Symantec.

Data Loss Prevention

Protecting Your Information and Reputation

May 2019

Bruce Ong

Director, Product Management

Symantec Data Loss Prevention

Solution Overview

Compliance

"I need to ensure compliance for regulated data across all channels."

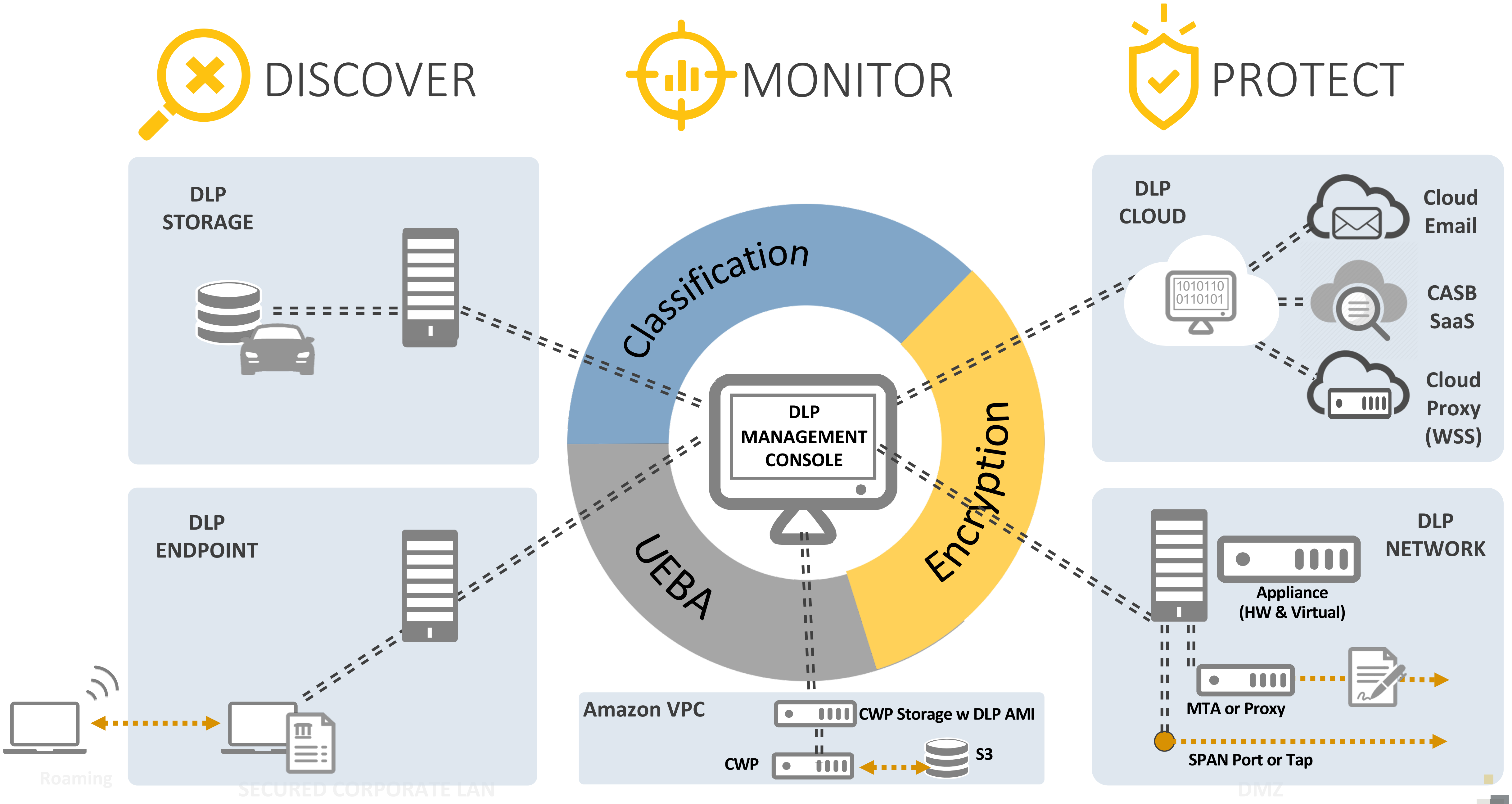
Intellectual Property

"I need to protect the company's secret sauce from competitors and spies."

Symantec DLP Today

Sensitive Cloud Data

"I need to extend my DLP coverage to the cloud in a non-disruptive way"



DISCOVER

MONITOR

PROTECT

DLP STORAGE

DLP ENDPOINT

Roaming

SECURED CORPORATE LAN

Classification

Encryption

UEBA

DLP MANAGEMENT CONSOLE

Amazon VPC

CWP Storage w DLP AMI

CWP

S3

DLP CLOUD

1010110
0110101

Cloud Email

CASB SaaS

Cloud Proxy (WSS)

DLP NETWORK

Appliance (HW & Virtual)

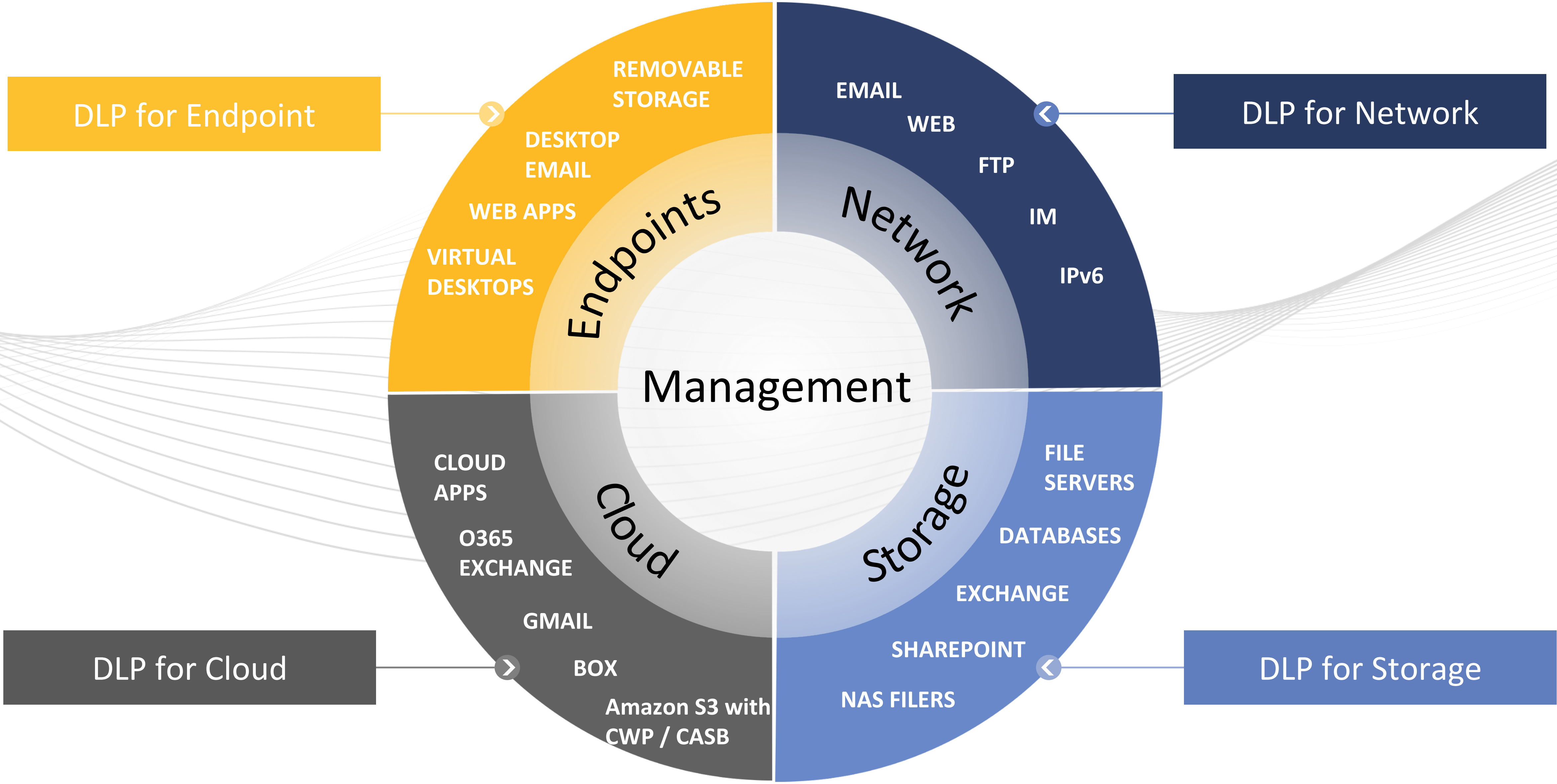
MTA or Proxy

SPAN Port or Tap

DMZ

Broadest coverage of data loss channels

Symantec



Most Comprehensive Data Detection

Gives you the highest accuracy and minimizes false positives

DESCRIBED CONTENT MATCHING	EXACT DATA MATCHING	NEW 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*

Certified for Cloud Deployment

amazon web services™

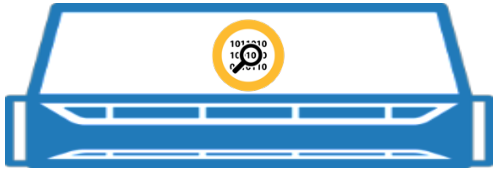
Azure

ORACLE®
CLOUD

- Enforce Server
- Network Discover Server
- Network Prevent for Email Server
- Network Prevent for Web Server
- Endpoint Server
- Oracle DB (BYOL)
- Oracle RDS on AWS

[1] An upgrade kit is available for upgrading to S500-20 (20 core / 64GB RAM / 4TB disk)

New DLP Detection appliances



VIRTUAL APPLIANCE

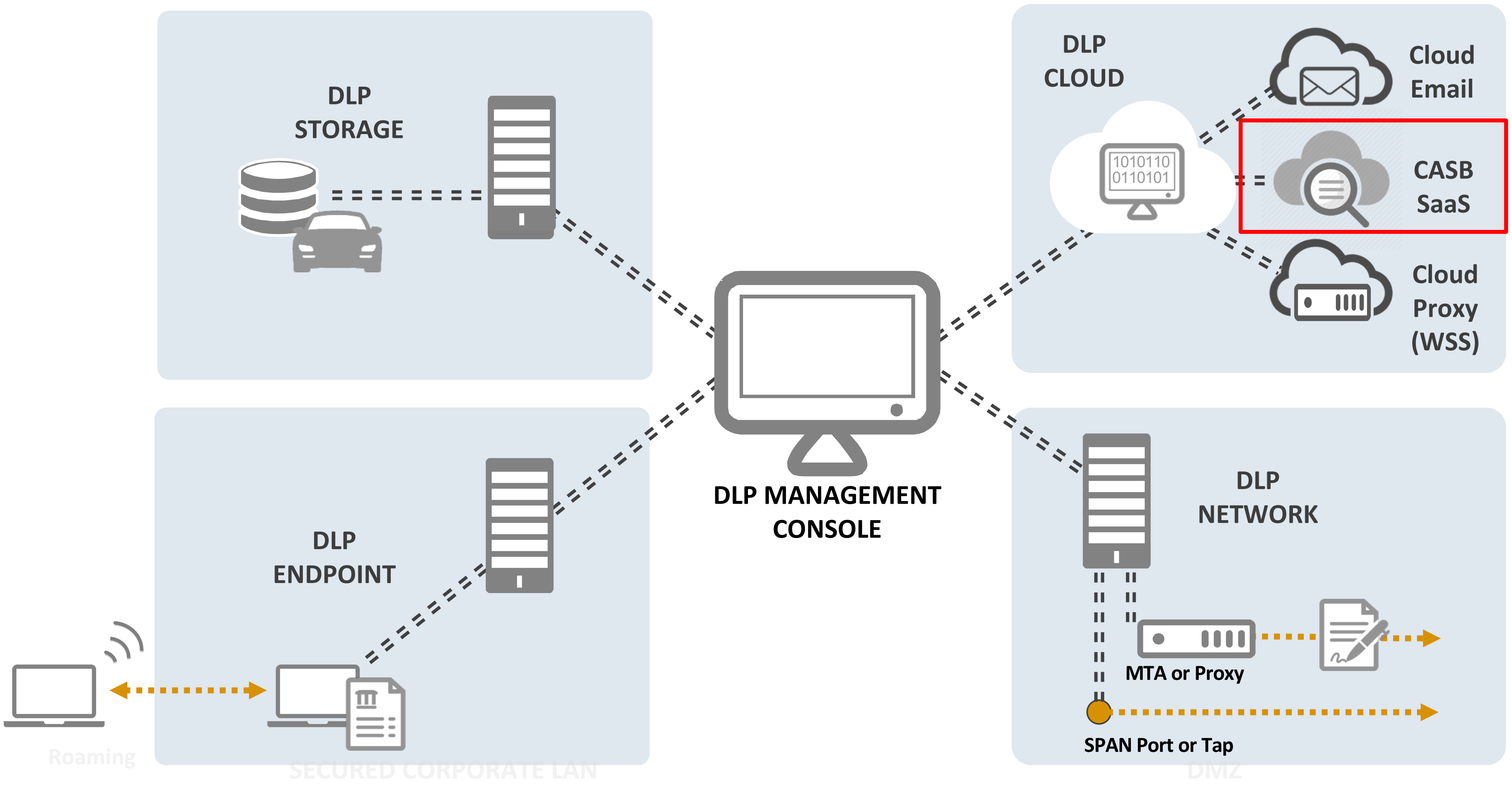
- Network Prevent for Web (ICAP)
- Network Prevent for Email (SMTP)
- API Detection for Developer Apps (REST API)

HARDWARE APPLIANCE

- Network Prevent for Web S500-10 [1]
  - 10 core
  - 64GB RAM
  - 4TB disk

[1] An upgrade kit is available for upgrading to S500-20 (20 core / 64GB RAM / 4TB disk)

