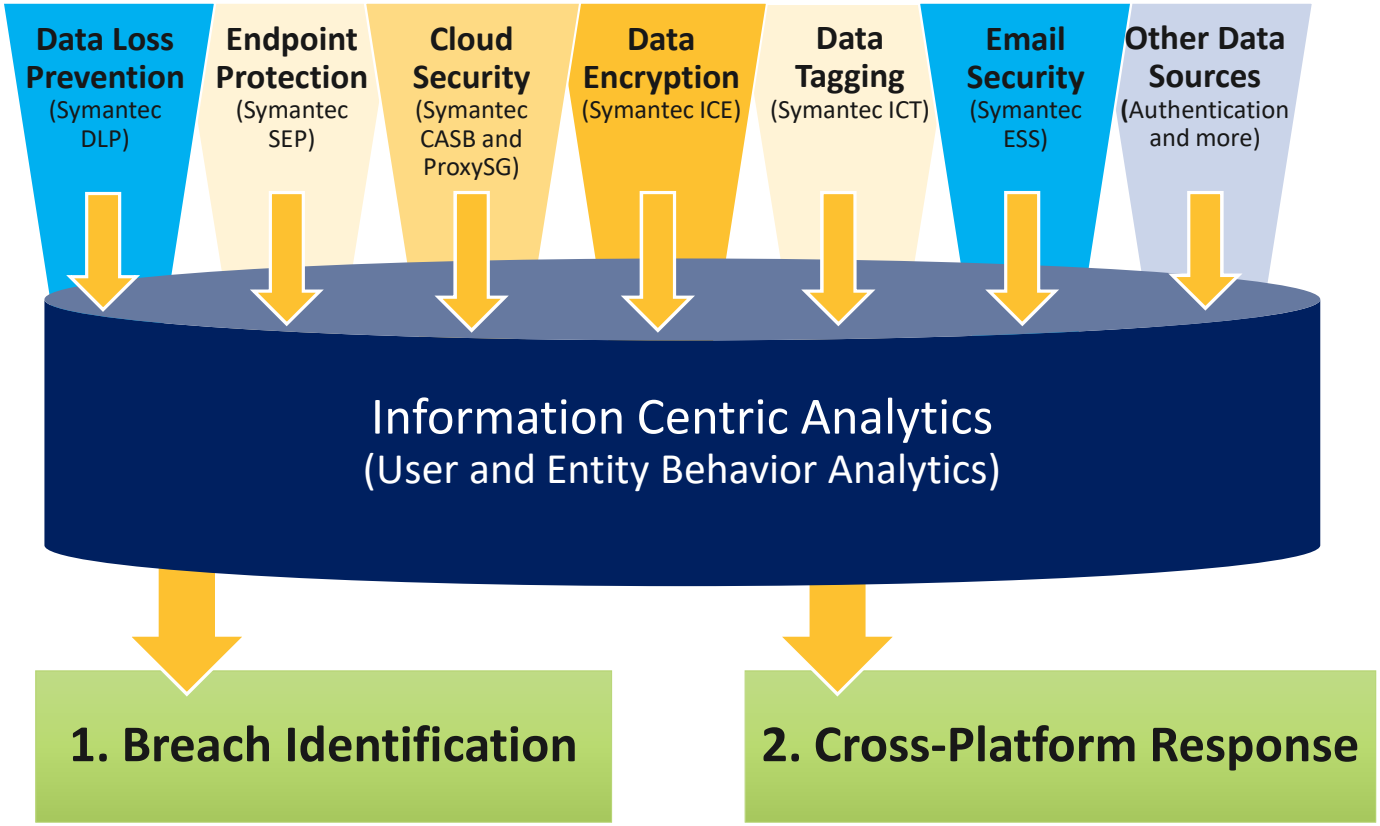
DLP Policy Suggests Classification to User



