



Protecting the human point.

# Data Loss Prevention

## An Introduction to Forcepoint DLP

# Presenters



**DAVID BRANCH**

Technical Account Manager  
Austin, TX



**JIMMY MEANS**

Technical Account Manager  
San Antonio, TX

# OBJECTIVE

By the end of this webinar participants should:

- ▶ Have a better understanding of Forcepoint's DLP functionality
- ▶ Be able to optimize the Data Loss Prevention configuration in their Forcepoint deployments



# TOPICS

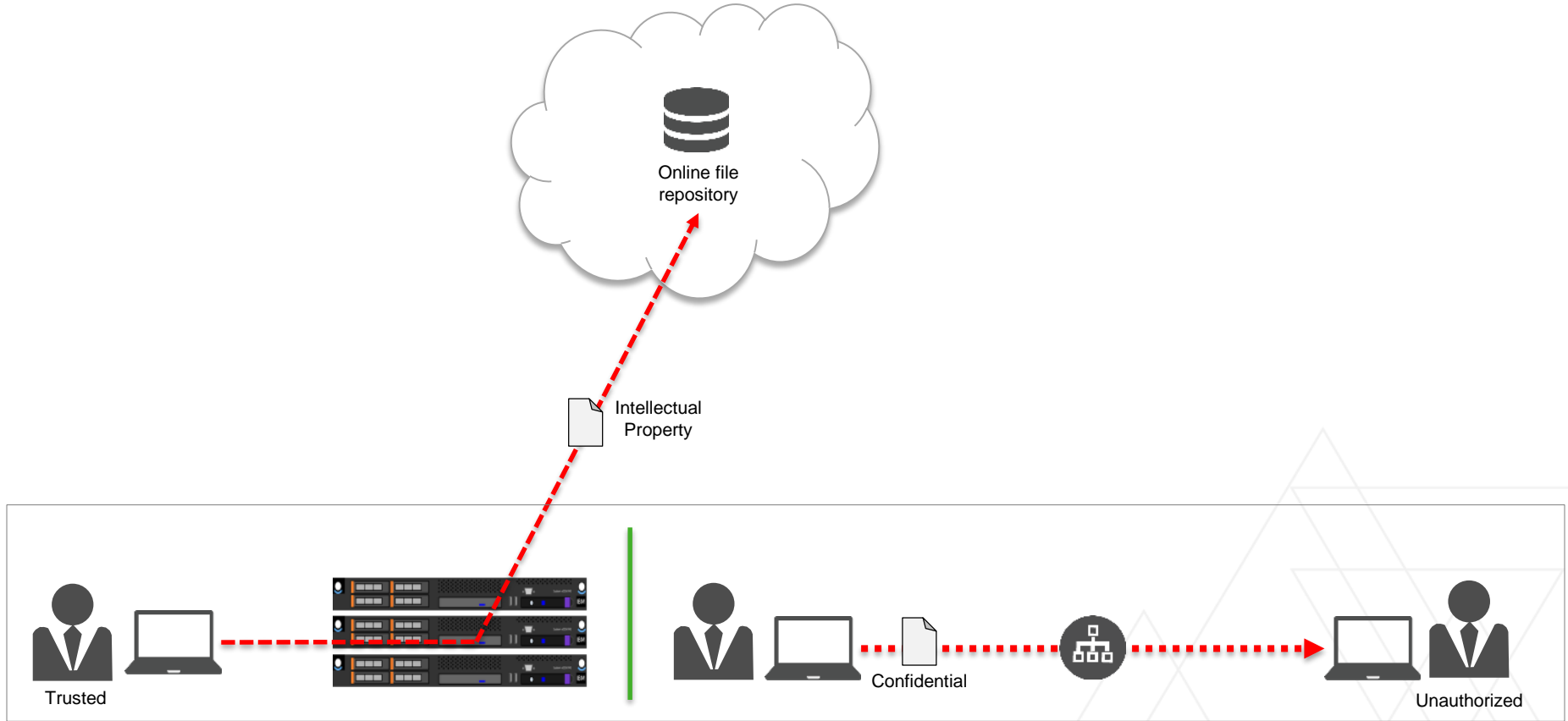
- ▶ Why is DLP important
- ▶ Which data should be protected and how
- ▶ Configuring DLP policies in your Forcepoint deployment
- ▶ Forcepoint DLP Best Practices
- ▶ Troubleshooting DLP Issues



# DLP WHY DATA LOSS PREVENTION IS IMPORTANT



# DLP WHY DATA LOSS PREVENTION IS IMPORTANT



# DLP WHY DATA LOSS PREVENTION IS IMPORTANT

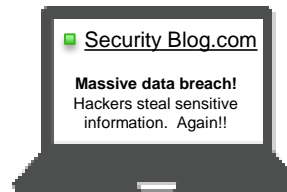
## Slide notes

DLP is important for protecting information such as Personally Identifiable Information, Payment Card Industry data, Protected Health Information, intellectual property and other sensitive company information.

Data leaks, whether intentional or accidental, can lead to the loss of critical IP. It can also be in violation of government regulations such as export laws, compliance standards required to conduct business, and loss of customer data that could lead to legal liabilities.



# DLP WHY DATA LOSS PREVENTION IS IMPORTANT





# DLP WHY DATA LOSS PREVENTION IS IMPORTANT

## Slide notes

The lack of a well thought out and executed DLP strategy can also lead to a loss of customer confidence.

As network security professionals you have to ask yourself, *“if my company encountered a data breach that became public would our customers want to continue to do business with us?”*



# DLP WHY DATA LOSS PREVENTION IS IMPORTANT



**Forcepoint** ✓

@Forcepointsec

Follow



"This is the new normal." A statement from [@rfordonsecurity](#) regarding today's news of the [#Equifax](#) [#cybersecurity](#) breach.