DISCOVER MONITOR PROTECT



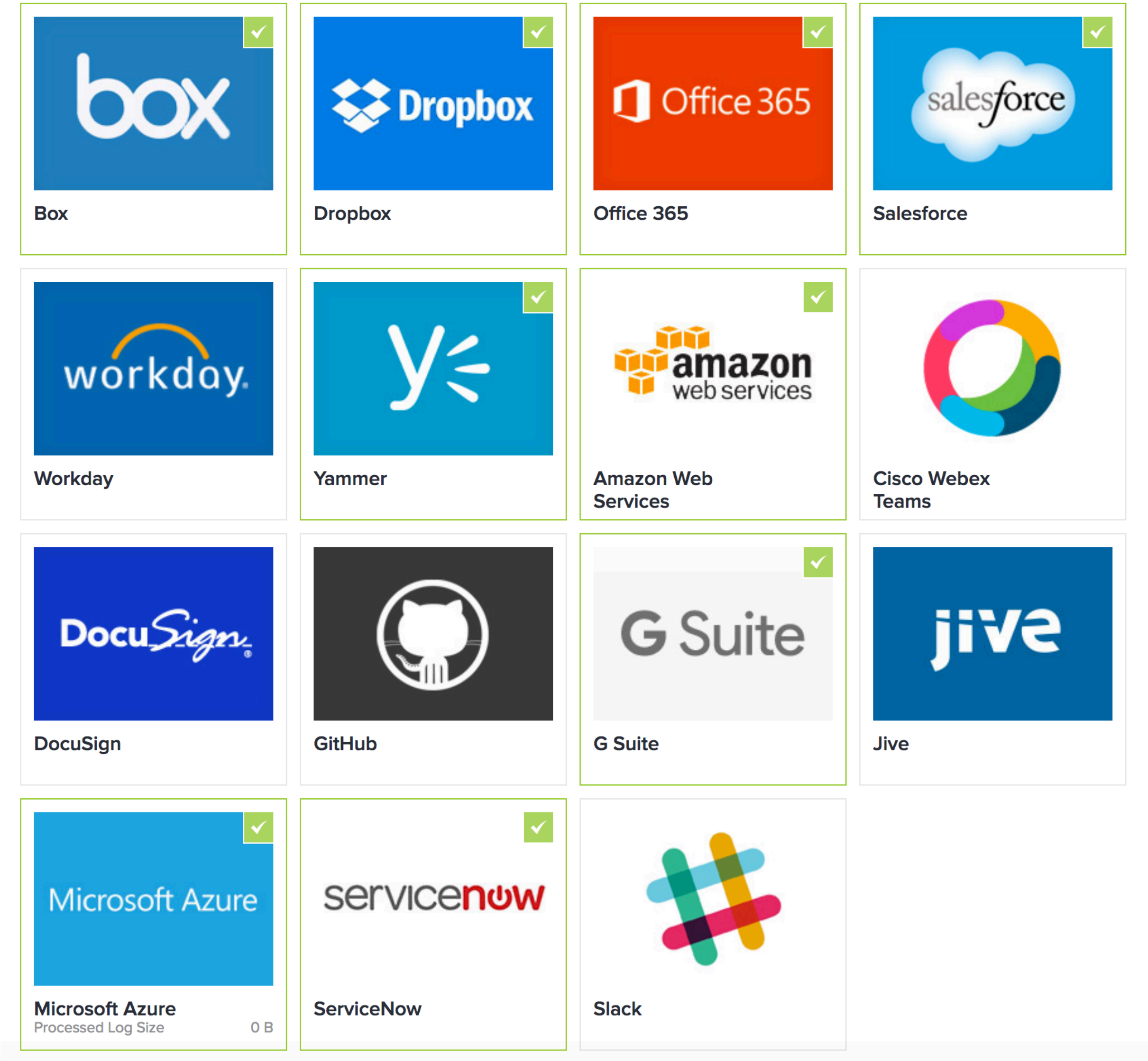
Coverage for sanctioned apps

Symantec.

API Coverage for Cloud Apps:

16+

Total



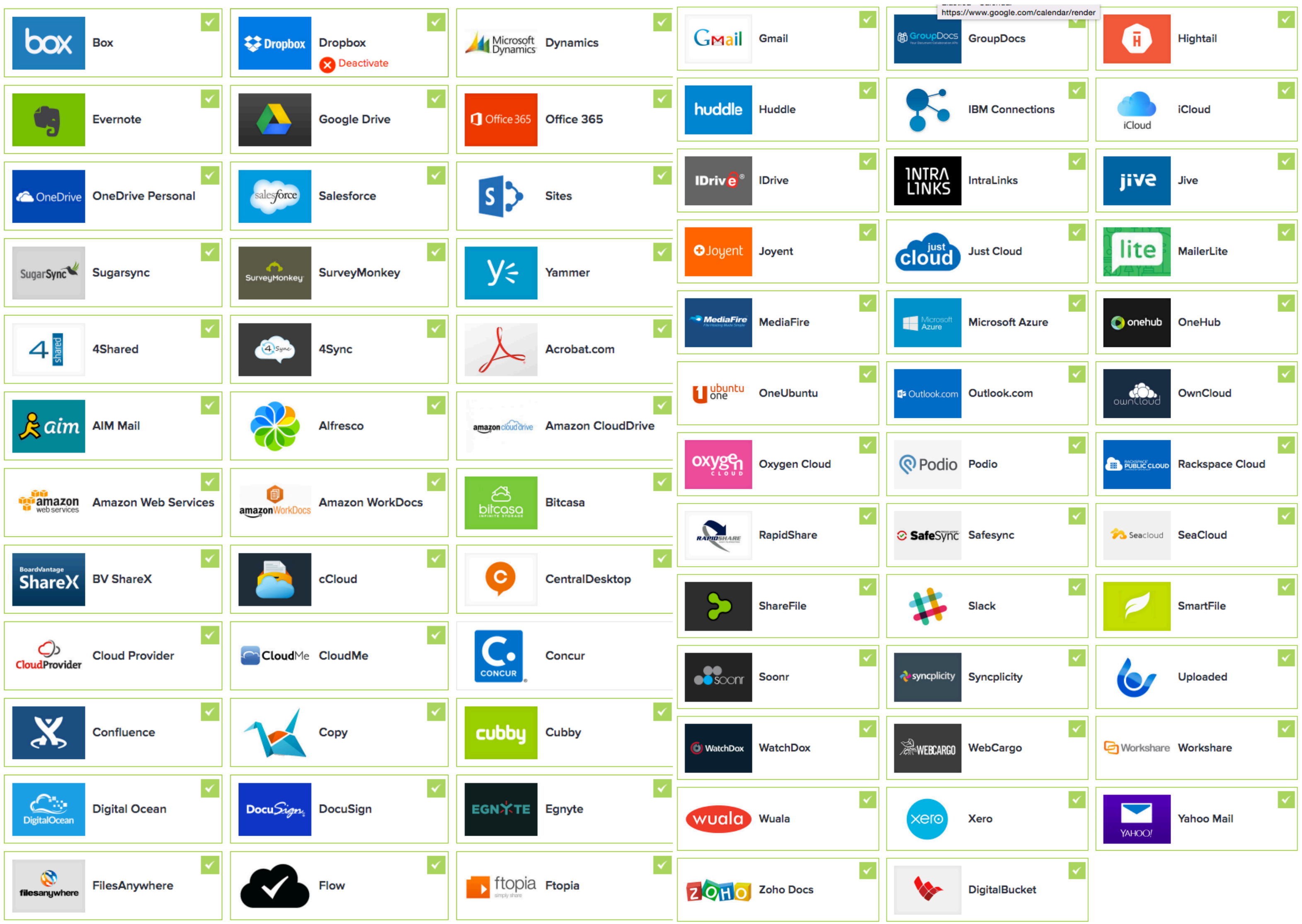
✓ Box	✓ Dropbox	✓ Office 365	✓ Salesforce
Workday	✓ Yammer	✓ Amazon Web Services	Cisco Webex Teams
DocuSign	GitHub	✓ G Suite	Jive
✓ Microsoft Azure Processed Log Size 0 B	✓ ServiceNow	Slack	

Coverage for unsanctioned apps

Gateway Coverage for Cloud Apps:

218+ 200

Total With DLP



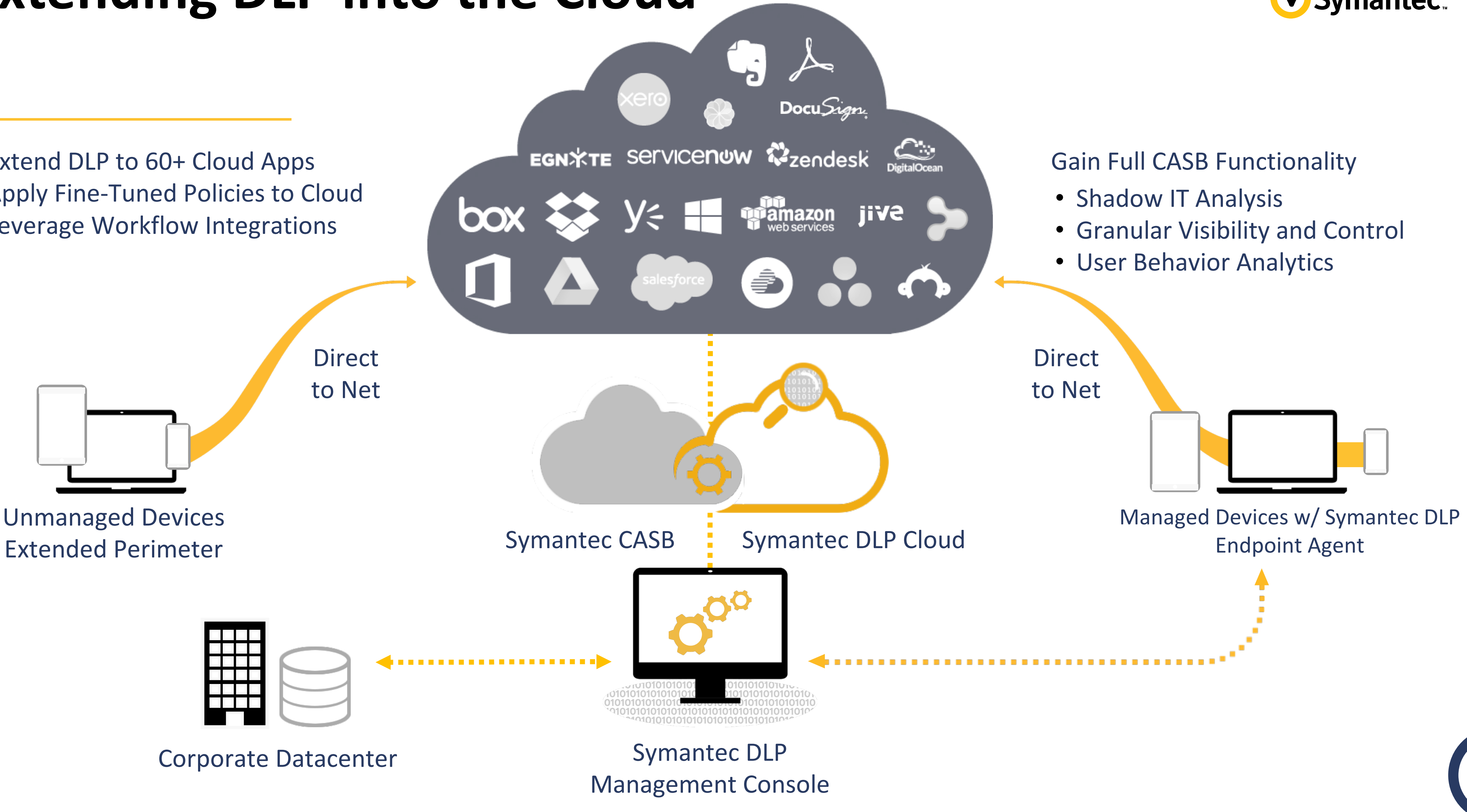
- Box ✓
- Evernote ✓
- OneDrive Personal ✓
- Sugarsync ✓
- 4Shared ✓
- AIM Mail ✓
- Amazon Web Services ✓
- BV ShareX ✓
- Cloud Provider ✓
- Confluence ✓
- Digital Ocean ✓
- FilesAnywhere ✓
- Dropbox ✓ Deactivate
- Google Drive ✓
- Salesforce ✓
- SurveyMonkey ✓
- 4Sync ✓
- Alfresco ✓
- Amazon WorkDocs ✓
- cCloud ✓
- CloudMe ✓
- Copy ✓
- DocuSign ✓
- Flow ✓
- Dynamics ✓
- Office 365 ✓
- Sites ✓
- Yammer ✓
- Acrobat.com ✓
- Amazon CloudDrive ✓
- Bitcasa ✓
- CentralDesktop ✓
- Concur ✓
- Cubby ✓
- Egnyte ✓
- Ftopia ✓
- Gmail ✓
- Huddle ✓
- IDrive ✓
- Joyent ✓
- MediaFire ✓
- OneUbuntu ✓
- Oxygen Cloud ✓
- RapidShare ✓
- ShareFile ✓
- Soonr ✓
- WatchDox ✓
- Wuala ✓
- Zoho Docs ✓
- GroupDocs ✓
- IBM Connections ✓
- IntraLinks ✓
- Just Cloud ✓
- Microsoft Azure ✓
- Outlook.com ✓
- Podio ✓
- Safesync ✓
- Slack ✓
- Syncplicity ✓
- WebCargo ✓
- Xero ✓
- DigitalBucket ✓
- Hightail ✓
- iCloud ✓
- Jive ✓
- MailerLite ✓
- OneHub ✓
- OwnCloud ✓
- Rackspace Cloud ✓
- SeaCloud ✓
- SmartFile ✓
- Uploaded ✓
- Workshare ✓
- Yahoo Mail ✓

Extending DLP into the Cloud

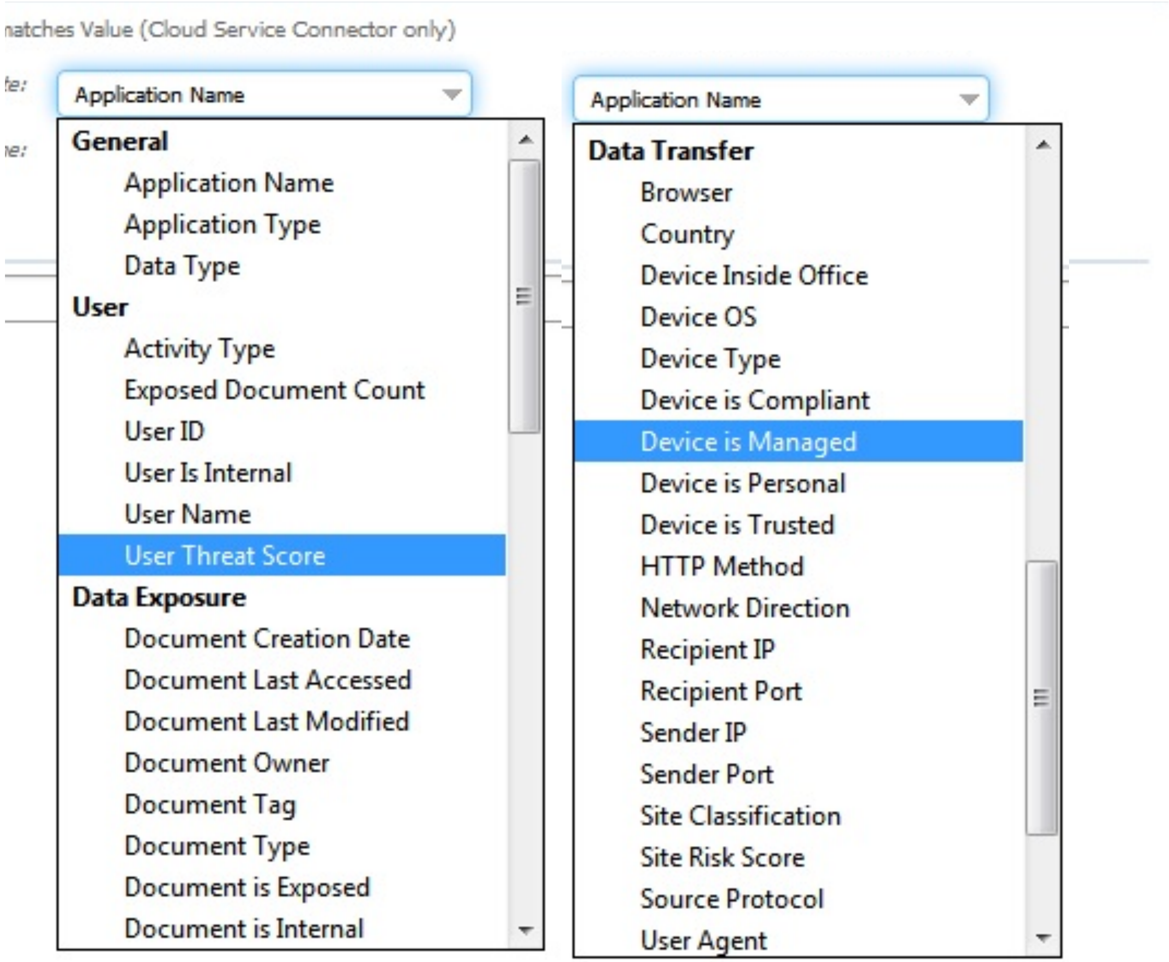
Extend DLP to 60+ Cloud Apps
Apply Fine-Tuned Policies to Cloud
Leverage Workflow Integrations

