Data Loss Prevention Partner Training

Patrick Duffey
Federal Account Manager
7 August 2018

Symantec™

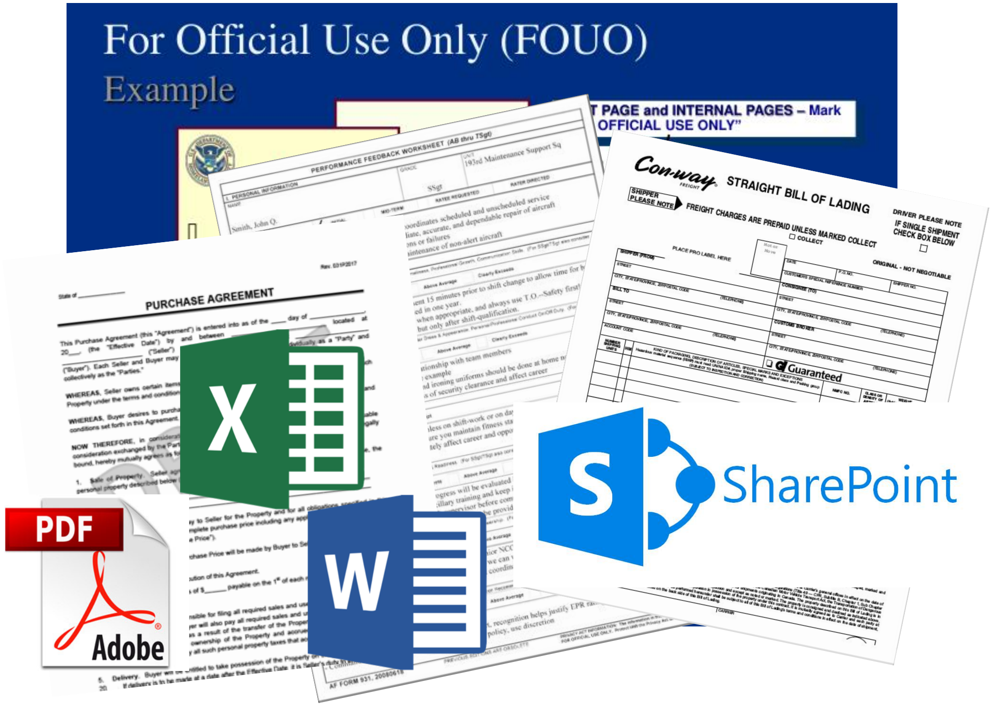
Overview

- **It’s About the Information**
- **Traditional CND Tools are Not Sufficient**
- **Current State**
- **How Data is Lost**
- **Why Symantec**
- **Data Loss Prevention Solution Overview**

Data is not necessarily Information. These terms will be used somewhat interchangeably throughout the briefing to describe important* ***content**. That content, either as raw data, or as processed information should be discovered and protected to mitigate risk of exfiltration or accidental loss.*

Data is Key Cyber Terrain; Information is a Crown Jewel of the Network

- What data results in the most damage if lost/leaked?
  - Operational Plans and Orders
  - Acquisition Material
  - Personally Identifiable Info (PII) (Social Security Numbers, Patient Health Records, etc.)
  - Logistics
- Where is that data stored today?
- How is the data being used?
- What systems are required to process this data?
- Who has access to this data?
- How does it move within the enterprise?
- How is the data protected?
  - At rest
  - In motion
  - In the cloud


For Official Use Only (FOUO)
Example
PAGE and INTERNAL PAGES – Mark "OFFICIAL USE ONLY"
PERFORMANCE FEEDBACK WORKSHEET
Con-way
STRAIGHT BILL OF LADING
PURCHASE AGREEMENT
PDF
Adobe
SharePoint

Mitigate Risk by Reducing the Attack Surface

- The DoD has been focused on securing infrastructure and transport against cyber threats & malware
  - Joint Information Environment (JIE)
    - Data Centers→ CDC/Data Center Consolidation
    - Enterprise Networks Boundary→ JRSS
  - Enterprise Services → DEE/Office 365
  - Desktops→ SDC/FDCC
- DLP Reduces the Attack Surface of the Data
  - Find and focus on what's important

- Report to the President on IT Modernization 2017
  - Prioritize the Modernization of High-Risk High-Value Assets (HVAs)
  - Reduce the Federal attack surface through enhanced application and data-level protections
  - HVAs must be driven toward implementation of modern architectures that are based on data-level protections. Systems that are most important to the Federal Government, yet are also most vulnerable, should be addressed first.

What is the DoD Doing Now?

