



DATA LOSS PREVENTION

PROTECTING YOUR INFORMATION AND REPUTATION

Petr Zahálka / Duben 2017





Cyber Security Services

Arm your team with actionable insights

Extend your team with experts who interpret and prioritize critical events to respond faster than you can alone



Threat Protection

Protect against the most advanced threats with complete protection from endpoint, to email, to servers, to cloud



Information Protection

Safeguard your information everywhere by keeping track of it when it's in motion, at rest or in use

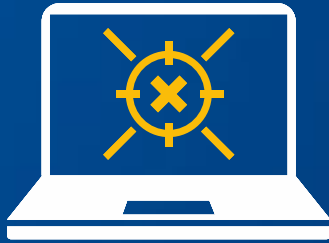


Unified Security Analytics Platform

Leverage Symantec Cyber Security Services, Threat Protection and Information Protection solutions in one platform and collect deep actionable intelligence from telemetry no other security solutions provider can claim

People

And their behavior increase risk of data loss



User habits and expectations are evolving

Creating, storing and consuming more information outside the corporate perimeter

Authorized and unauthorized cloud and mobile apps

Sharing data that shouldn't be shared

Storing sensitive information where it's vulnerable to loss or theft

Introduction



Symantec Data Loss Prevention



Protect Sensitive Data over cloud email



Betty G. - *Well Meaning Insider*

HR Manager | Insurance Company



Detection and Response

Problem

Betty attempts to email confidential employee data without knowing it



DLP Response

Cloud: DLP inspects content and context for policy match as email leaves Office 365

Endpoint: DLP inspects the mail when user hits “send”



Action

Cloud: Monitor, notify user, encrypt or block

Endpoint: Display pop-up, justify, block email, remove content



Result

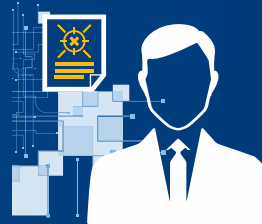
Secure your most sensitive assets – keep the malicious outsider from finding them

Discover Data “Spills” and clean them up



Charles N. - *Well Meaning Insider*

Software Developer | Investment Banking Firm



Detection and Response

Problem

Charles inadvertently stores source code on an unprotected share



DLP Response

Network Discover scan finds the exposed source code, Data Insight IDs Charles as the file owner



Action

Network Protect can:

- Notify Charles
- Encrypt the data
- Move the file
- Apply rights management policies



Result

Secure your most sensitive assets – keep the malicious outsider from finding them

Introduction



Symantec Data Loss Prevention

Where does your
confidential data
live?



Discover

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

Introduction



Symantec Data Loss Prevention

How is it being
used?



Monitor

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

Introduction



Symantec Data Loss Prevention

How do you
prevent data loss?



Protect

**Stop sensitive information
from being leaked or stolen**
by enforcing data loss policies
and educating employees

Our approach

Gives you comprehensive coverage across all channels



Manage easily

With unified data loss policies



Detection

Content

Credit Cards
SSNs
Intellectual
Property

Context

Who?
What?
Where?