Gain Full CASB Functionality

- Shadow IT Analysis
- Granular Visibility and Control
- User Behavior Analytics

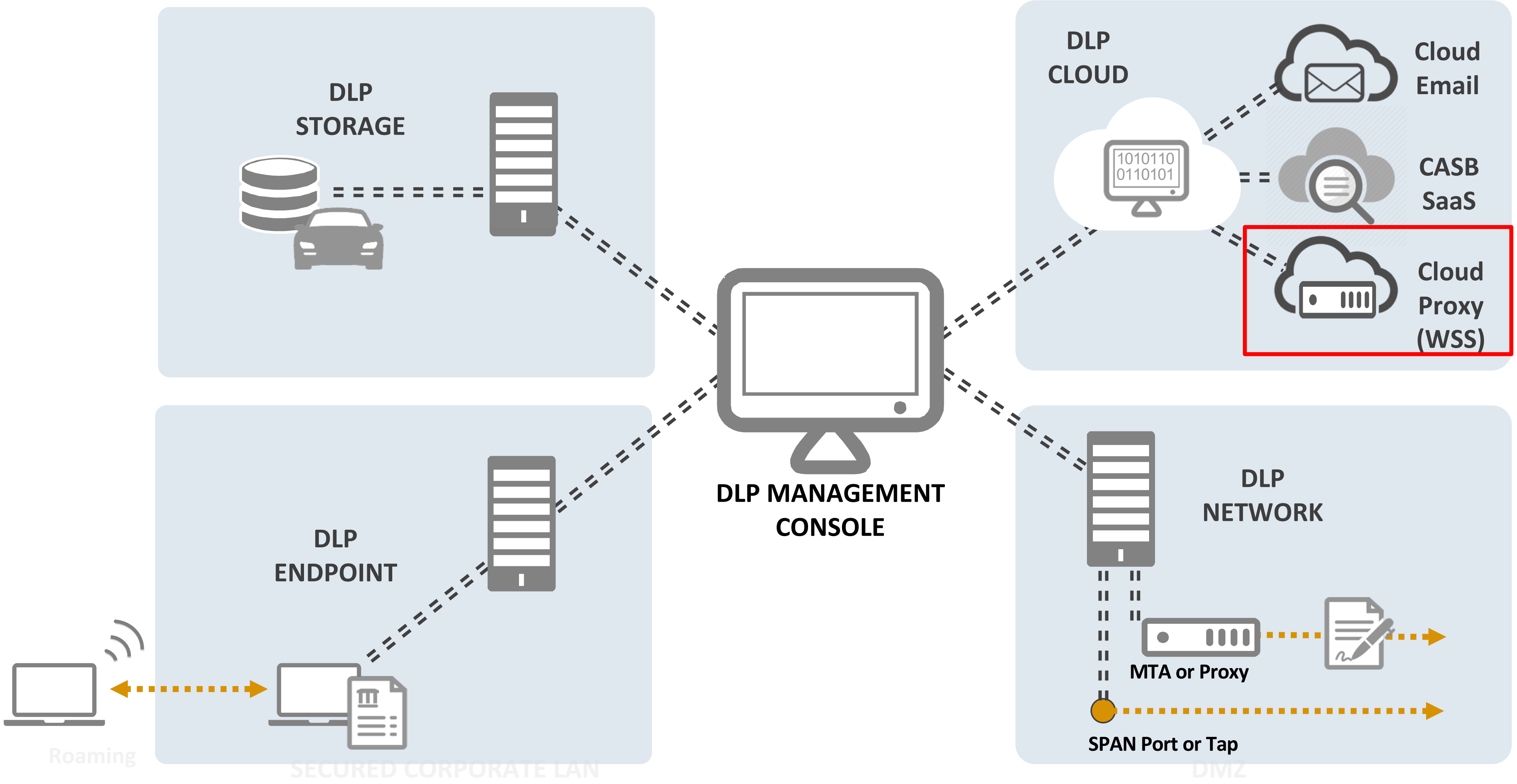


Attribute Rules based on Contextual Data from CASB



- **DLP Policy combines CASB Context with DLP Detection**
- **Rules based on 6 Contextual Dimensions:**
  - User (User Threat Score, Internal/External)
  - Region (Country/Geo-Location of the device)
  - Cloud Application (Application Name/Sanctioned)
  - Activity (Upload/Download, Sharing)
  - Device Posture (Managed/Personal)
  - Document Meta-Data (Internal/External, File Type)

DISCOVER MONITOR PROTECT



DLP STORAGE

DLP ENDPOINT

Roaming

SECURED CORPORATE LAN

DLP MANAGEMENT CONSOLE

DLP CLOUD

Cloud Email

CASB SaaS

Cloud Proxy (WSS)

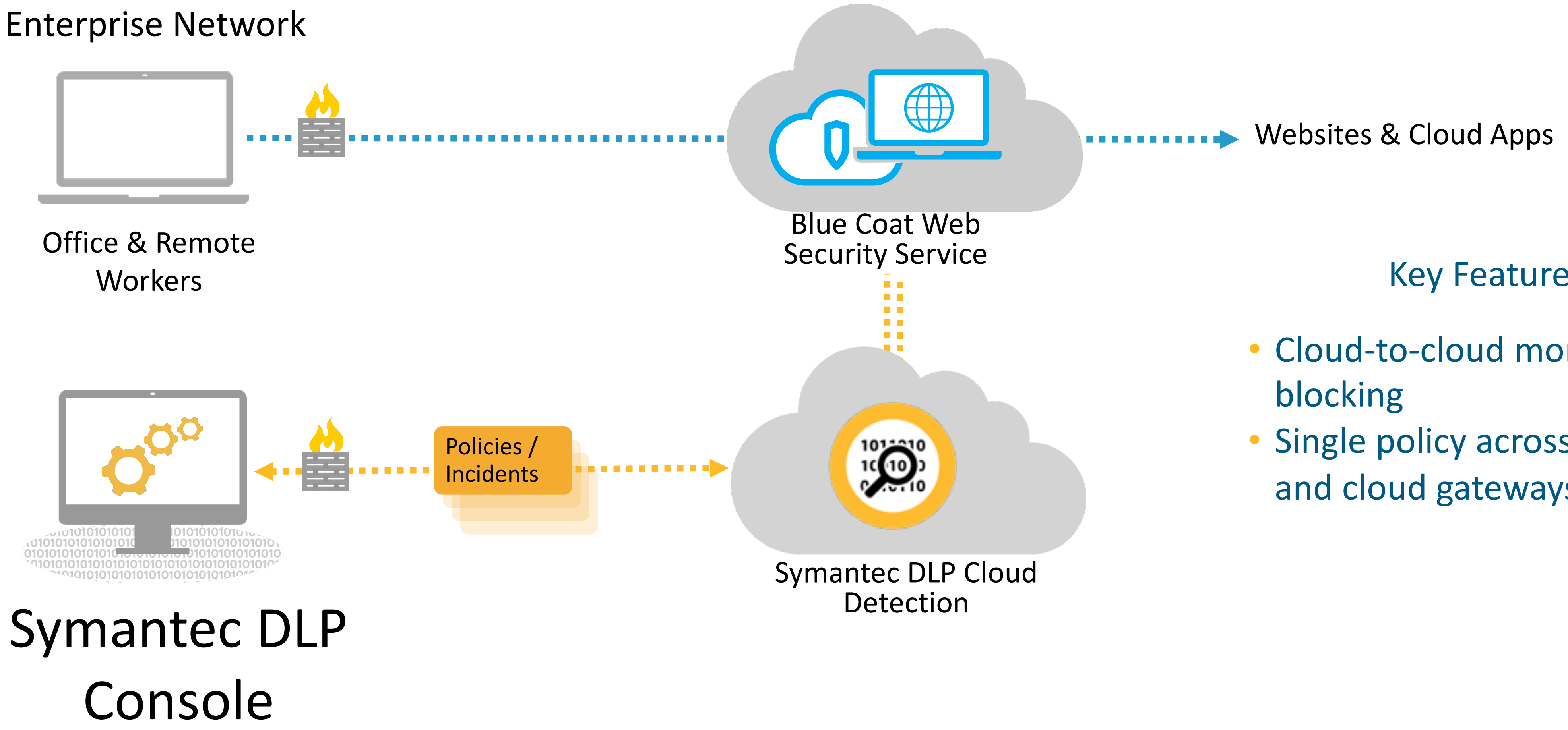
DLP NETWORK

MTA or Proxy

SPAN Port or Tap

DMZ

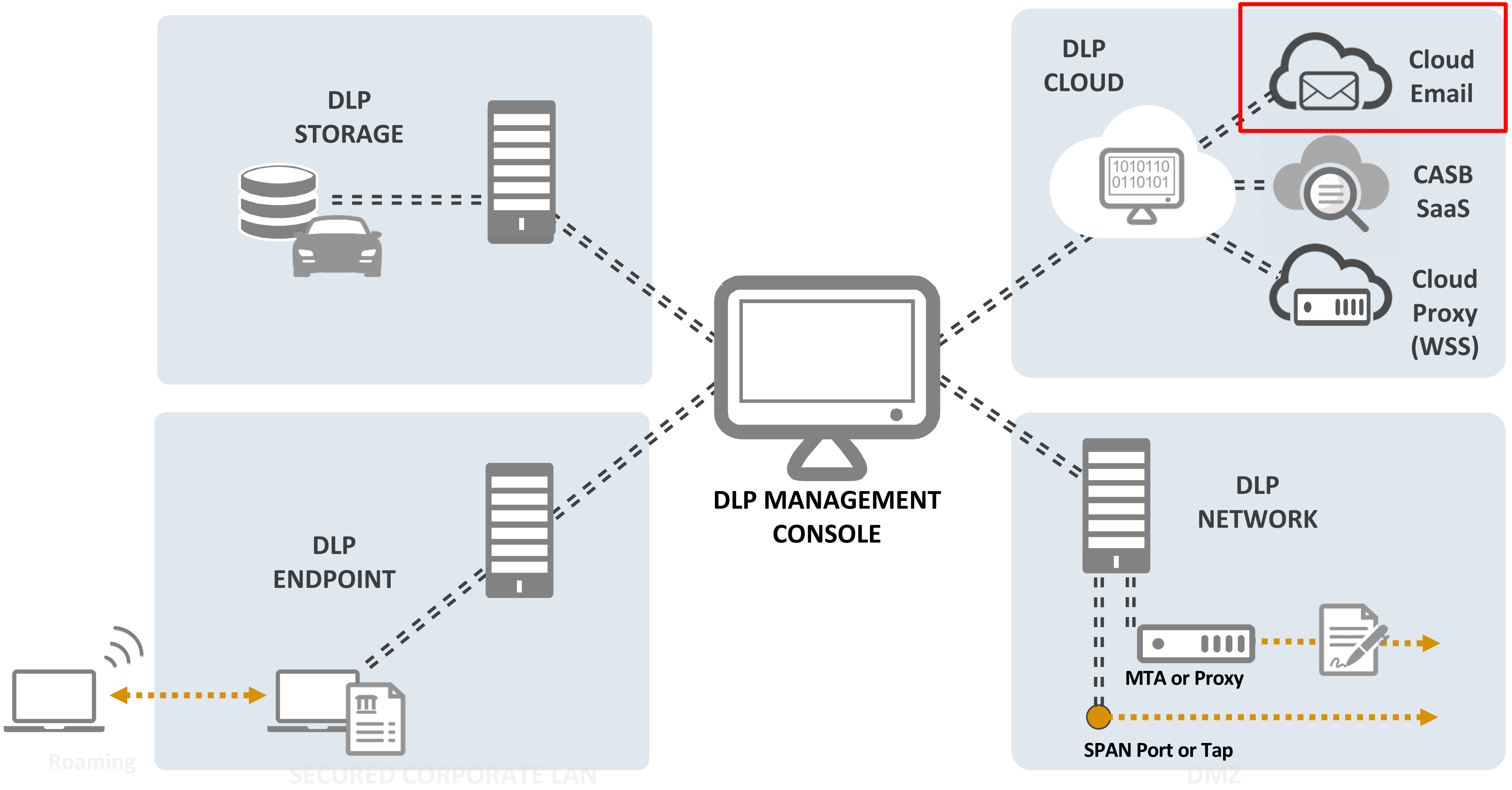
DLP + Blue Coat Web Security Service



Key Features

- Cloud-to-cloud monitoring and blocking
- Single policy across on-premises and cloud gateways

DISCOVER MONITOR PROTECT



DLP STORAGE

DLP CLOUD

Cloud Email

CASB SaaS

Cloud Proxy (WSS)