Dr. Richard Ford, chief scientist of Forcepoint:

"The unfortunate Equifax breach is just another embodiment of the threat environment that organizations face every day – this is the new normal. The rise of large scale data collection and aggregation has placed considerable pressure on organizations to preserve privacy while leveraging data for legitimate business purposes. The more sensitive the data the greater the liabilities caused by a breach. The threats to this data are diverse, ranging from the apparent hack disclosed here to accidental loss by authorized users. Focusing too narrowly on a single scenario can prevent companies from seeing the full spectrum of risk they face, with dire consequences. Companies need to augment legacy defenses with modern, human-centric approaches that look at how and why data is accessed and by whom; this intersection of people, data and systems can become the critical point for effective security and compliance."

6:06 PM - 7 Sep 2017

23 Retweets 18 Likes



23



18



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW



Geographical Region



Industry / Sector

# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

When deciding which rules apply to your organization, you must take a few things into consideration:

- **The geographical location of targeted data** because laws and regulations differ in each country.
- **Your *industry* should be taken into consideration** – Various industries dictate the type of data that must be protected to comply with laws and regulations, such as HIPAA data for the healthcare industry.
- **Your sector also matters** – Even companies that operate in the public sector may be subject to federal laws and regulations that govern data that is shared by the government organizations they serve.

Overall, there are legal requirements involved in, not only protecting *your* company's data, but also the data of your customers.



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

Where is the data stored in your network?

## Data-at-rest



Network Shares



Databases



Workstations



Removable Media



Cloud Storage

# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

Once the *types of data* to protect have been identified, the next step is to determine who owns the data and where and how it is stored in your environment. The most common locations for stored sensitive data include:

- Corporate File Servers or shared drives
- Databases
- Client workstations, laptops
- Removable media
- And Cloud storage

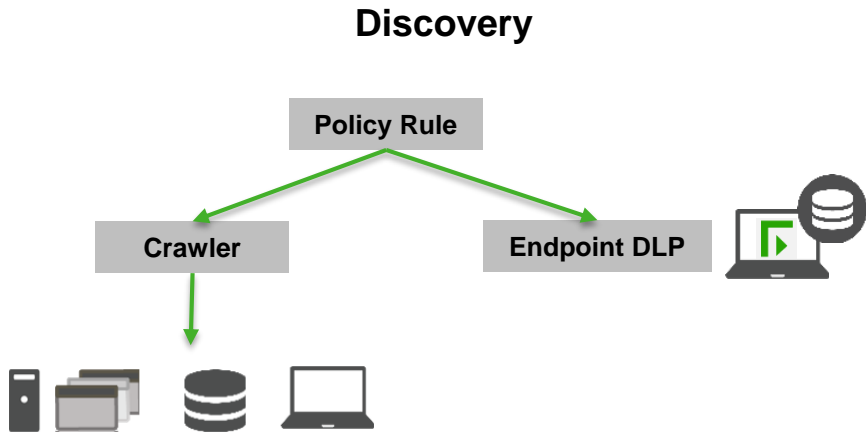
Focusing on these locations will provide a good starting point to find targeted data-at-rest. Once key locations have been determined, Discovery policies can be configured to take an inventory of what data exists in targeted locations.



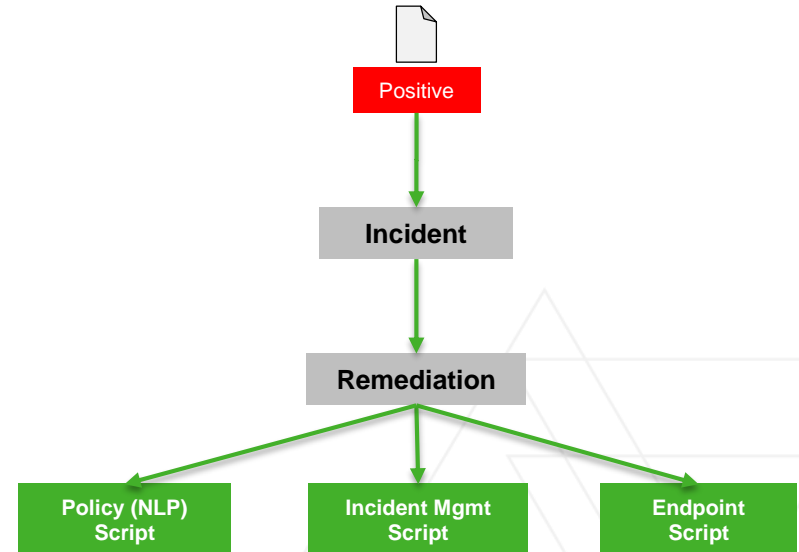
# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

Where is the data stored in your network?

## Scanning data-at-rest



## Policy Rule Violation





# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

The **Discovery** task can help with this step.

The Discovery task scans data-at-rest according to configured Discovery policy rules and tasks. When a policy task is configured the Crawler does a Network Discovery scan on files and folders that are specified in the task configuration. On machines with an Endpoint Client, the DLP Endpoint agent performs that discovery.

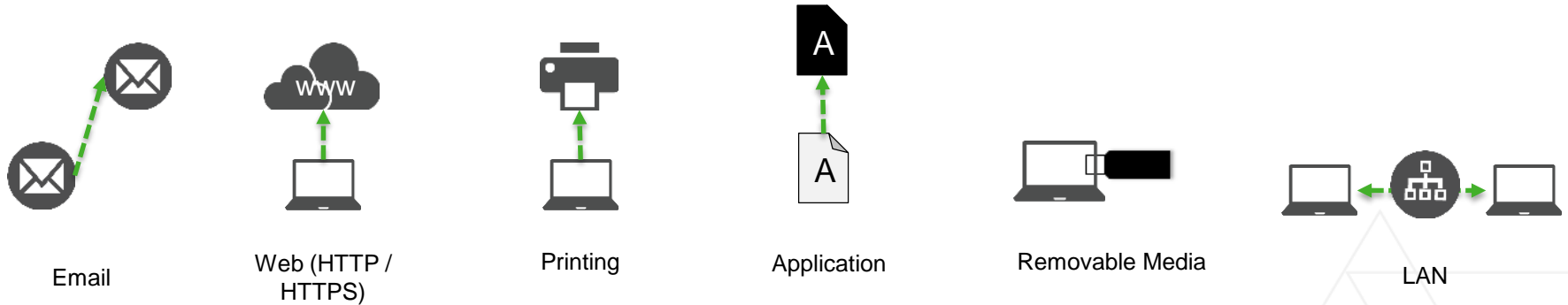
When a policy rule is matched, a **policy rule violation** occurs and an incident is triggered. The remediation of a violation is handled by the Policy Engine for both Policy Scripts and Incident Management Scripts. The Endpoint agent handles the incident remediation on machines with the Endpoint Client installed.