Response

Action

Notify
Justify
Encrypt
Prevent

Notification

User
Manager
Security
Escalate



Protect cloud data in Box



Scan Box Accounts

TO DISCOVER SENSITIVE DATA

Protect confidential files

USING YOUR EXISTING DLP POLICIES

Actively encourage self-remediation

WITH VISUAL FILE TAGS, NOTIFICATIONS EMAILS,
AND A SELF-SERVICE PORTAL



Protect cloud data

In Office 365 and Gmail



Single, convenient cloud-based email protection solution

Stop malware, spam and malicious links

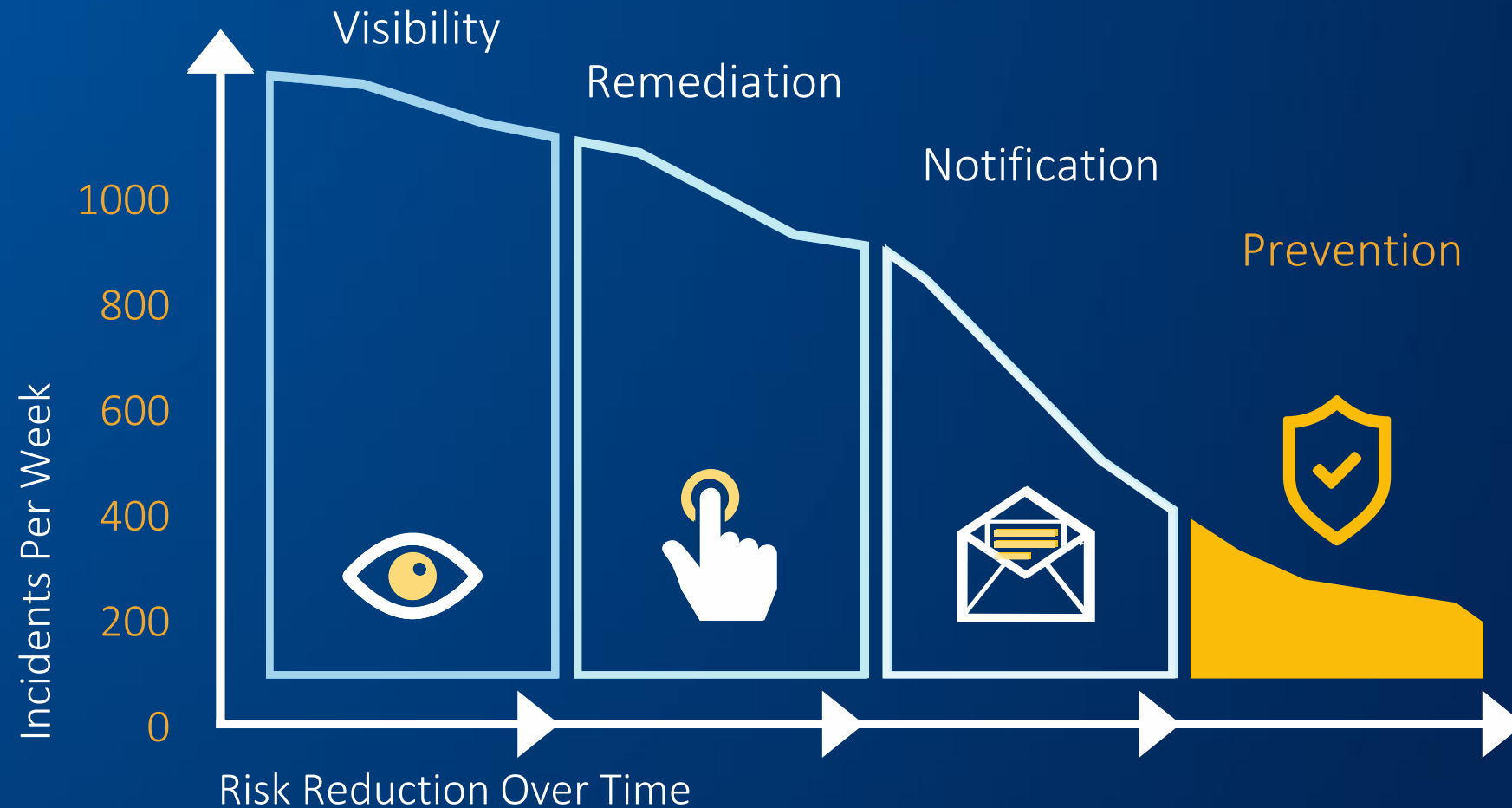
Protect against data breaches

Combines industry-leading email security and DLP



Proven

Methodology for risk reduction



Why Symantec

Innovation and market leadership



9 Consecutive Years of Technology Leadership



Why Symantec

Innovation and market leadership

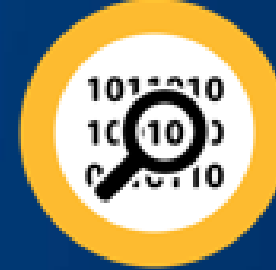


The Global Market Leader in DLP



Symantec Data Loss Prevention

A unified solution for
all your data loss channels

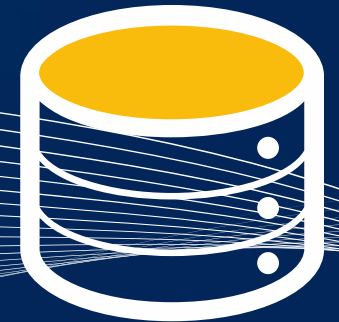
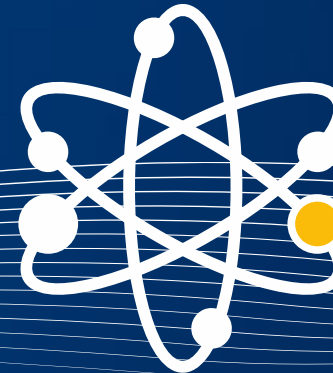
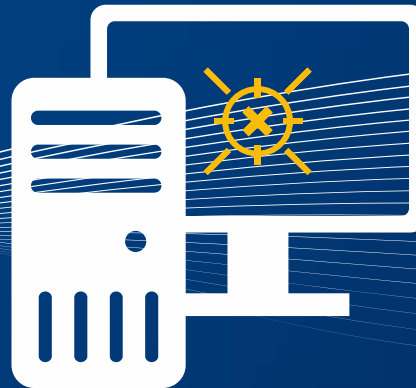


Network

Storage

Endpoint

Cloud & Mobile



3 kroky k nalezení a ochraně citlivých dat



- **Definice citlivých dat** – pravidla pro vyhledávání:
 - Podle obsahu – slova, věty, spojení, frekvence, externí slovníky
 - Podle otisku (fingerprint) dokumentu
 - Nastavení míst pro vyhledávání
- **Nalezení citlivých dat** – jednorázově a pravidelně:
 - Úložiště – úložiště SAN/NAS, databáze, Windows file-shares, SharePoint sites, Unix file-shares, ...