DLP MANAGEMENT CONSOLE

DLP ENDPOINT

DLP NETWORK

MTA or Proxy

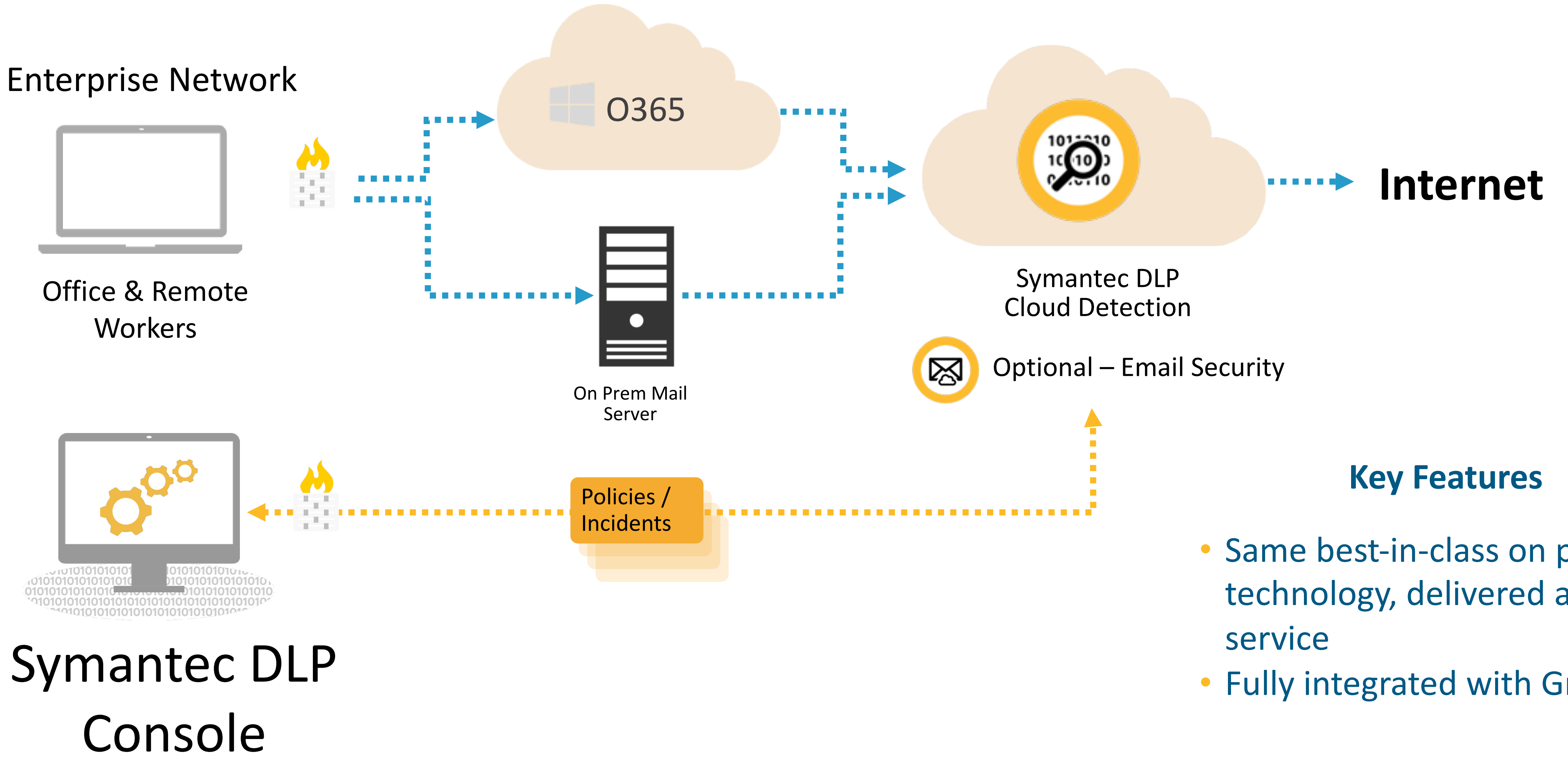
SPAN Port or Tap

Roaming

SECURED CORPORATE LAN

DMZ

DLP Cloud Service for Email



Key Features

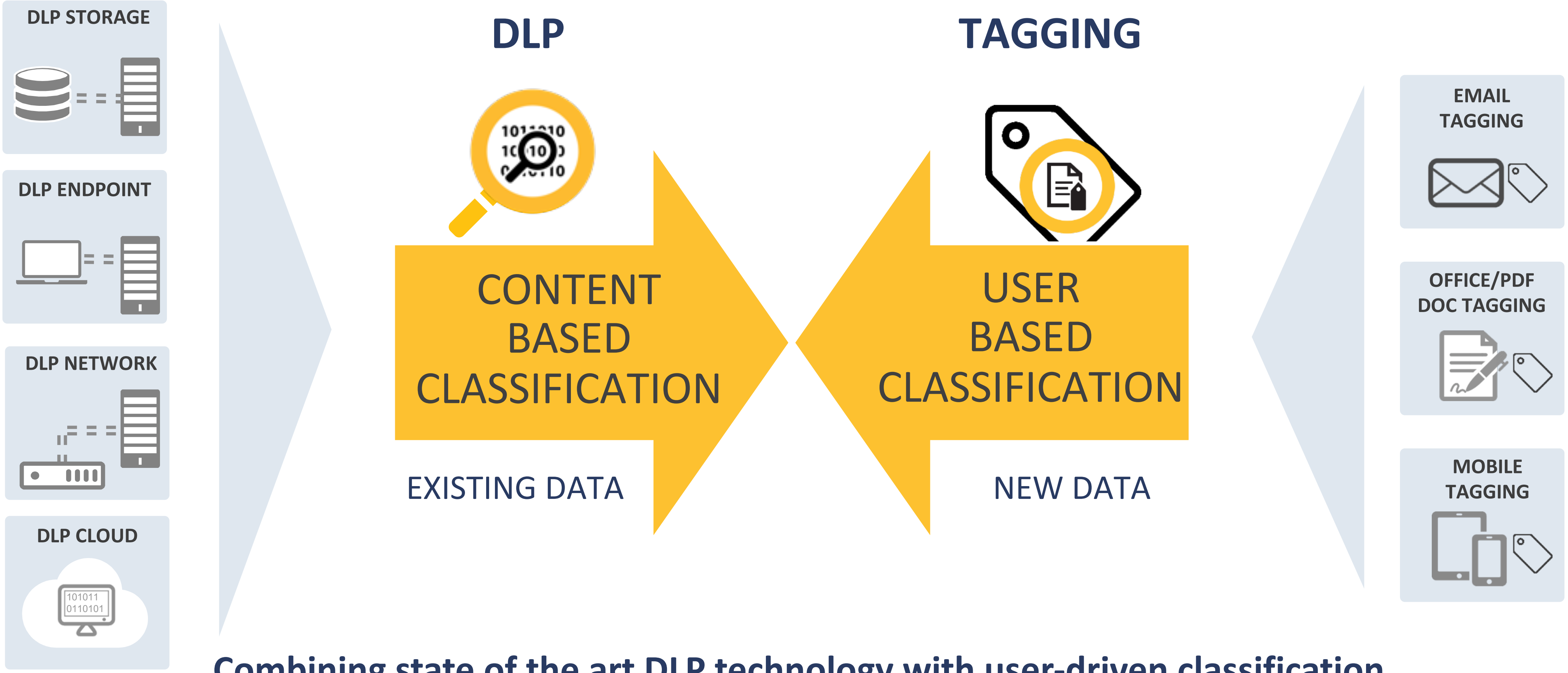
- Same best-in-class on premise technology, delivered as a cloud service
- Fully integrated with Gmail

Information Centric Security

Symantec™

Augment DLP with Data Classification

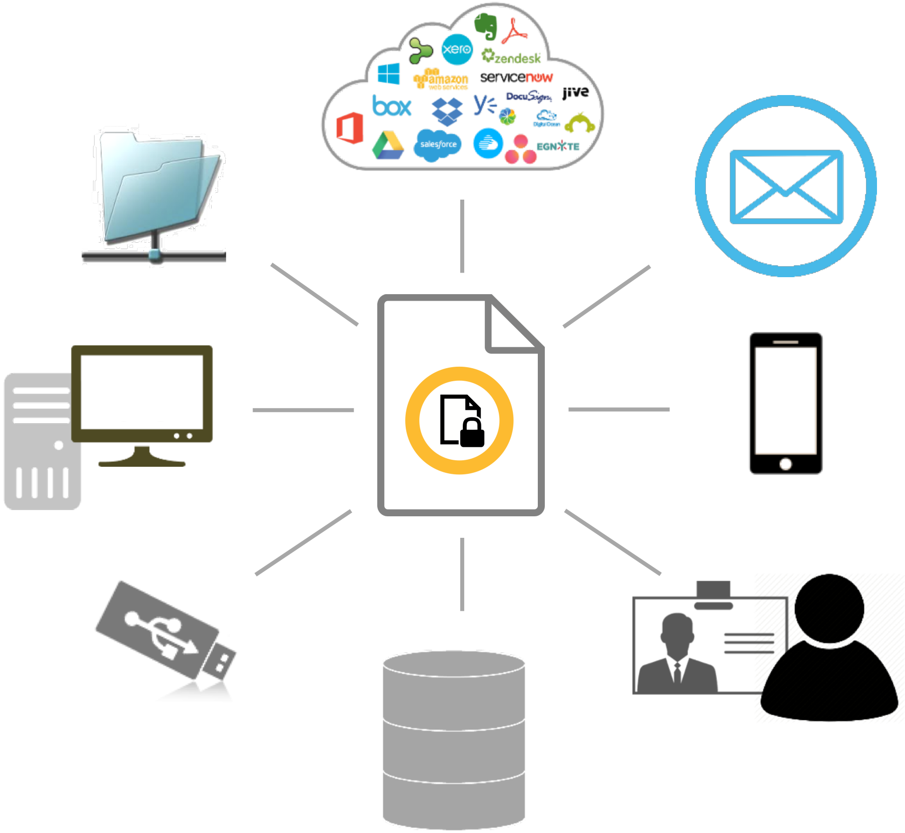
DLP with Symantec Information Centric Tagging (ICT)

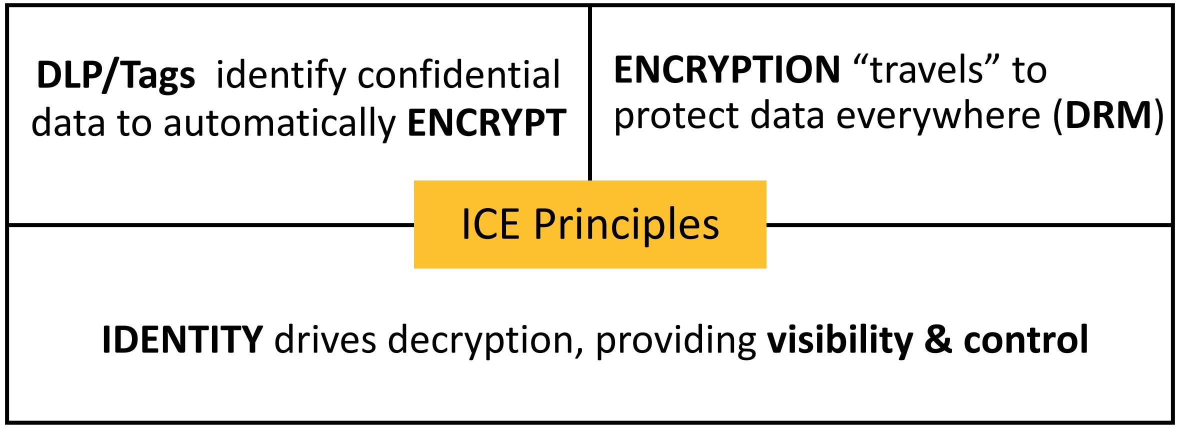


Combining state of the art DLP technology with user-driven classification to identify and protect sensitive data

Protect sensitive data when it leaves the managed channels

DLP with Information Centric Encryption (ICE)





DLP/Tags identify confidential data to automatically **ENCRYPT**

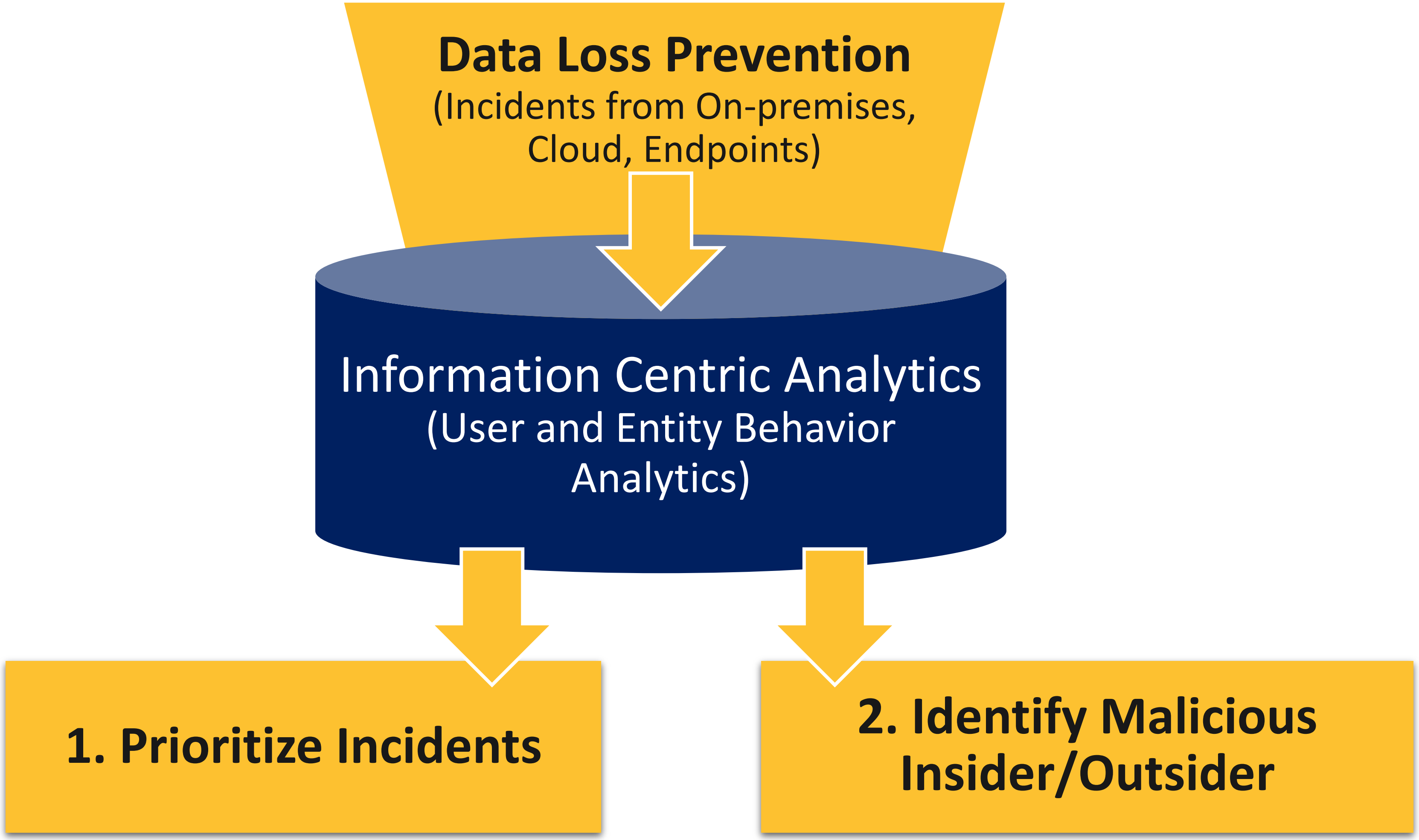
ENCRYPTION “travels” to protect data everywhere (**DRM**)

ICE Principles

IDENTITY drives decryption, providing **visibility & control**

Protects your organization’s sensitive data across its lifecycle. Integrates CASB, DLP, Encryption and Identity

Simplified Incident Management with ICA



Data Loss Prevention
(Incidents from On-premises, Cloud, Endpoints)

Information Centric Analytics
(User and Entity Behavior Analytics)