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

Centralized Risk Management with ICA

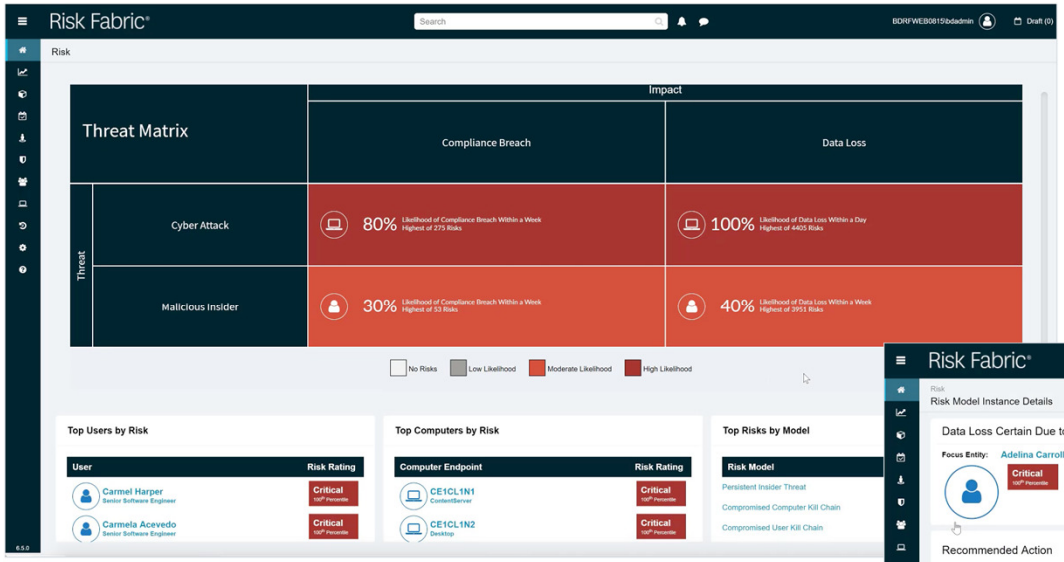
New Integration with Symantec Email Security