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

How is the data being transferred in and from your network?

## Data-in-motion



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

Along with data-at-rest locations, there are several data-in-motion channels that must be taken into consideration while planning your DLP strategy. Those channels are:

- **Email** – for monitoring data in outbound and internal emails
- **Web** – for monitoring data on the HTTP and HTTPS protocols
- **Printing** – for monitoring data being sent to a local or network printers
- **Application** – for monitoring data that is being copy and pasted from .pdf, Office, and other file types.
- **Removable media** – for monitoring data that is being sent to thumb drives, external HDDs, and optical drives
- **LAN** – for monitoring data being copied through an external LAN (for instance: from a home network)

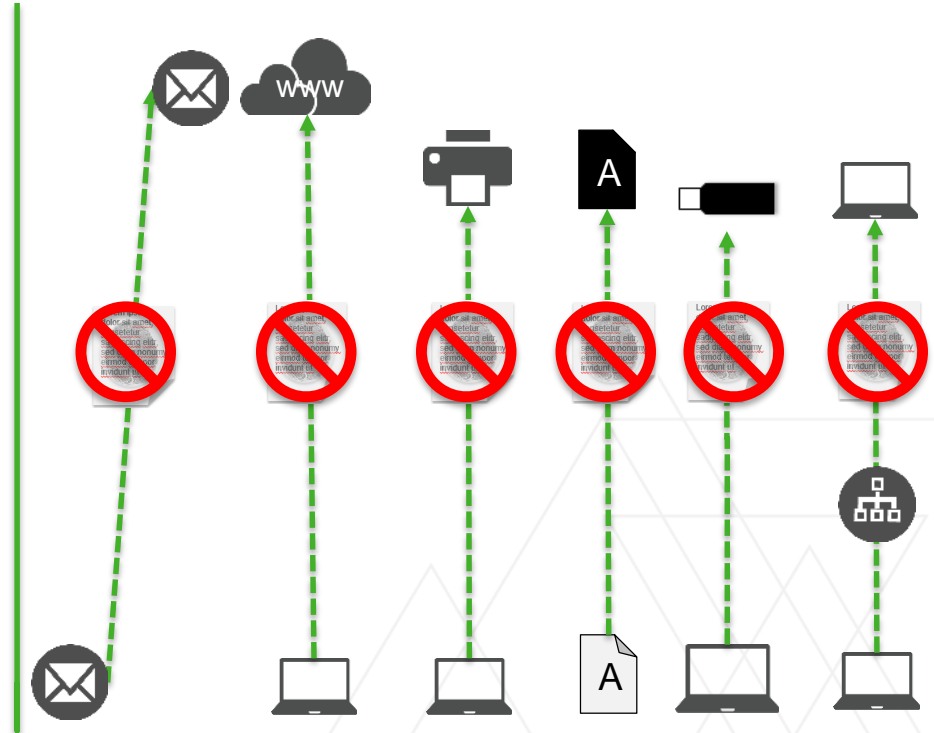
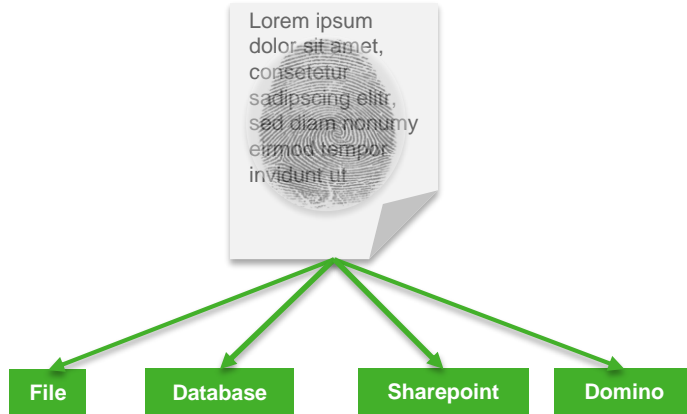


# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

How is the data being transferred in and from your network?