1. Prioritize Incidents

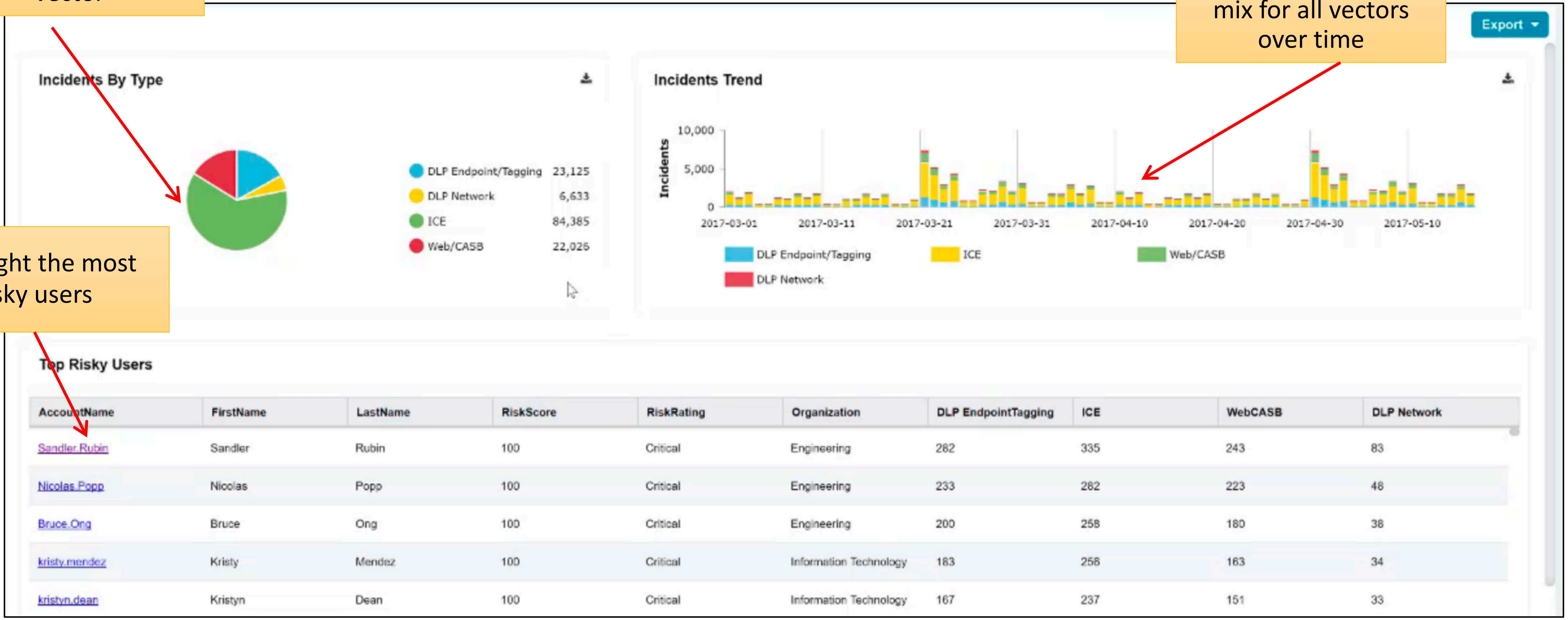
2. Identify Malicious Insider/Outsider

Risk Trends and Risky Users

Breakdown of risky behaviors by risk vector

Risk trends and risk mix for all vectors over time

Highlight the most risky users



Incidents By Type

● DLP Endpoint/Tagging	23,125
● DLP Network	6,633
● ICE	84,385
● Web/CASB	22,026

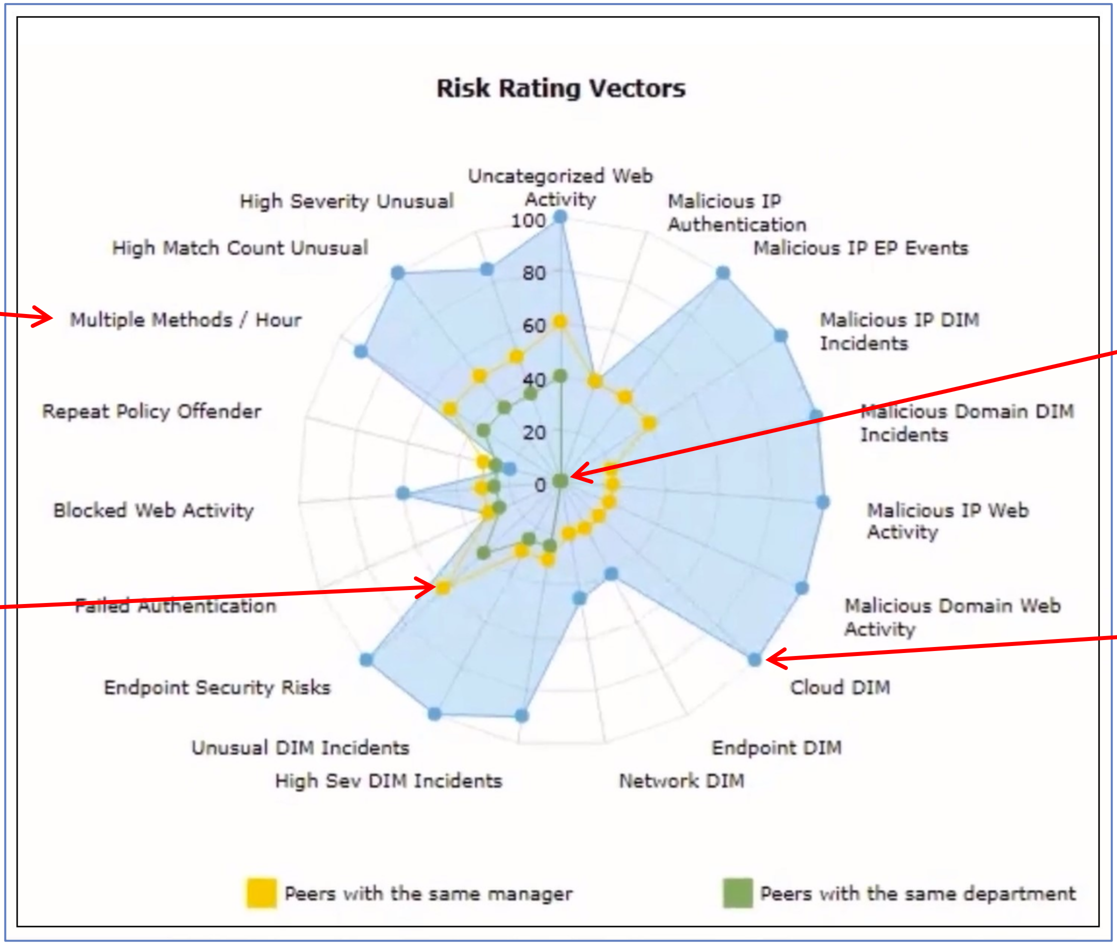
Top Risky Users

AccountName	FirstName	LastName	RiskScore	RiskRating	Organization	DLP EndpointTagging	ICE	WebCASB	DLP Network
Sandler.Rubin	Sandler	Rubin	100	Critical	Engineering	282	335	243	83
Nicolas.Popp	Nicolas	Popp	100	Critical	Engineering	233	282	223	48
Bruce.Ong	Bruce	Ong	100	Critical	Engineering	200	258	180	38
kristy.mendez	Kristy	Mendez	100	Critical	Information Technology	183	258	163	34
kristyn.dean	Kristyn	Dean	100	Critical	Information Technology	167	237	151	33

Comparative User Risk Analysis

Which Behaviors Occur

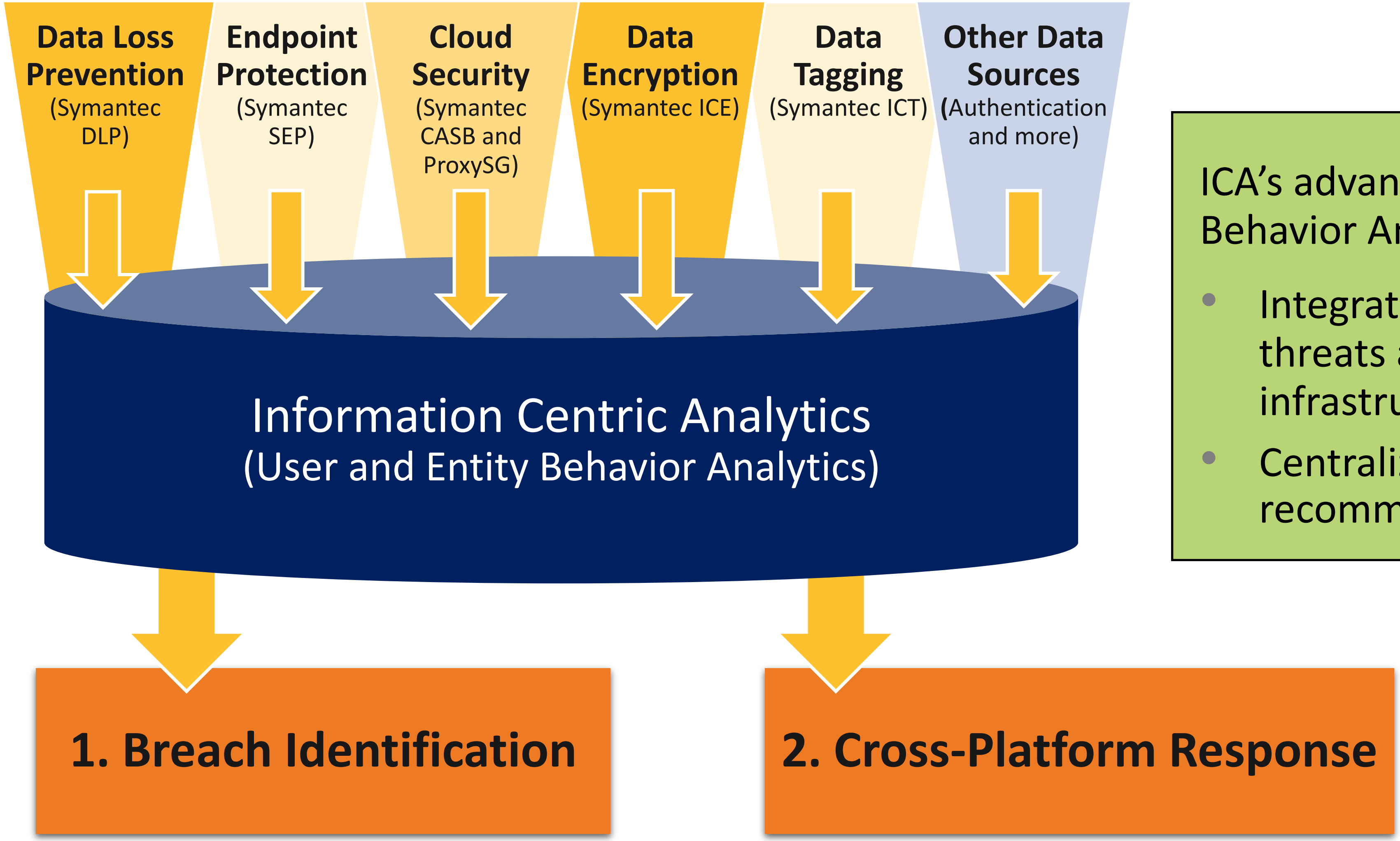
Manager Peer-based Risk Ranking



Department Peer-based Risk Ranking

100th Percentile Infractions

Centralized Visibility and Response with ICA



Data Loss Prevention (Symantec DLP)

Endpoint Protection (Symantec SEP)

Cloud Security (Symantec CASB and ProxySG)

Data Encryption (Symantec ICE)

Data Tagging (Symantec ICT)

Other Data Sources (Authentication and more)

Information Centric Analytics
(User and Entity Behavior Analytics)

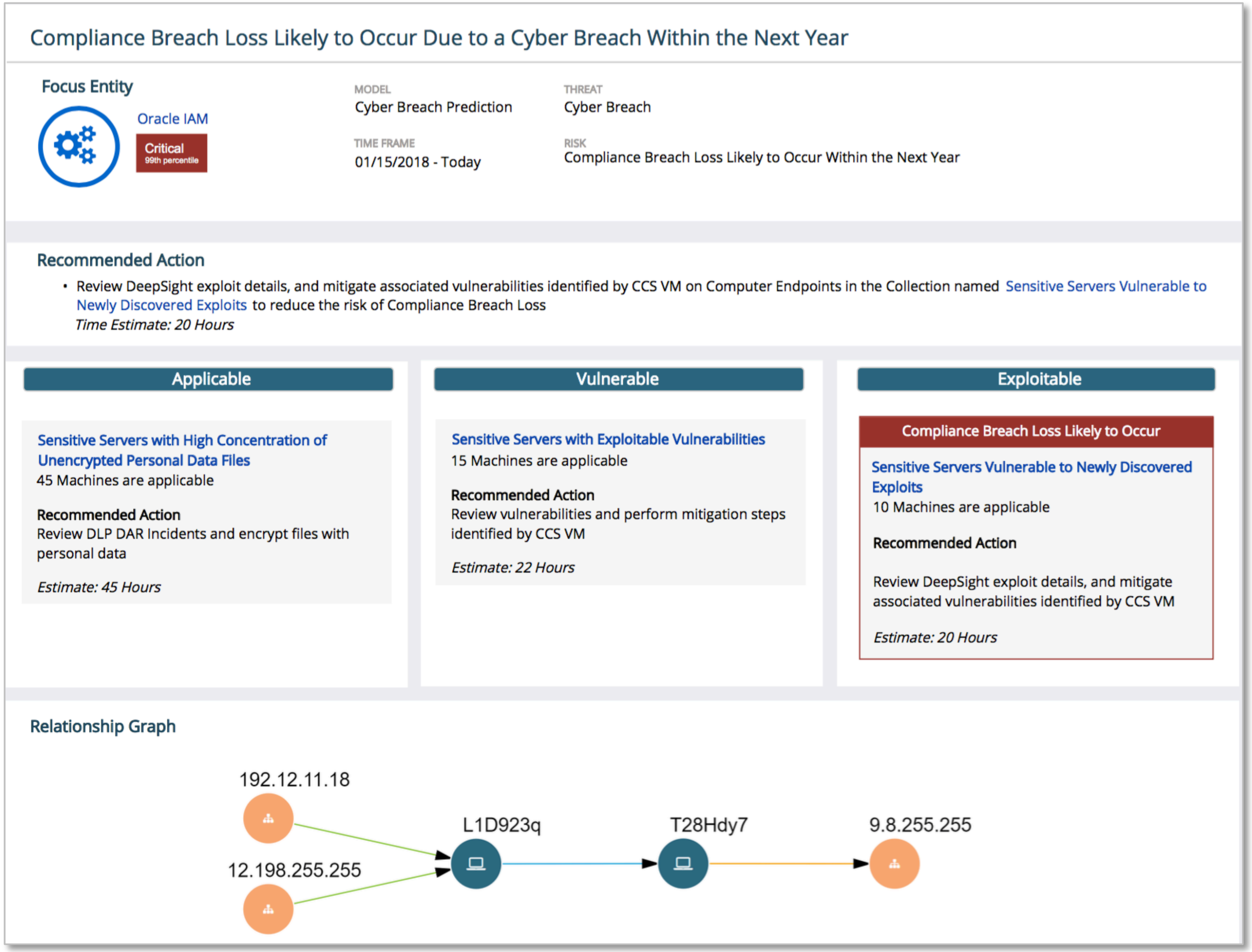
1. Breach Identification

2. Cross-Platform Response

ICA's advanced User and Entity Behavior Analytics (UEBA) provide:

- Integrated analysis of user-driven threats across security infrastructure
- Centralized visualization and recommended remediation

Cyber Breach Prediction With ICA



Compliance Breach Loss Likely to Occur Due to a Cyber Breach Within the Next Year

Focus Entity

Oracle IAM

Critical
99th percentile

MODEL
Cyber Breach Prediction

THREAT
Cyber Breach

TIME FRAME
01/15/2018 - Today

RISK
Compliance Breach Loss Likely to Occur Within the Next Year

Recommended Action

- Review DeepSight exploit details, and mitigate associated vulnerabilities identified by CCS VM on Computer Endpoints in the Collection named Sensitive Servers Vulnerable to Newly Discovered Exploits to reduce the risk of Compliance Breach Loss
  Time Estimate: 20 Hours

Applicable

Sensitive Servers with High Concentration of Unencrypted Personal Data Files
45 Machines are applicable

Recommended Action
Review DLP DAR Incidents and encrypt files with personal data

Estimate: 45 Hours

Vulnerable

Sensitive Servers with Exploitable Vulnerabilities
15 Machines are applicable

Recommended Action
Review vulnerabilities and perform mitigation steps identified by CCS VM

Estimate: 22 Hours

Exploitable

Compliance Breach Loss Likely to Occur

Sensitive Servers Vulnerable to Newly Discovered Exploits
10 Machines are applicable

Recommended Action

Review DeepSight exploit details, and mitigate associated vulnerabilities identified by CCS VM

Estimate: 20 Hours

Relationship Graph

Roadmap!