- Despite numerous high-profile losses: Manning, Snowden, Shadow Brokers, etc., DoD protection against data loss is fragmented and siloed
  - Boundary
    - Mostly passive network/boundary inspection only
  - Hosts
    - Primarily device control; lacks data awareness
  - Insider Threat Tool(s)
    - User behavior monitoring
    - Limited focus on the actual data/content
  - Insider Threat Program Offices have been established
    - Primarily focused on policy & user behavior at this point

How Data is Lost/Exfiltrated

Symantec.

- Well-meaning Insiders
  - Email
  - Contractors/Business Partners
  - Cloud Storage/Apps
  - Lost laptop/hard drive
  - Lack of business controls
- Malicious Insiders-any way possible
  - Email
  - USB devices/DVD
  - Print
  - Cloud Storage/Apps
  - Encrypted traffic (email/web/FTP)
- Outsiders/Malicious Code-any way possible
  - Email
  - Cloud Storage/Apps
  - Encrypted traffic (web, FTP)

Too Many Unknowns, Current Risk Profile is Way Too High

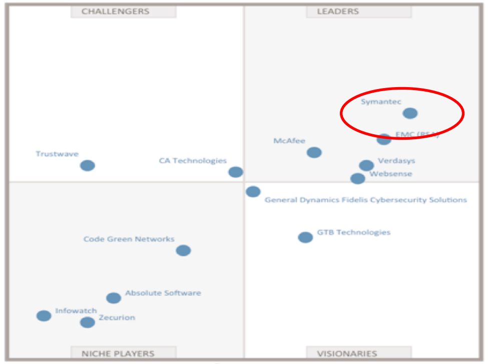
Why Symantec for Data Loss Prevention

Symantec

Past Performance, Innovation and Market Leadership

Gartner

10 Consecutive Years of Technology Leadership



IDC

The Global Market Leader in DLP

Symantec

FORTUNE

Used by over half of the Fortune 100

Data Loss Prevention

Find and Protect the Information that Matters Most

Automated Discovery, Rapid Response & Remediation

What are you looking for?

Content

- Tasking Orders
- Acquisition Data
- Personnel Data (PII,PHI)
- Logistics (OPSEC)
- Etc.

Context

- Who has access to it?
- What do they actually need?
- Where is the information?

What do you do once you've found it?

Action

- Document the incident
- Encrypt the content
- Prevent exfiltration
- Apply Data Tags / DRM

Notification

- User
- Manager
- Security Forces/OSI
- Escalate

Where is your important data?

Discover

Locate where your sensitive information resides across your cloud, network, endpoint and storage systems

How is the data being used?

Monitor

Understand how your sensitive information is being used, including what data is being handled and by whom

How do you prevent data loss?

Protect

Stop sensitive information from being leaked or stolen by enforcing data loss policies and educating end-users