 - Koncové body – uživatelské stolní počítače a notebooky
- **Ochrana citlivých dat** – vynucení bezpečnostních pravidel
 - Úložiště – mazání, přesuny citlivých dat
 - Síť – sledování pohybu citlivých dat, zamezení úniku přes perimetr
 - Koncové body – sledování a případné omezení práce uživatele s citlivými daty (kopírování, e-mail, HTTP, FTP, tisk, vypalování, atd.)

Datový audit – zadání

- Zpracováváme osobní údaje našich zákazníků. Jsme přesvědčeni, že data zpracováváme v souladu s našimi předpisy, které jsou přísné a zajišťují ochranu dat požadující GDPR.
- Zavedení naprostého souladu však vyžaduje úpravu některých core systémů a před jejich zahájením potřebujeme zjistit zda nejsou osobní údaje zpracovávána ještě jinde a jinak.

Datový audit – provedení

- 3 fáze
- Definice scope
 - GDPR - použitý template
 - Přidáno vyhledání ještě „Obchodní dokumenty“
- Provedení auditu
 - Provedení skenu uložišť, databází, serverů i desktopů **Data in rest**
 - Monitoring práce uživatelů **Data in move**
- Vyhodnocení
 - Vypracování zprávy
 - Prezentace výsledků

Datový audit - výsledky

- Data spadající pod GDPR byla nalezena na více než 2000 místech mimo informační systém
- Přes 200 z nich bylo na místech s minimální úrovní zabezpečení
- Bylo zjištěno více jak 500 zásadních selhání oprávněných uživatelů
- Opatření ještě nebyla stanovena, ale výsledky jsou použity pro analýzu nezbytných úprav procesů i systémů
- Ukázalo se, že zavedení pravidelného monitorování je nezbytné pro udržení dosažené úrovně zabezpečení.