Symantec™

FORWARD LOOKING STATEMENTS

This presentation contains statements which may be considered forward-looking within the meaning of the U.S. federal securities laws, including statements regarding our projected financial and business results, the expected benefits to Symantec, its customers, stockholders and investors from completing the acquisition of Blue Coat, Inc. ("Blue Coat"), including without limitation expected growth, cross-sell and upsell opportunities, earnings accretion and cost savings, statements regarding the share repurchase program and cost reduction efforts, statements regarding Symantec's planned capital return program, and statements regarding leadership changes in connection with the acquisition and investments and the potential benefits to be derived therefrom.

These statements are subject to known and unknown risks, uncertainties and other factors that may cause our actual results, performance or achievements to differ materially from results expressed or implied in this presentation. Such risk factors include those related to: the potential impact on the businesses of Blue Coat and Symantec due to uncertainties in connection with the acquisition; the retention of employees of Blue Coat and the ability of Symantec to successfully integrate Blue Coat and to achieve expected benefits; general economic conditions; fluctuations and volatility in Symantec's stock price; the ability of Symantec to successfully execute strategic plans; the ability to maintain customer and partner relationships; fluctuations in tax rates and currency exchange rates; the timing and market acceptance of new product releases and upgrades; and the successful development of new products, and the degree to which these products and businesses gain market acceptance. Actual results may differ materially from those contained in the forward-looking statements in this press release. Symantec assumes no obligation, and do not intend, to update these forward-looking statements as a result of future events or developments. Additional information concerning these and other risks factors is contained in the Risk Factors section of Symantec's Form 10-K for the year ended April 1, 2016.

Any information regarding pre-release of 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.

We assume no obligation to update any forward-looking information contained in this presentation.

What's New in Data Loss Prevention 15.5

DLP - SEP Integration

SEP Intensive Protection

Protection based on reputation

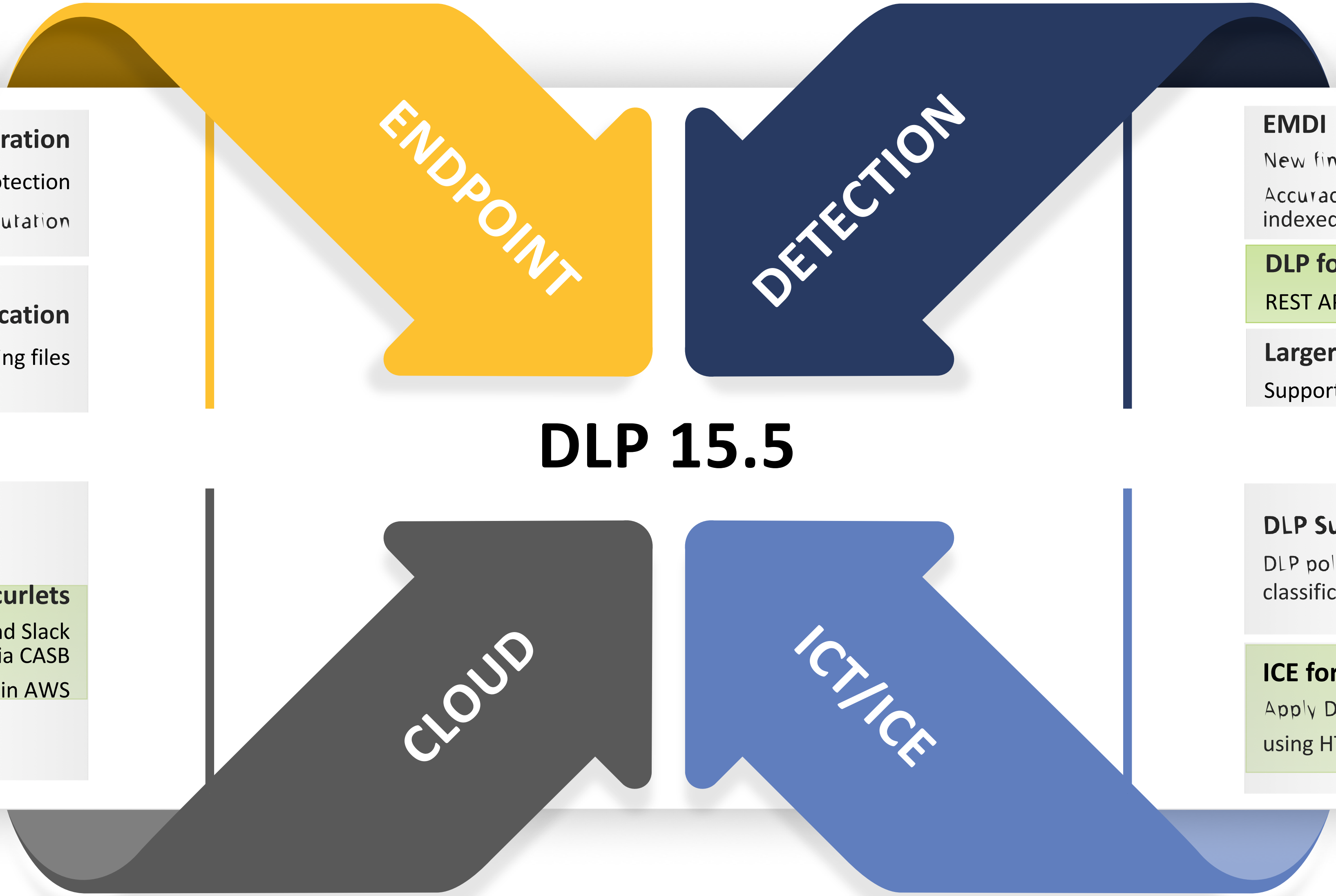
Automatic Classification

DLP classifies existing files

Added Securlets

Support for Amazon S3, Spark, and Slack via CASB

Oracle RDS support in AWS



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

DLP 15.7 | 2H2019 (Planned)
Simplification and Integration – Customer Satisfaction

Symantec.

DLP-ICT

- Classifying existing data on file shares and Sharepoint
- Integrated IP Agent (DLP + ICT)
- ICT manageability improvements

DLP Cloud Service

- First class support of Slack, Cisco Spark and Amazon S3 w/CloudSOC
- Email quarantine integration with ESS

DLP

- Grid scanning: Stats added to give better performance visibility
- Enforce: AD group mapped to Enforce roles
- Oracle: 12c RAC / PDB/CDB
- Chrome for Enforce
- TCP/TLS support for Syslog response rule

DLP-ICE

- DLP Insight - Ability to inspect and apply DLP response rules on ICE encrypted files on endpoints, file-shares and emails

User Driven Encryption

- Enabling users to encrypt files and emails, specify permissions and add authorize recipients

Content updates

- New out-of-the-box Data Identifiers
- Updating and adding new policy templates

DLP 16.0 | 1H2020 (Concept Phase)

DLP-ICT integration

- Console integration

Simplified DLP management (2HCY2019)

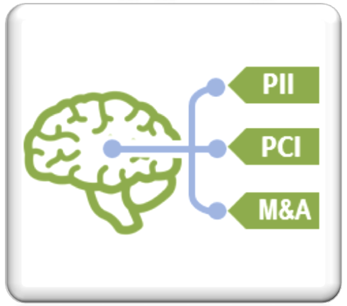
- End use remediation for Discover
- Self Service
- Integrated with ServiceNow
- Update Endpoint from Enforce *(via Cloud Endpoint Gateway – CY2020)*

DLP – ICE Integration

- Expanded channel support for ICE Insight
- User driven Encryption v2 (Mac)

Malicious Activity Monitoring

- Record activities
- Discover anomalous behavior
- Investigate users



Automatic data classification

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

Increased DLP speed & scale

- Larger Files
- Faster detection
- Improved UX

Symantec™

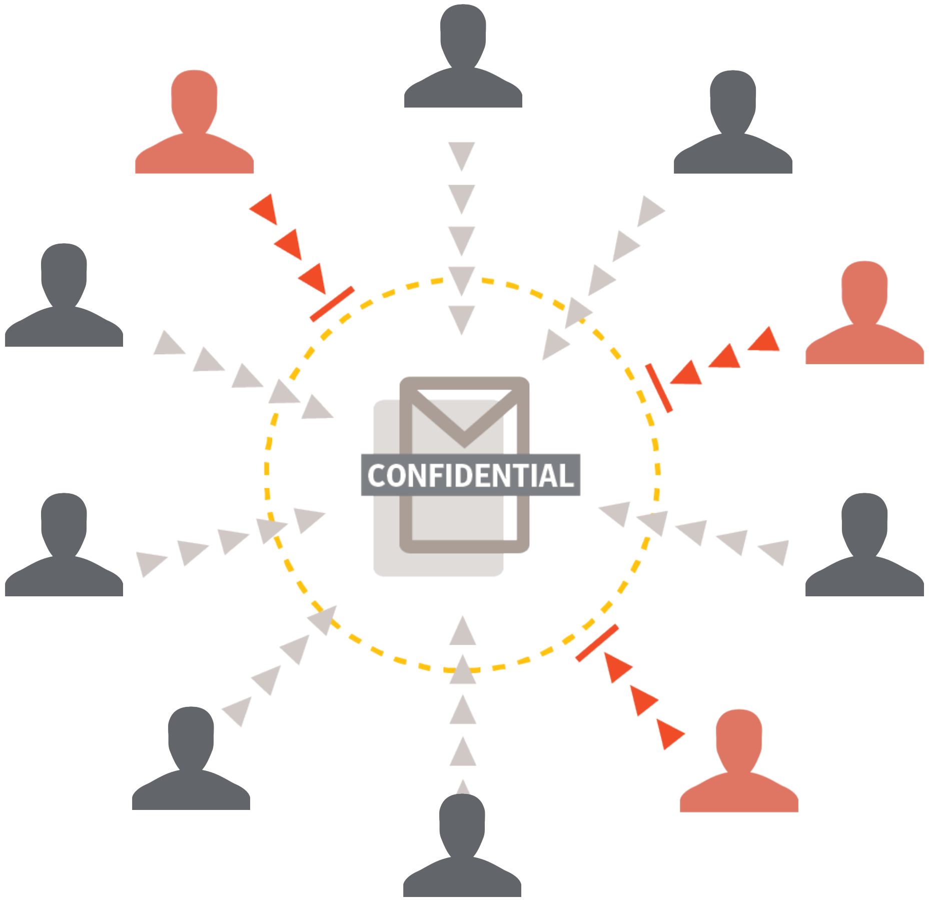
Thank You!

Symantec Data Loss Prevention Data Access Governance

Protecting Your Information and Reputation

Risks to Shared Sensitive Data

Lack of visibility and excessive exposure



- Data residing in multiple places
- Excessive Access and Complex Entitlements
- Unknown Threats in the Midst
- Compliance Requirements

The Need for Data Access Governance

Symantec.

Lack of Visibility into User Privileges and Data Access Activities

Malicious / Inappropriate User Access Behavior

How do I monitor and control high-risk user access behavior around sensitive data?

- More unstructured data is being created by users than can be easily governed by security teams, making it vulnerable to loss and theft
- Compliance mandates such as GDPR, PCI, HIPAA require evidence of data security governance policies and controls
- Data loss incidents are difficult to remediate due to potentially inaccurate and unreliable file metadata

Symantec DLP Data Access Governance

Least privileged access model reduces data loss and compliance risks

USER ACCESS, PERMISSIONS & ACTIVITY MONITORING

Who has access to data?

What are they doing with it?

What level of access do do they have?

MONITOR USER ACTIVITY & IDENTIFY TOXIC "OPEN ACCESS" CONDITIONS

DATA DISCOVERY, CLASSIFICATION & GOVERNANCE

Where does data reside?

Which files have sensitive content?

Who owns the data?

Who can make decisions about it?

DISCOVER SENSITIVE DATA & IDENTIFY PROBABLE OWNERS

DATA CLEANUP & ACCESS TRANSFORMATION

Is the data stale or outdated?

Is it still needed by the business?