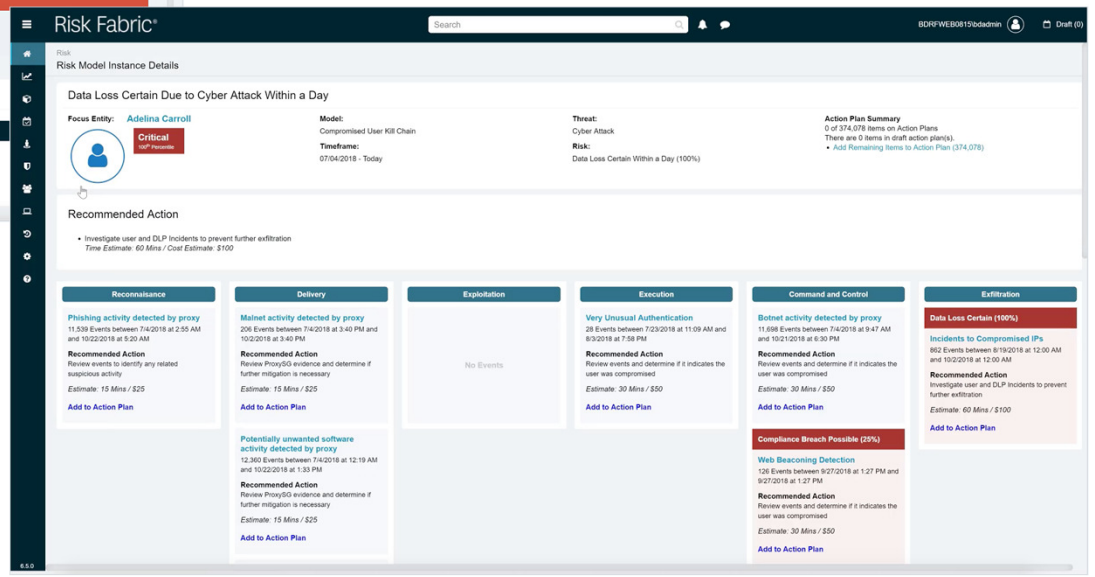


Compromised User Kill Chain Risk Model

- **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*

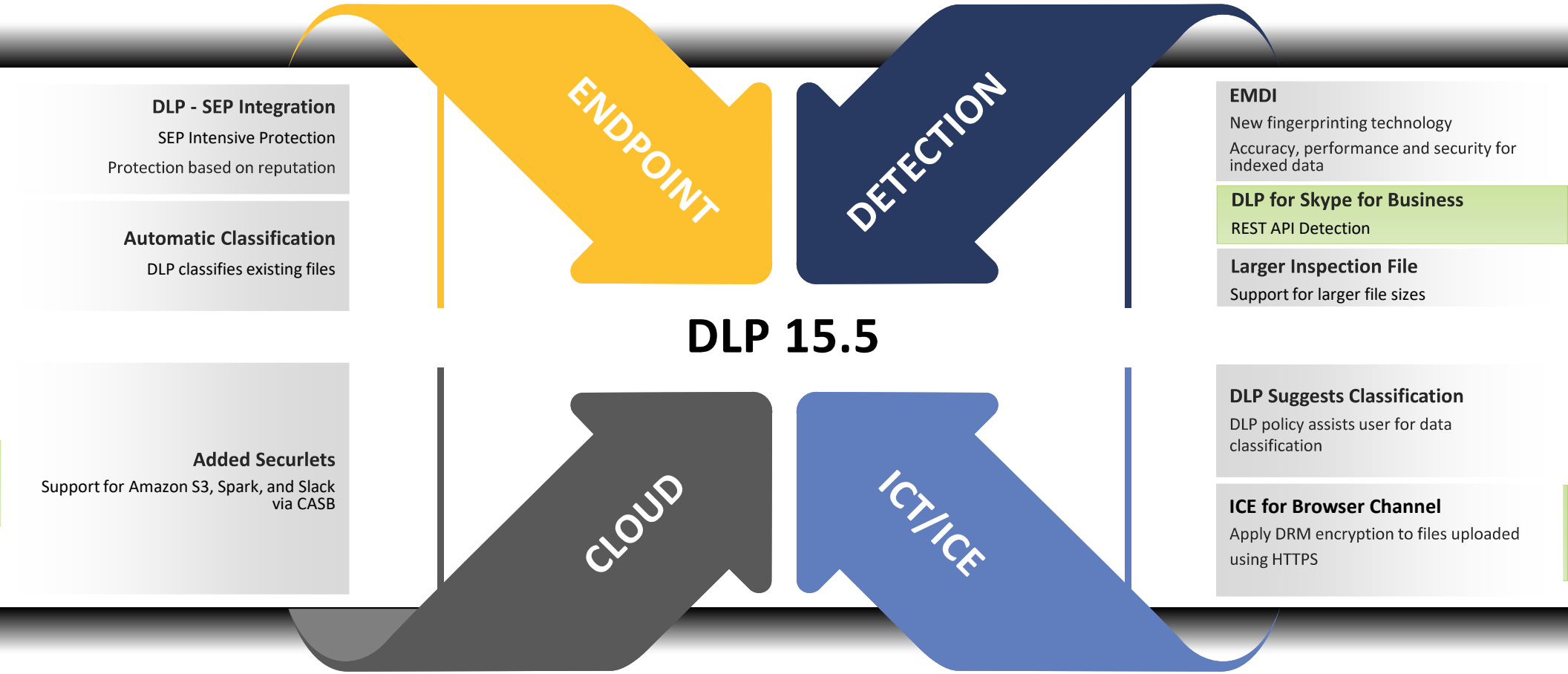
End-to-End View of Compromised User Kill Chain





What's New in Data Loss Prevention 15.5

Symantec.



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

Symantec

	Make DLP easier to Use	Expand Data Protection Beyond Company	Protect from Malicious Users and Processes
Product Outcome			

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!