## Scanning data-in-motion

### Fingerprinting



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

**Fingerprinting** can be used to monitor and control the data-in-motion in your environment.

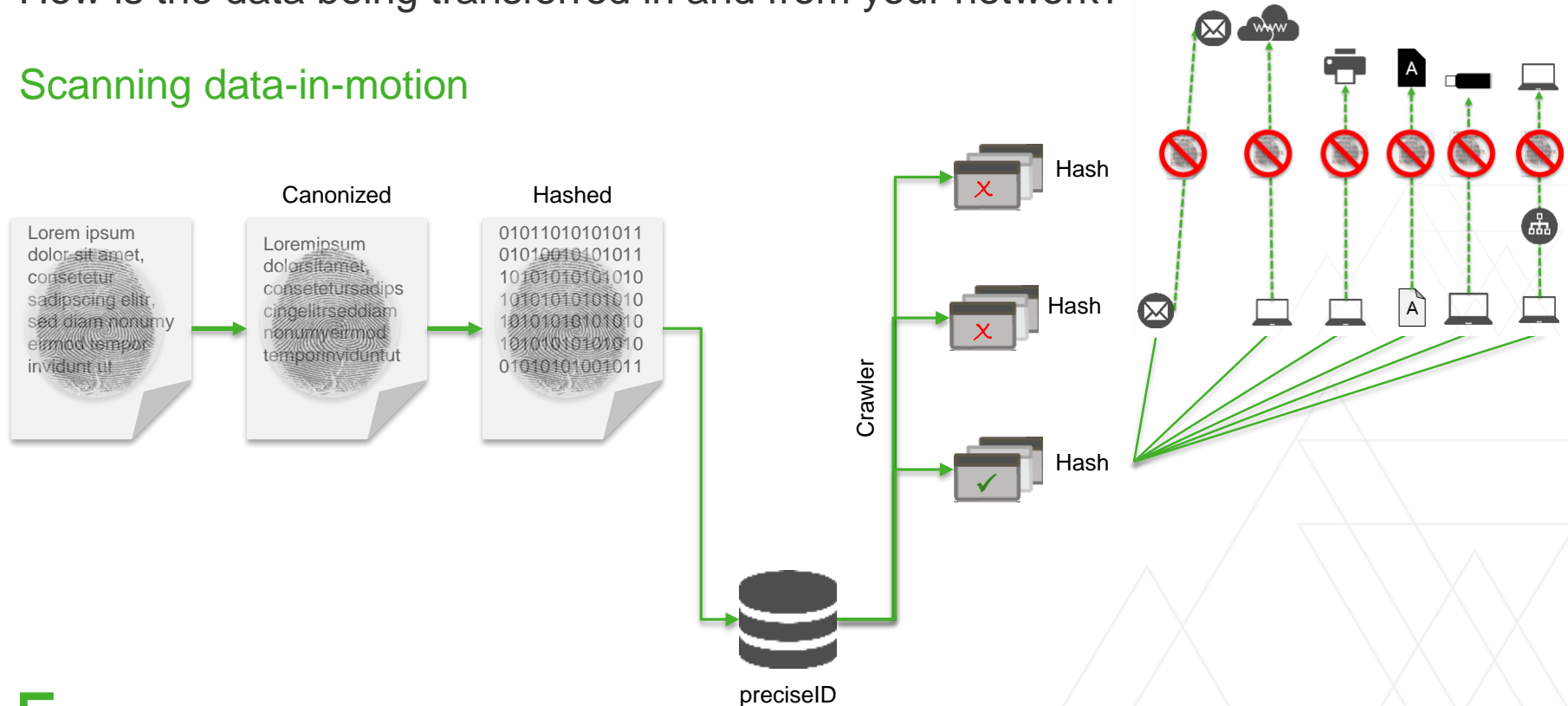
Fingerprinting is similar to Discovery in that, it's used to identify sensitive data. However, with Fingerprinting *you determine* the content of sensitive documents (all or in part), which is sensitive, as opposed to content that is protected by predefined classifiers.



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

How is the data being transferred in and from your network?

## Scanning data-in-motion



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

**Fingerprinting** starts with the canonization of the file you wish to fingerprint. This is basically removing likely insignificant characters and words such as, “I”, “and”, “the”, “a”, etc.. Spaces are also removed.

The remaining content is then hashed to uniquely define the fingerprinted content. This hash is then stored in the PreciseID database.

The Crawler then scans files and folders according to the policy configuration and canonizes and hashes those documents.

And lastly, files that match the hash of the original fingerprinted document are then protected from leaving a device or your network or just monitored, depending on your policy configuration.



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

Assessing job roles and privileged users





# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

When deciding which policies to deploy there're many factors that should be considered, such as:

How user job roles are taken into account when considering a policy action.

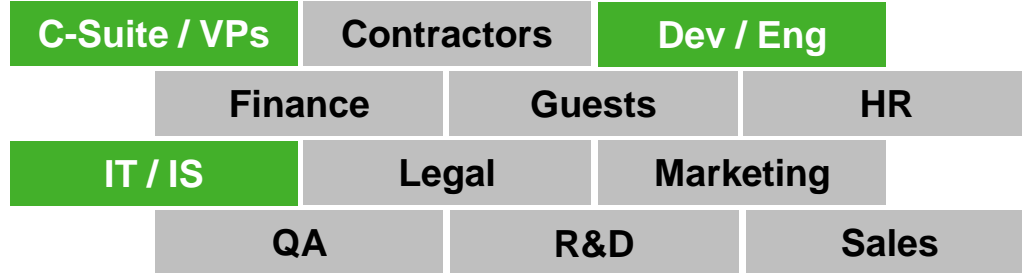
- **Example 1:** Members of the payroll team may need to send a bulk list of social security numbers to the IRS during tax season. However, members of the Human Resources team should never send SSNs outside of the internal network in bulk at any time.
- **Example 2:** Your company has a spreadsheet that contains quarterly financial data. Members of the CFO team may need to share that information with outside auditors. However, members of the Business Analyst team should never be allowed to send this information outside of the internal network.

In these examples, there is a clear segmentation of permissions base on the job role.



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

Assessing job roles and privileged users



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

Policy exceptions for high profile or privileged users should also be taken into account.

High profile users are inherently more vulnerable to data loss. This is because they are regarded as the most responsible and trusted members of our user base. Creating effective DLP policies for these users is important for the overall effectiveness of your DLP enforcement. While some exceptions may apply, you should keep them to a minimum.

- **Example 1:** The laptop of the VP of Human Resources contains PII for your company's employees. While the VP may never intentionally leak the data that is stored on this laptop, a virus on the laptop may be able to extract the data without the user's knowledge.
- **Example 2:** A Sr. Network Administrator has unobstructed access to all directories and files on the network. Before leaving the company, the admin downloads sensitive information about the company's network topography, including MAC addresses, IP addresses, host names, and machine passwords to an external drive.