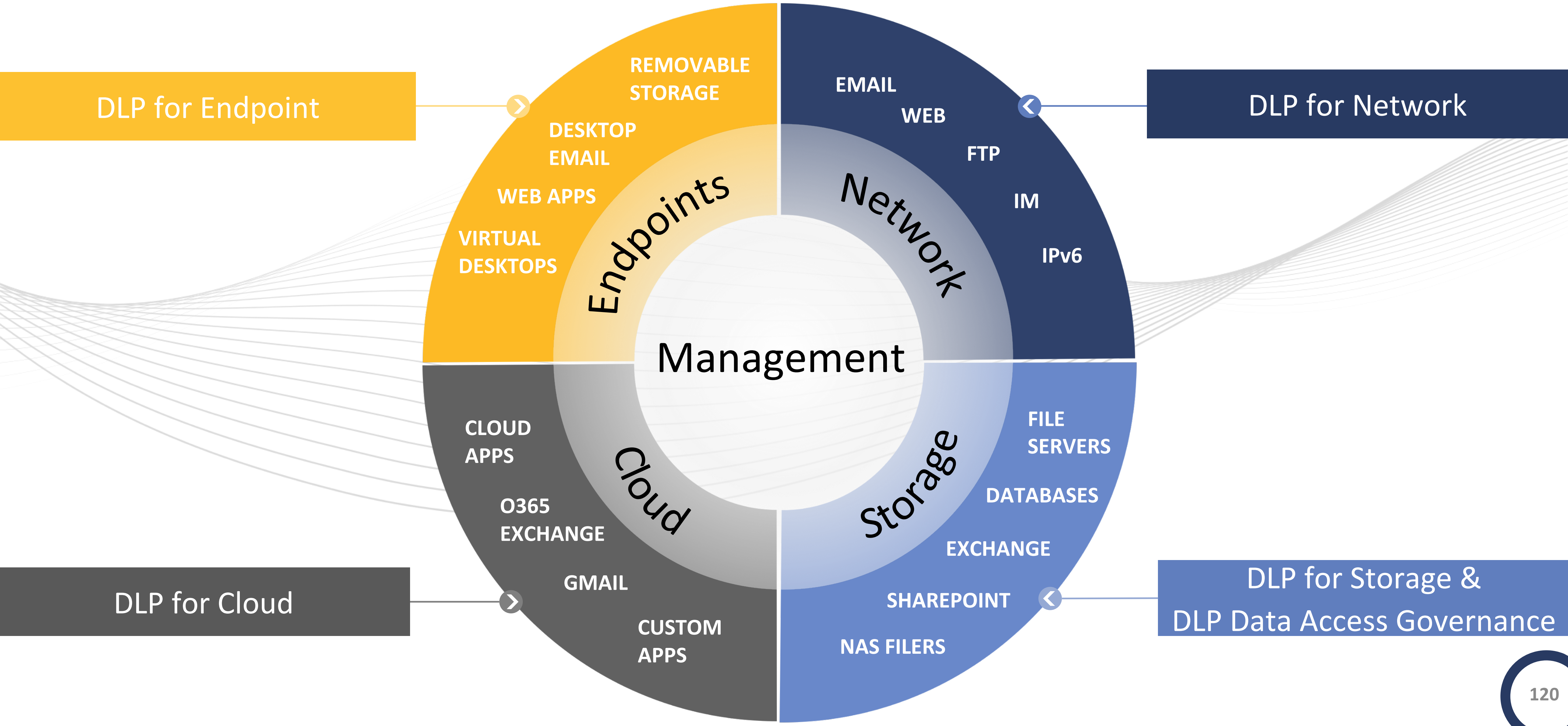
How do I assign least privilege access?

MANAGE STALE RESOURCES & RESTRUCTURE ACCESS PRIVILEGES

Limits the number of users who have access to data and reduces privileges to the lowest levels possible.

Symantec Data Loss Prevention

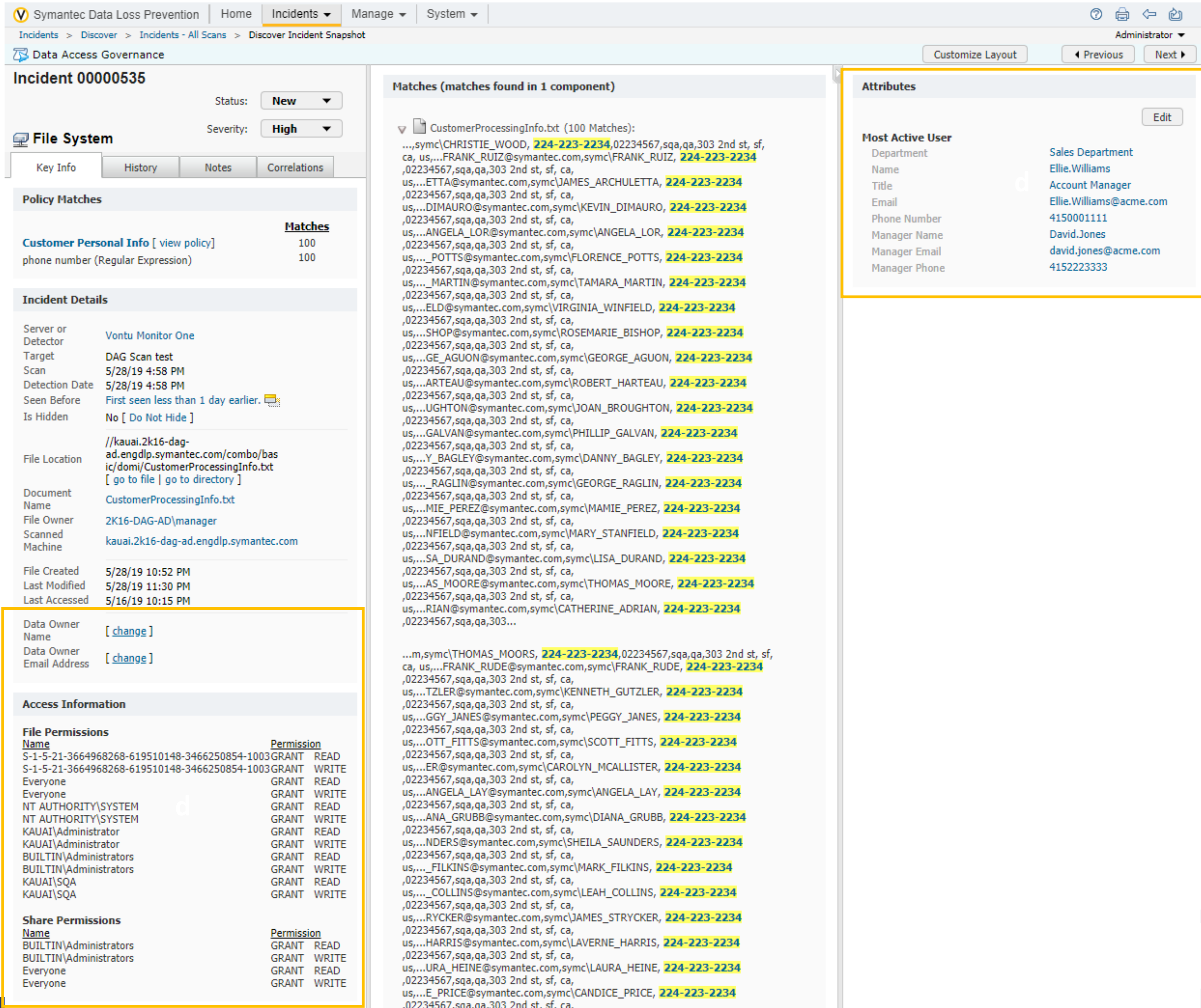
Symantec



DLP Enforce Console with Data Access Governance

In the DLP data policy incident view it provides file information including:

- owner name, email, phone #, manager name, phone #, etc.
- most active users for the file that generated a policy incident



Symantec Data Loss Prevention
Home
Incidents
Manage
System
Administrator
Incidents > Discover > Incidents - All Scans > Discover Incident Snapshot
Data Access Governance
Customize Layout
Previous
Next

Incident 00000535

Status: New

Severity: High

File System

Policy Matches

	Matches
Customer Personal Info [view policy]	100
phone number (Regular Expression)	100

Incident Details

Server or Detector	Vontu Monitor One
Target	DAG Scan test
Scan	5/28/19 4:58 PM
Detection Date	5/28/19 4:58 PM
Seen Before	First seen less than 1 day earlier.
Is Hidden	No [Do Not Hide]
File Location	//kauai.2k16-dag-ad.engdlp.symantec.com/combo/basic/domi/CustomerProcessingInfo.txt [go to file | go to directory]
Document Name	CustomerProcessingInfo.txt
File Owner	2K16-DAG-AD\manager
Scanned Machine	kauai.2k16-dag-ad.engdlp.symantec.com
File Created	5/28/19 10:52 PM
Last Modified	5/28/19 11:30 PM
Last Accessed	5/16/19 10:15 PM
Data Owner Name	[change]
Data Owner Email Address	[change]

Access Information

File Permissions

Name	Permission	
S-1-5-21-3664968268-619510148-3466250854-1003	GRANT	READ
S-1-5-21-3664968268-619510148-3466250854-1003	GRANT	WRITE
Everyone	GRANT	READ
Everyone	GRANT	WRITE
NT AUTHORITY\SYSTEM	GRANT	READ
NT AUTHORITY\SYSTEM	GRANT	WRITE
KAUAI\Administrator	GRANT	READ
KAUAI\Administrator	GRANT	WRITE
BUILTIN\Administrators	GRANT	READ
BUILTIN\Administrators	GRANT	WRITE
KAUAI\SQA	GRANT	READ
KAUAI\SQA	GRANT	WRITE

Share Permissions

Name	Permission	
BUILTIN\Administrators	GRANT	READ
BUILTIN\Administrators	GRANT	WRITE
Everyone	GRANT	READ
Everyone	GRANT	WRITE

Matches (matches found in 1 component)

```
CustomerProcessingInfo.txt (100 Matches):
...,symc\CHRISTIE_WOOD, 224-223-2234,02234567,sqa,qa,303 2nd st, sf,
ca, us,...FRANK_RUIZ@symantec.com,symc\FRANK_RUIZ, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ETTA@symantec.com,symc\JAMES_ARCHULETTA, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...DIMAURO@symantec.com,symc\KEVIN_DIMAURO, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ANGELA_LOR@symantec.com,symc\ANGELA_LOR, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,..._POTTS@symantec.com,symc\FLORENCE_POTTS, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,..._MARTIN@symantec.com,symc\TAMARA_MARTIN, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ELD@symantec.com,symc\VIRGINIA_WINFIELD, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...SHOP@symantec.com,symc\ROSEMARIE_BISHOP, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...GE_AGUON@symantec.com,symc\GEORGE_AGUON, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ARTEAU@symantec.com,symc\ROBERT_HARTEAU, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...UGHTON@symantec.com,symc\JOAN_BROUGHTON, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...GALVAN@symantec.com,symc\PHILLIP_GALVAN, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...Y_BAGLEY@symantec.com,symc\DANNY_BAGLEY, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,..._RAGLIN@symantec.com,symc\GEORGE_RAGLIN, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...MIE_PEREZ@symantec.com,symc\MAMIE_PEREZ, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...NFIELD@symantec.com,symc\MARY_STANFIELD, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...SA_DURAND@symantec.com,symc\LISA_DURAND, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...AS_MOORE@symantec.com,symc\THOMAS_MOORE, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...RIAN@symantec.com,symc\CATHERINE_ADRIAN, 224-223-2234
,02234567,sqa,qa,303...

...m,symc\THOMAS_MOORS, 224-223-2234,02234567,sqa,qa,303 2nd st, sf,
ca, us,...FRANK_RUDE@symantec.com,symc\FRANK_RUDE, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...TZLER@symantec.com,symc\KENNETH_GUTZLER, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...GGY_JANES@symantec.com,symc\PEGGY_JANES, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...OTT_FITTS@symantec.com,symc\SCOTT_FITTS, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ER@symantec.com,symc\CAROLYN_MCALLISTER, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ANGELA_LAY@symantec.com,symc\ANGELA_LAY, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...ANA_GRUBB@symantec.com,symc\DIANA_GRUBB, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...NDERS@symantec.com,symc\SHEILA_SAUNDERS, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,..._FILKINS@symantec.com,symc\MARK_FILKINS, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,..._COLLINS@symantec.com,symc\LEAH_COLLINS, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...RYCKER@symantec.com,symc\JAMES_STRYCKER, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...HARRIS@symantec.com,symc\LAVERNE_HARRIS, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...URA_HEINE@symantec.com,symc\LAURA_HEINE, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
us,...E_PRICE@symantec.com,symc\CANDICE_PRICE, 224-223-2234
,02234567,sqa,qa,303 2nd st, sf, ca,
```

Attributes

Most Active User

Department	Sales Department
Name	Ellie.Williams
Title	Account Manager
Email	Ellie.Williams@acme.com
Phone Number	4150001111
Manager Name	David.Jones
Manager Email	david.jones@acme.com
Manager Phone	4152223333

Respond Faster

By knowing who owns the data

Monitor file access and usage

Monitor file access and usage

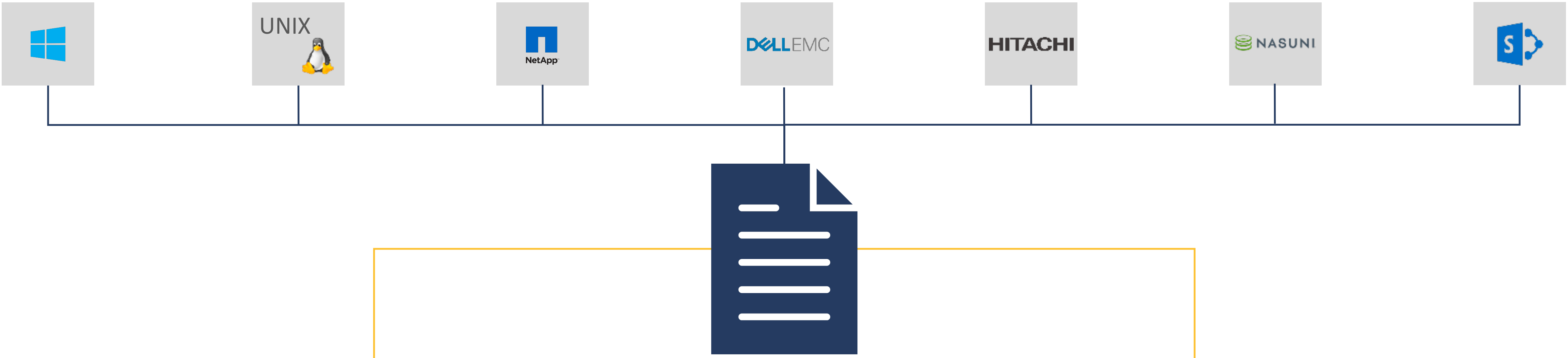
Identify true data owners

Identify true data owners

Data Access Governance – How?