Shrnutí

- Ochrana dat musí být cílená
- Potřebuji vědět kde data leží a jak se s nimi pracuje
- Potřebuji pokrýt všechna rizika, všechny vektory úniku
- Lepší je mít jedno řešení, které mi zajistí kompletní ochranu, než mít více oddělených
- Pozor na právní důsledky podrobného monitorování korespondence a činnosti uživatelů
- Pokud potřebujete pomoci s analýzou stávajícího stavu a navrhnout optimální řešení obraťte se na nás!



THANK YOU



Ing. Petr Zahálka
Avnet s.r.o.
+420 602 354 836
petr.zahalka@avnet.com



APPENDIX

Protect Sensitive Data over cloud email



Betty G. - *Well Meaning Insider*

HR Manager | Insurance Company



Detection and Response

Problem

Betty attempts to email confidential employee data without knowing it



DLP Response

Cloud: DLP inspects content and context for policy match as email leaves Office 365

Endpoint: DLP inspects the mail when user hits “send”



Action

Cloud: Monitor, notify user, encrypt or block

Endpoint: Display pop-up, justify, block email, remove content



Result

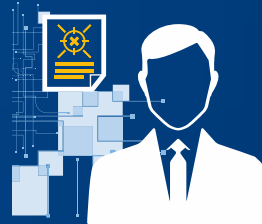
Secure your most sensitive assets – keep the malicious outsider from finding them

Discover Data “Spills” and clean them up



Charles N. - *Well Meaning Insider*

Software Developer | Investment Banking Firm



Detection and Response

Problem

Charles inadvertently stores source code on an unprotected share



DLP Response

Network Discover scan finds the exposed source code, Data Insight IDs Charles as the file owner



Action

Network Protect can:

- Notify Charles
- Encrypt the data
- Move the file
- Apply rights management policies



Result

Secure your most sensitive assets – keep the malicious outsider from finding them

Gain Visibility and Control of information in cloud storage



Sanjay V. - *Well Meaning Insider*

Assistant Controller | Manufacturing Company



Detection and Response

Problem

Sanjay copies pre-released financial data to a cloud storage site



DLP Response

Cloud Storage scans Box for sensitive files and tags them

Endpoint: DLP detects sensitive files before upload to personal cloud storage



Action

Enable user self-remediation via Data Insight self service portal

Block sensitive files



Result

Higher visibility into where data is going

Change users' behavior

Prevent Information theft



Mimi L. - *Malicious Insider*

Soon-to-be-former Account Executive | Staffing Firm



Detection and Response

Problem

Unhappy or departing employees copy or share client records and resumes via email or removable storage



DLP Response

DLP monitors desktop and network activity



Action

Notify (warn) the user of their actions

Inform manager, security and/or HR

Stop the transmission or copy



Result

Information assets don't leave with the employee

People know they are being monitored

Ochrana dat x ochrana soukromí

- Ochrana soukromí x ochrana majetku
 - Jedná se o střet těchto práv
- Implementace monitoringu znamená splnit třístupňový test proporcionality
 - Vhodnost
 - Potřebnost
 - Porovnání, vyvážení

Vhodnost

- Umožňuje opatření, kterým zasahujeme do práva na soukromí (nebo jej omezujeme) vůbec dosáhnout sledovaný cíl?
- Pokud podezříváme zaměstnance z toho, že odesílá data e-mailem konkurenci, je vhodné uchovávat i obsah soukromé korespondence neobsahující firemní data?
- Jak takové e-maily poslouží k deklarovanému účelu?

Potřebnost

- Pokud jsme zvolili vhodné opatření, měli bychom jej porovnat s jinými v úvahu připadajícími opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod, respektive zasahujícími do konfliktních práv v menší míře.

Porovnání, vyvážení

- Zvážení zásahu do soukromí bude nutné často učinit až v konkrétních případech:
 - paušalizované reakce na zjištěný problém (narušení pravidel, výskyt definovaného stavu) nemusí odpovídat adekvátní obraně práv zaměstnavatele
- Pokud se přesto nekvalifikovaně rozhodneme zásah do soukromí učinit, může být ve svém důsledku protiprávní