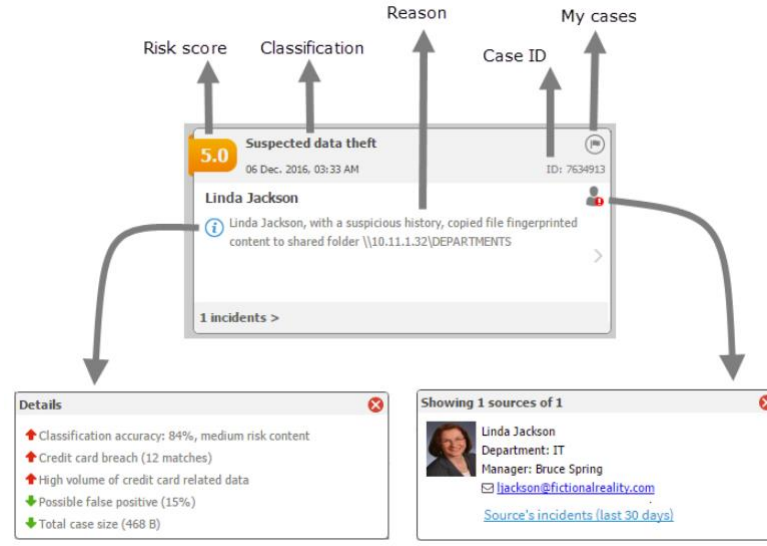
You can configure a policy scheme in your environment to avoid data loss in these scenarios. In 8.4 (our latest release), we made this easier with a new feature called **Incident Risk Ranking**.



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

Assessing job roles and privileged users

## New to 8.4 - Incident Risk Ranking



<http://www.websense.com/content/support/library/data/v84/help/ubaTopRisks.aspx>



# DLP WHICH DATA SHOULD BE PROTECTED AND HOW

## Slide notes

In 8.4 administrators can now identify high-risk resources and configure incident risk ranking reports to include the **high-risk** classification as a factor in calculating a case's risk score. With this feature, administrators can bring in information about known high-risk employees from external data sources and have that information factored into the incident risk ranking process.

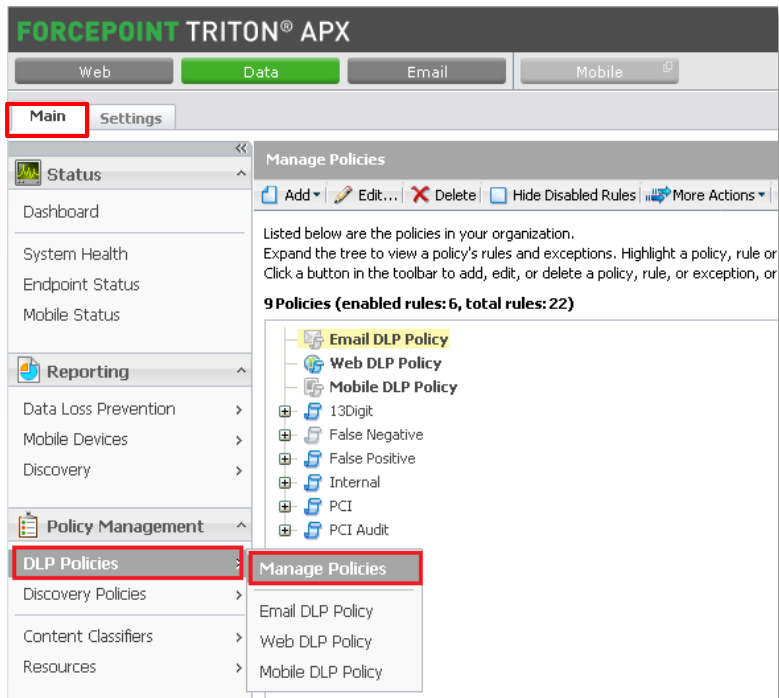


# DLP CONFIGURING DLP POLICIES



# DLP CONFIGURING DLP POLICIES

## Adding a policy



FORCEPOINT TRITON® APX

Web Data Email Mobile

Main Settings

Status

Dashboard

System Health

Endpoint Status

Mobile Status

Reporting

Data Loss Prevention

Mobile Devices

Discovery

Policy Management

DLP Policies

Discovery Policies

Content Classifiers

Resources

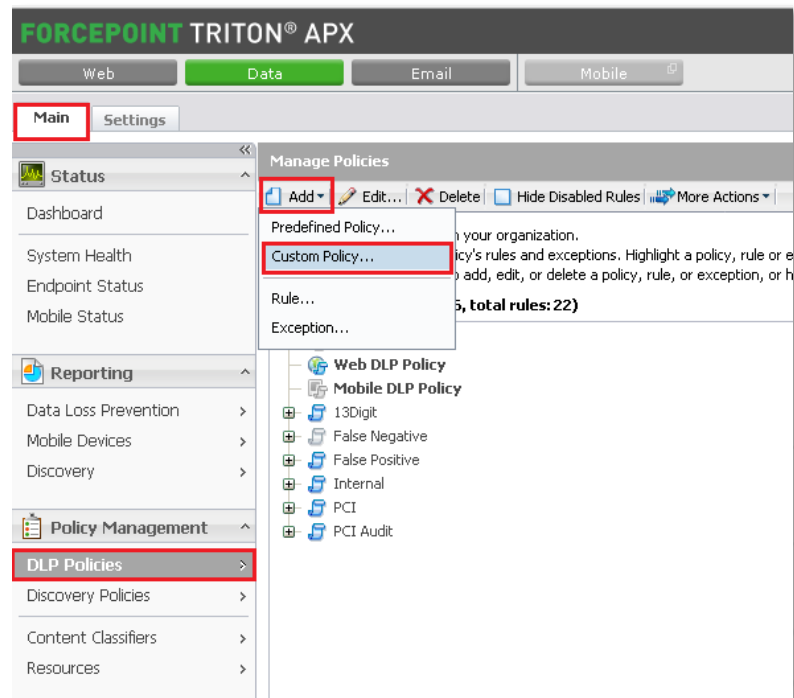
Manage Policies

Add Edit... Delete Hide Disabled Rules More Actions

Listed below are the policies in your organization. Expand the tree to view a policy's rules and exceptions. Highlight a policy, rule or Click a button in the toolbar to add, edit, or delete a policy, rule, or exception, or

9 Policies (enabled rules: 6, total rules: 22)

- Email DLP Policy
- Web DLP Policy
- Mobile DLP Policy
  - 13Digit
  - False Negative
  - False Positive
  - Internal
  - PCI
  - PCI Audit



FORCEPOINT TRITON® APX

Web Data Email Mobile

Main Settings

Status

Dashboard

System Health

Endpoint Status

Mobile Status

Reporting

Data Loss Prevention

Mobile Devices

Discovery

Policy Management

DLP Policies

Discovery Policies

Content Classifiers

Resources

Manage Policies

Add Edit... Delete Hide Disabled Rules More Actions

Predefined Policy...