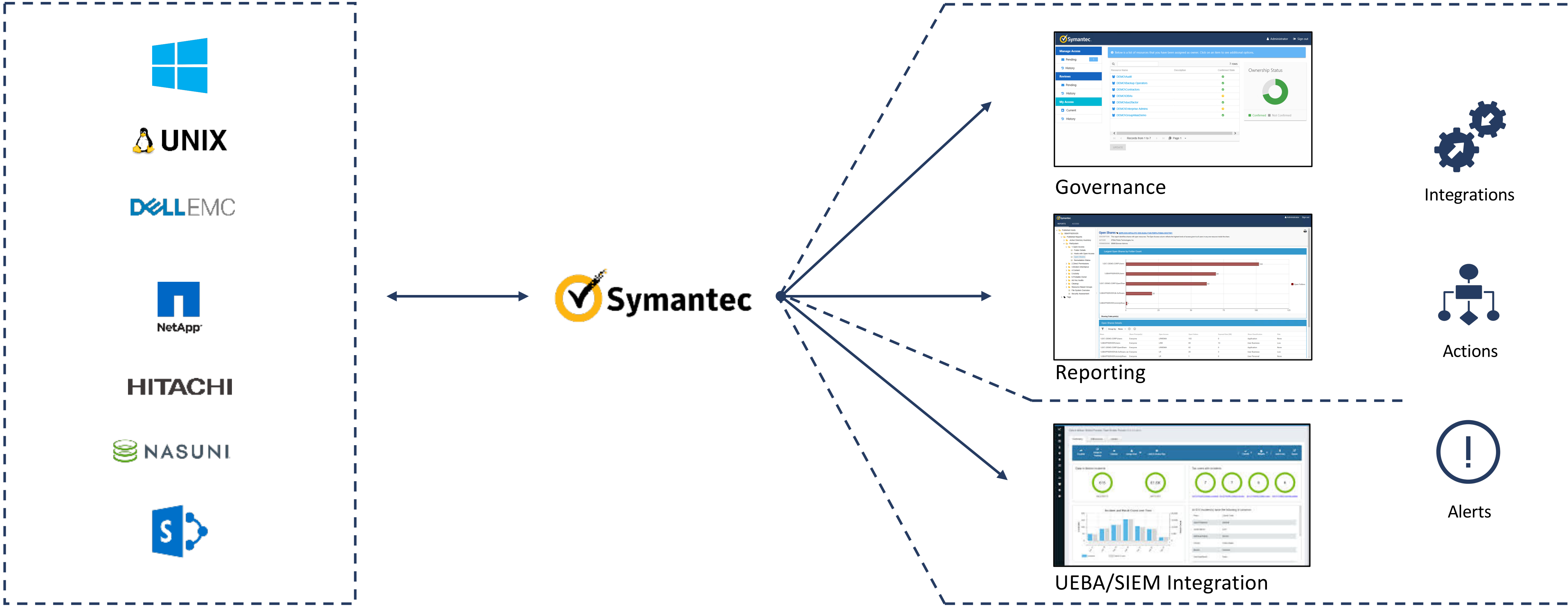
01 DISCOVER	02 COLLECT & ANALYZE	03 MONITOR	04 RESTRUCTURE	05 GOVERN
Discover where data lives to obtain a complete view of your data footprint.	**Collect & Analyze** relevant data points to answer critical questions (e.g. sensitivity, access, ownership, age, etc.)	**Monitor** activity to understand user interactions with data	**Restructure** access to achieve Least Privilege principles and position for effective governance	**Govern** access ongoing to ensure security, compliance, and operational standards are met

Supported Platforms

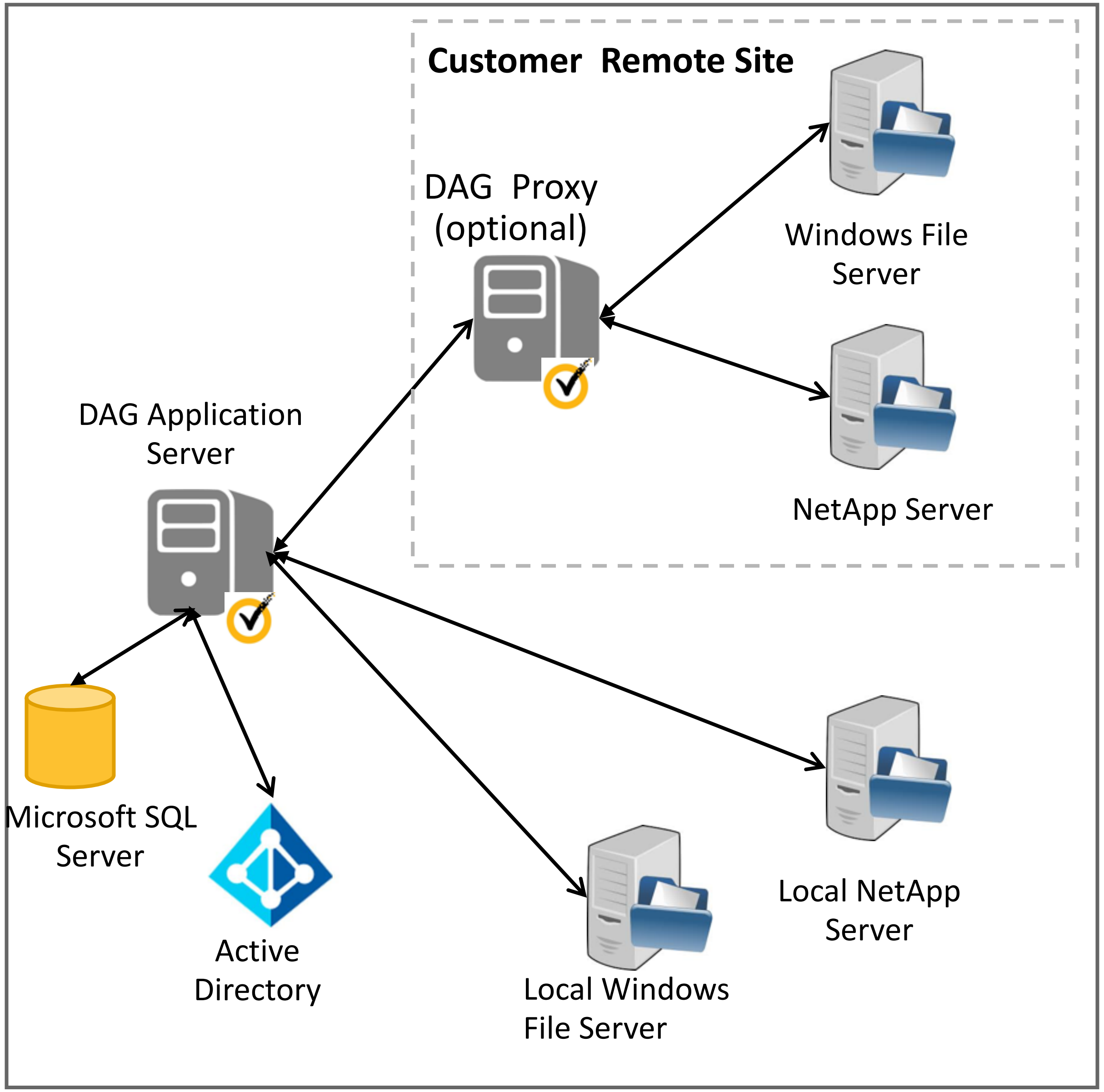


Windows File Servers
Unix/Linux File Systems
Network Attached Storage (NAS) Devices
Microsoft SharePoint

Symantec DLP Data Access Governance Architecture

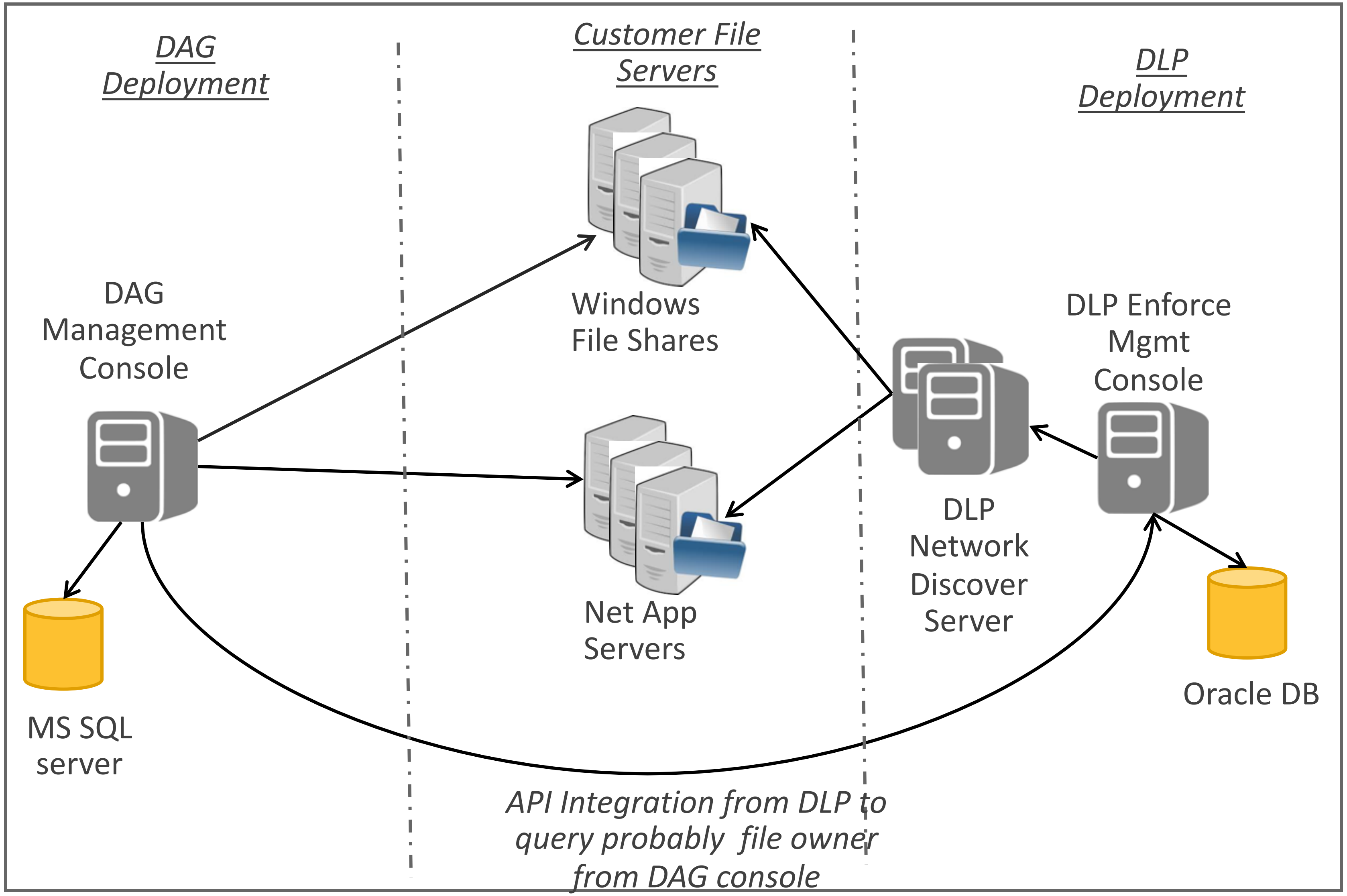


DLP Data Access Governance Deployment Architecture

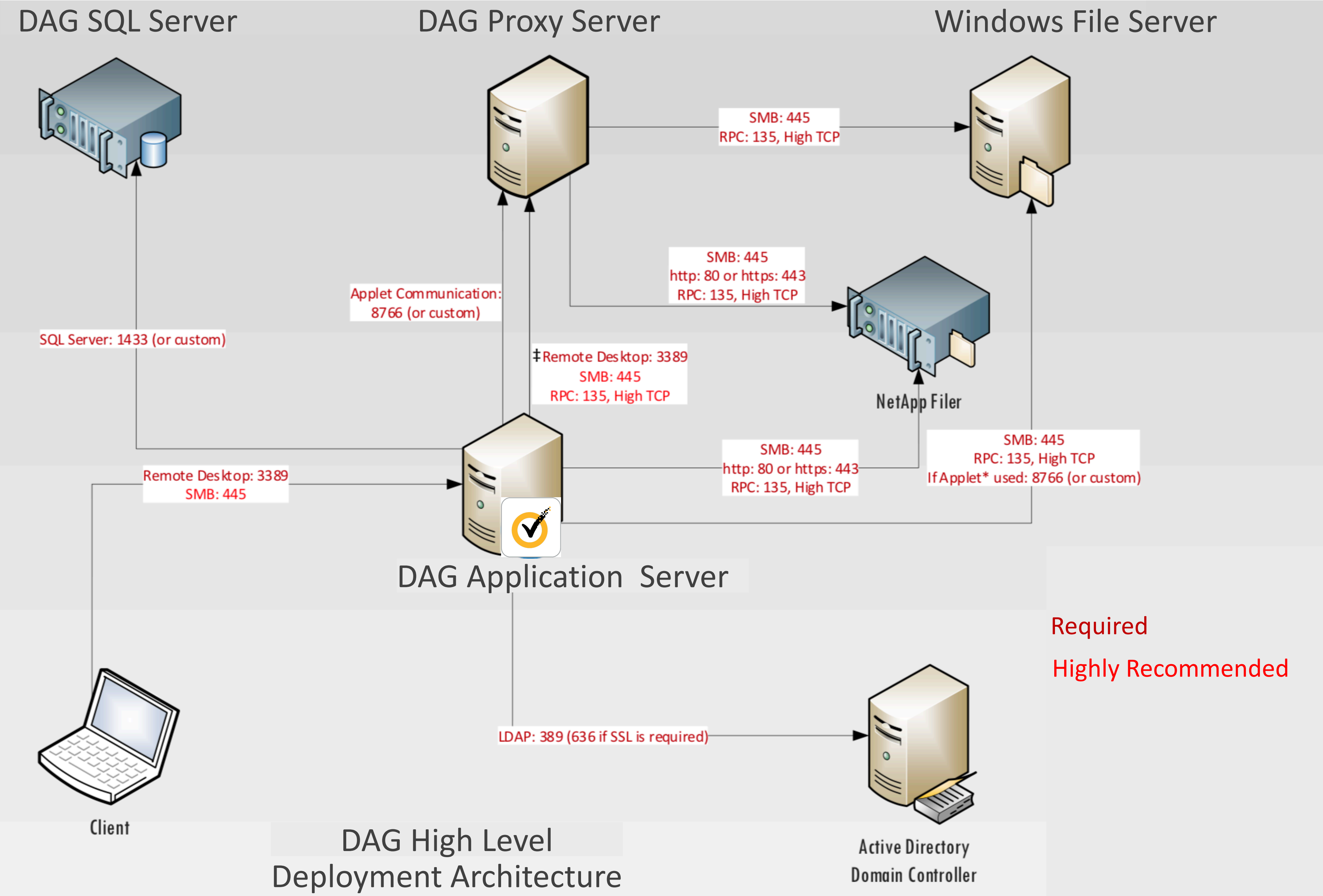


- Platform
  - Windows Based Application Server
  - Microsoft SQL Server for data/configuration storage
  - Windows based ‘Proxy servers’ as data relays
    - Go across network boundaries to remote sites
- On-premise deployment

DAG/DLP Integration Architecture at a Customer Site



1. DAG scans customer file servers and collects permissions and activity history, including probable file owner info in its SQL server
2. DLP scans customer file servers and reports files that violate DLP policies in its Enforce Mgmt Console as DLP incidents
3. DLP Enforce queries DAG Mgmt Console on Inferred File Owners for each file that violates DLP policies



DAG SQL Server

DAG Proxy Server

Windows File Server

SMB: 445
RPC: 135, High TCP

SMB: 445
http: 80 or https: 443
RPC: 135, High TCP

Applet Communication:
8766 (or custom)

SQL Server: 1433 (or custom)

‡Remote Desktop: 3389
SMB: 445
RPC: 135, High TCP

NetApp Filer

SMB: 445
http: 80 or https: 443
RPC: 135, High TCP

SMB: 445
RPC: 135, High TCP
If Applet* used: 8766 (or custom)

Remote Desktop: 3389
SMB: 445

DAG Application Server

Required

Highly Recommended

LDAP: 389 (636 if SSL is required)

Client

Active Directory
Domain Controller

DAG High Level
Deployment Architecture

Thank You!