Symantec Data Loss Prevention

Better Detection, Everywhere

Symantec

Advantage

DESCRIBED CONTENT MATCHING

DESCRIBED DATA

Non-indexable data

EXACT DATA MATCHING

STRUCTURED DATA

Account Numbers,
Credit Cards,
Government IDs,

INDEXED DOCUMENT MATCHING

UNSTRUCTURED DATA

Financial Reports,
Marketing Plans

MACHINE LEARNING

UNSTRUCTURED TEXT

Source Code,
Product Designs

FORM RECOGNITION

IMAGES

Scanned or
Electronically-
Filled Forms

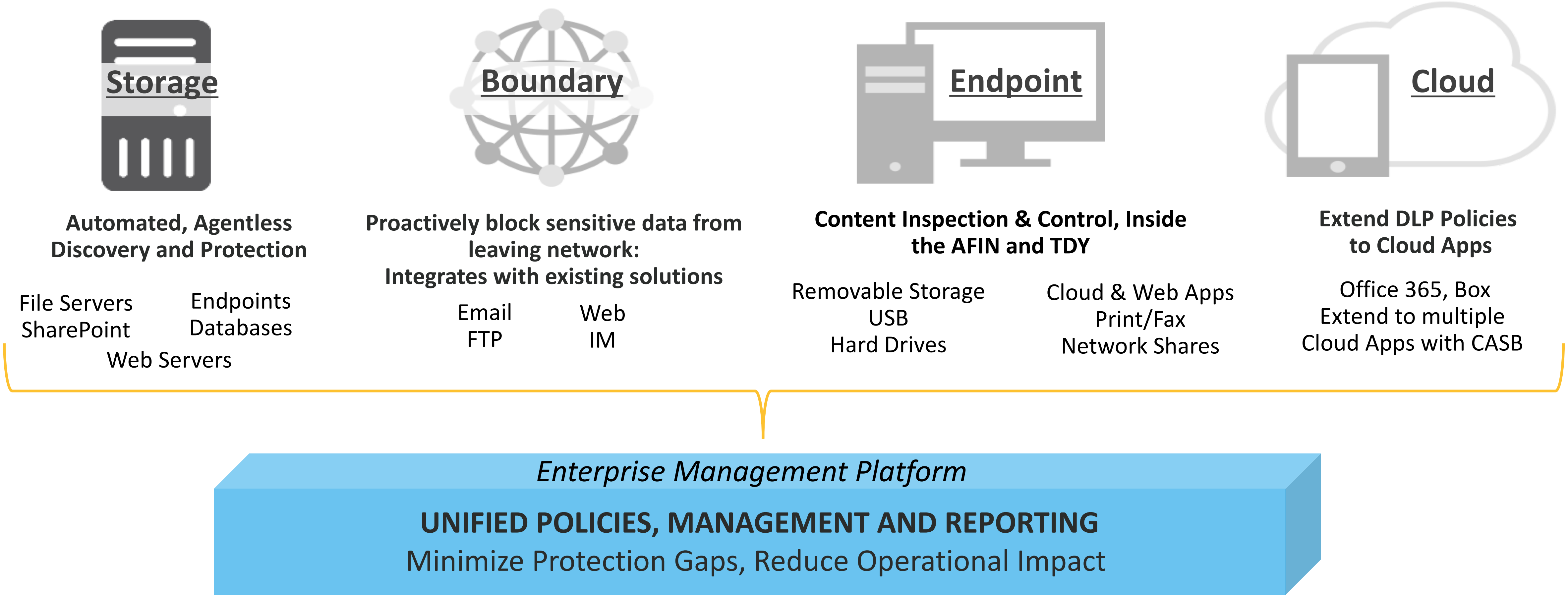
"Symantec offers the most comprehensive sensitive data detection techniques in the market, with advanced functionality such as form detection, image analysis and handwriting recognition that can cover a wide breadth of data loss scenarios"

Magic Quadrant for Data Loss Prevention, Gartner, February 2017

Data Loss Prevention

Symantec

Symantec's Modular Approach Provides Deployment Flexibility with Total Coverage; Inspect and Control Information Flow Across the Enterprise



Storage

Automated, Agentless Discovery and Protection

File Servers
SharePoint
Endpoints
Databases
Web Servers

Boundary

Proactively block sensitive data from leaving network:
Integrates with existing solutions