Custom Policy...

Rule...

Exception...

Listed below are the policies in your organization. Expand the tree to view a policy's rules and exceptions. Highlight a policy, rule or Click a button in the toolbar to add, edit, or delete a policy, rule, or exception, or

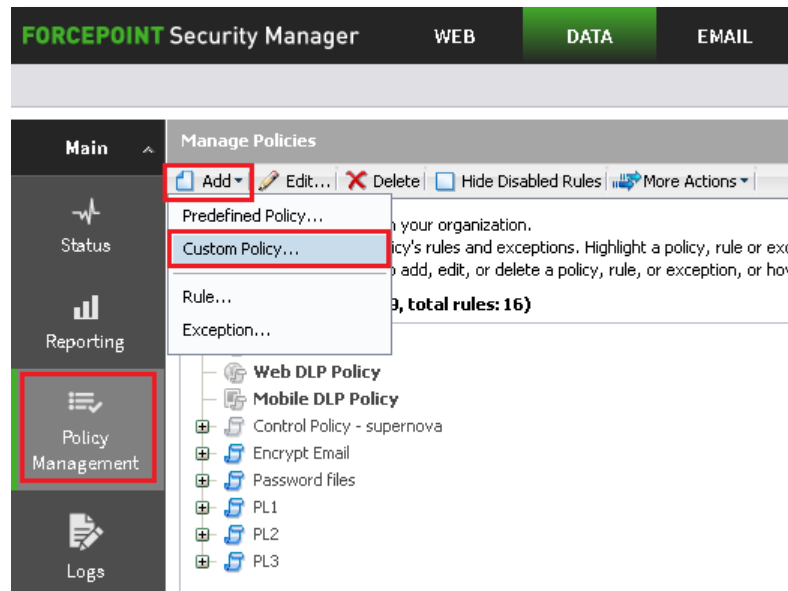
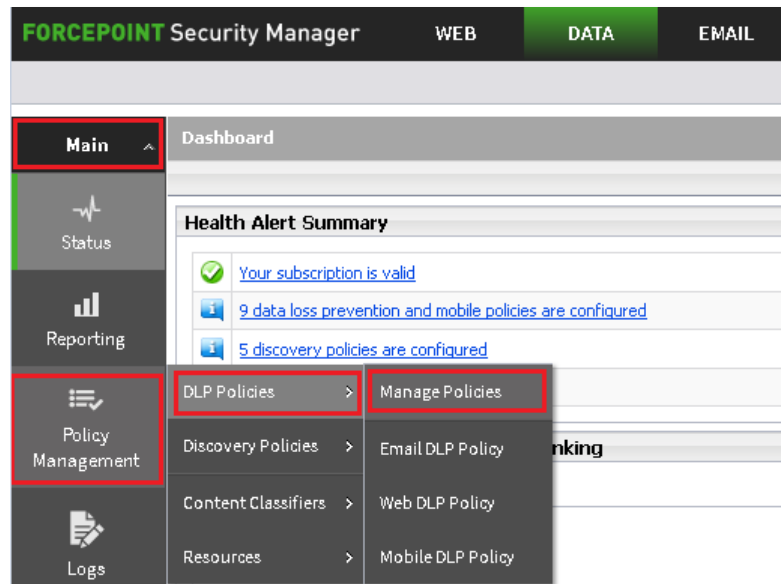
5, total rules: 22)

- Web DLP Policy
- Mobile DLP Policy
  - 13Digit
  - False Negative
  - False Positive
  - Internal
  - PCI
  - PCI Audit



# DLP CONFIGURING DLP POLICIES

## Adding a policy (8.4)





# DLP CONFIGURING DLP POLICIES

## Policy Elements

### Rules

The screenshot shows the Forcepoint Triton APX interface. The top navigation bar includes 'Web', 'Data' (selected), 'Email', and 'Mobile'. The left sidebar has 'Main' and 'Settings' tabs. Under 'Main', there's a 'Status' section with links to Dashboard, System Health, Endpoint Status, and Mobile Status. Below that is a 'Reporting' section with links to Data Loss Prevention, Mobile Devices, and Discovery. The 'Policy Management' section is expanded, showing 'DLP Policies' (highlighted with a red box), 'Discovery Policies', 'Content Classifiers', and 'Resources'. The 'Manage Policies' section on the right has a toolbar with 'Add' (highlighted with a red box), 'Edit...', 'Delete', 'Hide Disabled Rules', and 'More Actions'. The 'Add' dropdown menu is open, showing options: 'Predefined Policy...', 'Custom Policy...', 'Rule...' (highlighted with a red box), and 'Exception...'. The 'Rule...' option is selected, and the interface shows a list of rules under 'Web DLP Policy' and 'Mobile DLP Policy', including '13Digit', 'False Negative', 'False Positive', 'Internal', 'PCI', and 'PCI Audit'. The total number of rules is 22.

### Exceptions

The screenshot shows the Forcepoint Triton APX interface. The top navigation bar includes 'Web', 'Data' (selected), 'Email', and 'Mobile'. The left sidebar has 'Main' and 'Settings' tabs. Under 'Main', there's a 'Status' section with links to Dashboard, System Health, Endpoint Status, and Mobile Status. Below that is a 'Reporting' section with links to Data Loss Prevention, Mobile Devices, and Discovery. The 'Policy Management' section is expanded, showing 'DLP Policies' (highlighted with a red box), 'Discovery Policies', 'Content Classifiers', and 'Resources'. The 'Manage Policies' section on the right has a toolbar with 'Add' (highlighted with a red box), 'Edit...', 'Delete', 'Hide Disabled Rules', and 'More Actions'. The 'Add' dropdown menu is open, showing options: 'Predefined Policy...', 'Custom Policy...', 'Rule...', and 'Exception...' (highlighted with a red box). The 'Exception...' option is selected, and the interface shows a list of exceptions under 'Web DLP Policy' and 'Mobile DLP Policy', including '13Digit', 'False Negative', 'False Positive', 'Internal', 'PCI', and 'PCI Audit'. The total number of rules is 22.