Email
FTP
Web
IM

Endpoint

Content Inspection & Control, Inside the AFIN and TDY

Removable Storage
USB
Hard Drives

Cloud & Web Apps
Print/Fax
Network Shares

Cloud

Extend DLP Policies to Cloud Apps

Office 365, Box
Extend to multiple
Cloud Apps with CASB

Enterprise Management Platform

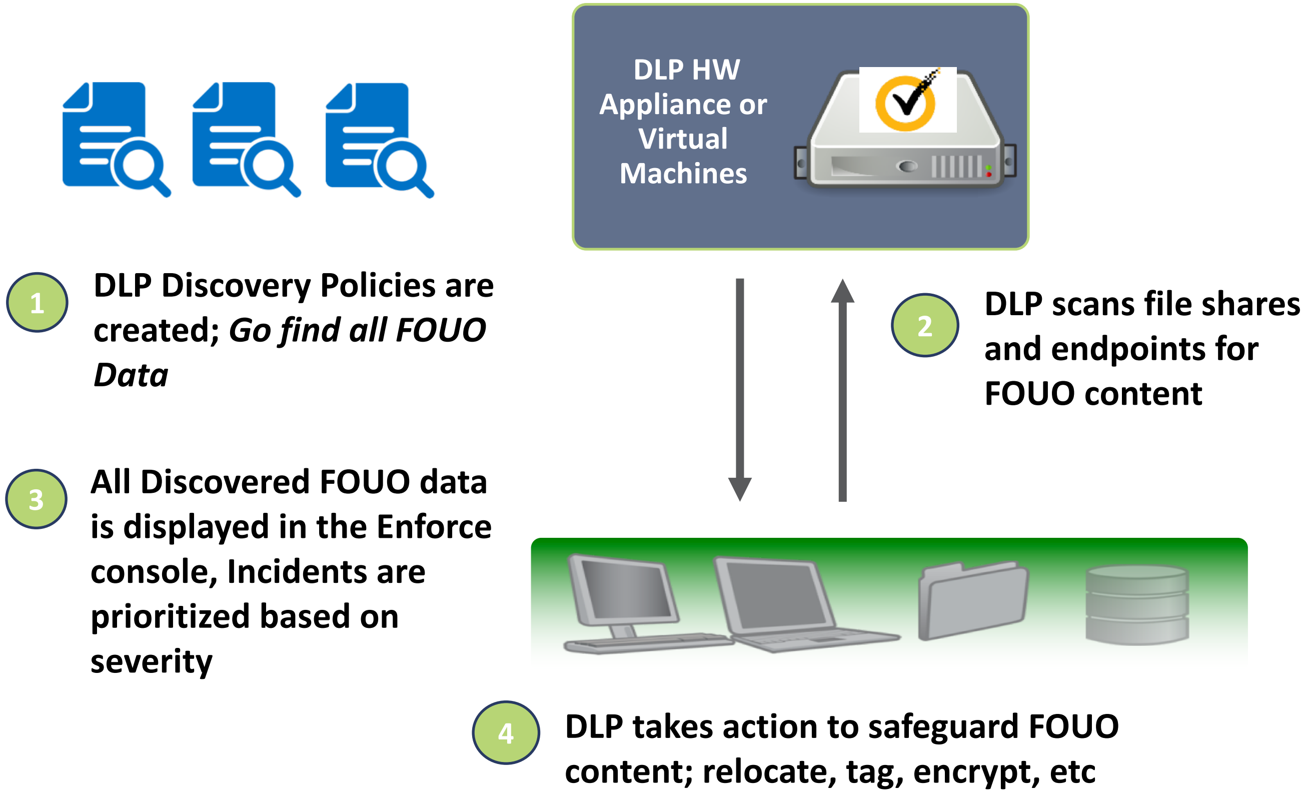
UNIFIED POLICIES, MANAGEMENT AND REPORTING

Minimize Protection Gaps, Reduce Operational Impact

Automated, Agentless Data Discovery

FIND & PROTECT THE CRITICAL DATA:
Significantly Reduce Risk of Data Spills and Exfiltration

- Baseline the Environment
  - Identify where the important data is
    - File Shares
    - Storage
    - Clients and Servers
- NO AGENT REQUIRED for Discovery or Protect
- Provides Robust Situational Awareness
  - Where is my important data?
  - Expose and mitigate risk
- Includes Automated, Customizable Remediation Options
  - Apply data tagging
  - Relocate files
  - Encrypt content
  - Alert/educate users
  - Not just "admiring the problem"



1 **DLP Discovery Policies are created; *Go find all FOUO Data***

2 **DLP scans file shares and endpoints for FOUO content**

3 **All Discovered FOUO data is displayed in the Enforce console, Incidents are prioritized based on severity**

4 **DLP takes action to safeguard FOUO content; relocate, tag, encrypt, etc**

Critical Information Protection Technologies

- **Reduce Exposure & Monitor Behavior *(Data Loss Prevention)***
  - Discover and protect sensitive or classified data, wherever it exists on the network
  - Track, alert and restrict improper end-user behavior
  - Provide integrated workforce education and training
- **Protect the Data *(Encryption)***
  - Encrypt data at rest and in-motion
  - Can leverage existing tools
- **Harden the Systems *(System Hardening)***
  - Lock down access to critical platforms, safeguarding against compromise or misuse
  - Includes Robust System Auditing
- **Inspect Encrypted Traffic *(Break and Inspect)***
  - Provides unmatched visibility into encrypted traffic, regardless of port number or application
  - Supports content inspection and protection from advanced threats
- **User-Behavior Monitoring *(Data Fusion Platforms)***
  - Collects user behavior and events from a variety of sources (cyber, bldg. access, HR violations, etc.)
  - Quickly coordinates data collected to identify risky behavior

Data Loss Prevention

Automatically discover and protect important data at-rest, in-motion or in the cloud

- Potential Opportunities
  - Big Data efforts
  - Joint/Coalition Networks
  - Cloud Migration
  - Cyber Protection Teams/Mission Defense Teams
  - Data Exfiltration concerns
  - Privacy Offices, A1/J1/G1 Organizations
  - Insider Threat

- Potential Challenges
  - DoD Insider Threat = User Behavior Monitoring
  - "Requirement"-driven mentality
  - Limited Resources and funding
  - Different conversation for Account Teams

Questions?

Symantec™

Thank You!

Patrick Duffey
patrick_duffey@symantec.com
813-363-0020