# DLP CONFIGURING DLP POLICIES

## Slide notes

To create a DLP policy you must define a few policy elements:

**Rules** are the conditions that define the behavior of a policy. You can have *multiple* rules in a policy. As we discussed earlier, incidents are generated each time a rule is matched. They can also be generated over time, after a rule has reached a cumulative number of matches.

- **Example:** You can configure a rule to generate an incident every time a single credit card number is detected versus generating an incident after 10 credit card numbers are detected from the same source IP address.

**Exceptions** are used to create more granular rules by specifying a new action that should be applied when certain conditions are met. This can be used to exclude a part of a larger group by specifying a different action for the rule. It can also be used to implement a different action plan with a higher severity. Since exceptions are configured as part of a rule, the exceptions are only checked when a rule is triggered. Although you can add an exception to a cumulative rule, the exceptions themselves cannot be cumulative.

You can either exclude or *include* with exceptions.

- **Exclude exception example:** Only users in the Finance Group are allowed to send files from the Finance file server as an email attachment. The Finance Group would be defined as the exception to a rule to block all other users from sending these files as an email attachment.
- **Include exception example:** An exception is created to prevent users in the Research & Development group from sending files with sensitive IP from the R&D server as an email attachment. A Chief Developer attempts to email another Chief Developer a document that contains intellectual property, and the transmission of this document is blocked. The Forcepoint Administrator then configures an exception for a “Chief Developer Group” to allow the two developers to share IP documents over email.



# DLP CONFIGURING DLP POLICIES

## Policy Elements (8.4)

### Rules

FORCEPOINT Security Manager WEB DATA EMAIL

Main Manage Policies

Add Edit... Delete Hide Disabled Rules More Actions

Predefined Policy...  
Custom Policy...  
Rule...  
Exception...

Web DLP Policy  
Mobile DLP Policy  
Control Policy - supernova  
Encrypt Email  
Password files  
PL1  
PL2  
PL3

Policy Management

### Exceptions

FORCEPOINT Security Manager WEB DATA EMAIL

Main Manage Policies

Add Edit... Delete Hide Disabled Rules More Actions

Predefined Policy...  
Custom Policy...  
Rule...  
Exception...

Web DLP Policy  
Mobile DLP Policy  
Control Policy - supernova  
Encrypt Email  
Password files  
PL1  
PL2  
PL3

Policy Management



# DLP CONFIGURING DLP POLICIES

## Policy Elements

### Content Classifiers

The screenshot shows the 'Content Classifiers' page in the Forcepoint Triton APX interface. The left sidebar has a red box around 'Content Classifiers' and a sub-menu with 'Patterns & Phrases', 'File Properties', 'File Fingerprinting', 'Database Fingerprinting', and 'Machine Learning'. The main content area is titled 'Content Classifiers' and includes a description: 'Describe the content you are protecting. Classify it according to characteristics such as dictionary terms and file properties, or create fingerprints for more precise definition. The system compares data to these classifiers and triggers an incident when it detects a match. Be sure to add a classifier to your policy to initiate analysis.' Below this, there are sections for 'Attributes' (Identify attributes that should trigger an incident, such as a particular RegEx pattern, phrase, or file.) and 'Fingerprints' (Create fingerprints of your most sensitive data. When even a partial fingerprint is matched, an incident is triggered.).

### Resources

The screenshot shows the 'Resources' page in the Forcepoint Triton APX interface. The left sidebar has a red box around 'Resources' and a sub-menu with 'User Directory Entries', 'Custom User Directory Groups', 'Custom Users', 'Custom Computers', 'Networks', 'Domains', 'Business Units', 'URL Categories', 'Endpoint Devices', 'Endpoint Applications', 'Endpoint Application Groups', 'Endpoint Printers', 'Action Plans', 'Remediation Scripts', and 'Notifications'. The main content area is titled 'Resources' and includes a description: 'the data you want to protect and the actions you want to take when a policy breach is discovered. This page lists the resources that are protected by your policies, such as domains, business units, URL categories, endpoint devices, endpoint applications, endpoint application groups, endpoint printers, action plans, remediation scripts, and notifications.' Below this, there are sections for 'Custom User Directory Groups' and 'Custom User Directory Entries'.



# DLP CONFIGURING DLP POLICIES

## Slide notes

**Content Classifiers** define what specific data will trigger the rule. A rule may contain one Content Classifier or multiple Content Classifiers if a more granular policy is needed. Data can be classified by Patterns or Phrases, File Properties, File or Database Fingerprinting or Machine Learning.

- **For example:** A Data Security Administrator wants to create a content classifier using the phrase “Date of Discharge”. This classifier can be used in a discovery policy to help locate sensitive patient records and in a DLP policy to control how those documents are shared. In this case the Data Security Administrator will use the “Patterns & Phrases” Content Classifier.

**Resources** are logical groupings to tailor a policy to apply to a smaller group. In a standard policy, the default for source and destination is *all* users, computers, networks, and devices. If the policy needs to be applied to only a subset of one of these groupings, a Resource can be defined to be used in the policy as either the source or destination.

There are multiple resource types that can be used to identify a customized source or destination. A few are these are:

**Business Units** – which is a grouping that can consist of users, groups, networks and domains that form a logical business unit within the company

**Custom User Directory Groups** – which is a logical grouping of directory entries created with advanced LDAP queries

**Endpoint Applications** – which is one or more applications defined in a logical grouping that can be monitored by the Endpoint agent running on client workstations

Similar to the function provided for customizing source and destination, Resources can also be used to define customized actions or remediation. Resource groupings that can be used for purposes of remediation or taking a custom action when a Policy triggers include:

Action Plans

Remediation Scripts

Custom Notifications



# DLP CONFIGURING DLP POLICIES

## Policy Elements (8.4)

### Content Classifiers

The screenshot shows the Forcepoint Security Manager interface with the 'DATA' tab selected. The left sidebar contains a 'Main' menu with 'Policy Management' highlighted. A dropdown menu is open from 'Policy Management', showing 'DLP Policies', 'Discovery Policies', 'Content Classifiers', and 'Resources'. The 'Content Classifiers' dropdown is further expanded, showing a list of options: 'Patterns & Phrases', 'File Properties', 'File Fingerprinting', 'Database Fingerprinting', and 'Machine Learning'. The main dashboard area shows a 'Health Alert Summary' with three status messages: 'Your subscription is valid', '9 data loss prevention and mobile policies are configured', and '5 discovery policies are configured'.

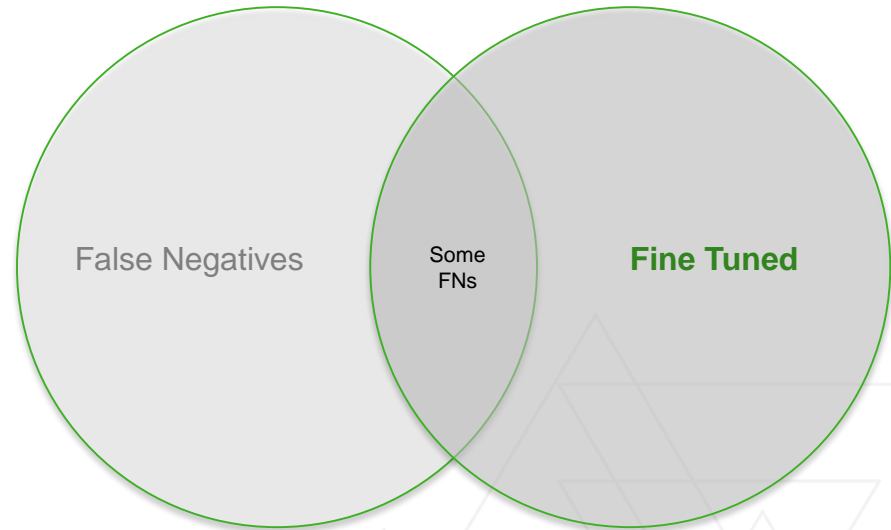
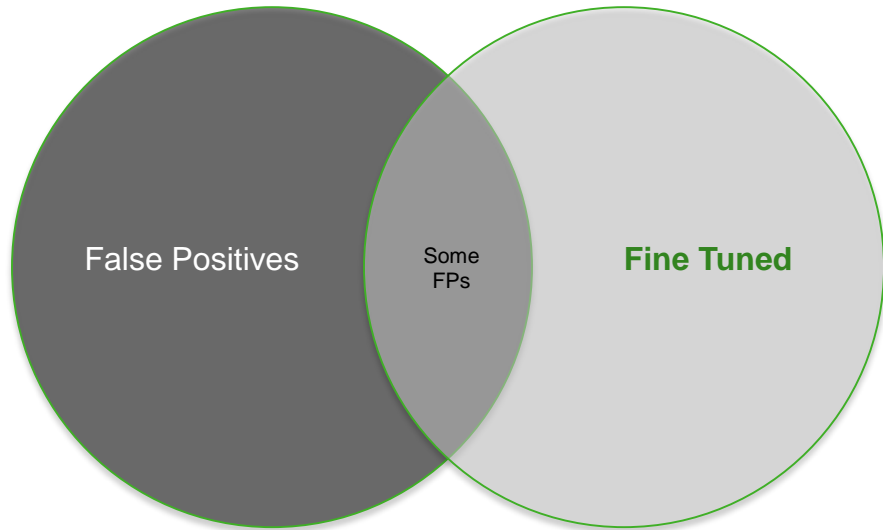
### Resources

The screenshot shows the Forcepoint Security Manager interface with the 'DATA' tab selected. The left sidebar contains a 'Main' menu with 'Policy Management' highlighted. A dropdown menu is open from 'Policy Management', showing 'DLP Policies', 'Discovery Policies', 'Content Classifiers', and 'Resources'. The 'Resources' dropdown is further expanded, showing a list of options: 'User Directory Entries', 'Custom User Directory Groups', 'Custom Users', 'Custom Computers', 'Networks', 'Domains', 'Business Units', 'URL Categories', 'Endpoint Devices', 'Endpoint Applications', 'Endpoint Application Groups', and 'Endpoint Printers'. The main dashboard area shows a 'Health Alert Summary' with three status messages: 'Your subscription is valid', '9 data loss prevention and mobile policies are configured', and '5 discovery policies are configured'.



# DLP CONFIGURING DLP POLICIES

## False Positives vs. False Negatives



# DLP CONFIGURING DLP POLICIES

## Slide notes

After deploying a DLP policy you'll have to contend with False Positives and False Negatives.

As a rule of thumb, false positives are more secure than false negatives. However, there is an increase of administrative overhead when examining and remediating false positives.

When a **false positive** occurs, intended recipients don't receive documents that contain information that is not controlled by DLP policies. False positives also lower the trust that end users have in the Information Security team when false positives have a noticeable impact on the business.

### Example:

A Security Administrator configured a DLP policy to block any outgoing documents that contain credit card numbers. An order processor notices that receipts for orders, which contain order numbers, are also being blocked by this policy. As a result, receipts were not received by customers. In this instance, the Security Administrator selected the "Credit Card (Wide)" classifier, which identified 14 digit order numbers as credit card numbers.

When a **false negative** occurs documents that contain DLP policy protected content are not detected, and are sent to unauthorized recipients, computers, or devices.

### Example:

A health care organization has a database that contains social security numbers of patients. The Security Administrator of this organization configured a DLP policy using the "US SSN (Narrow)" classifier to ensure these records are protected. However, several tables in the database contained social security numbers only. As a result, a Database Administrator mistakenly sent social security numbers to a less secure server on the network. These records were not detected because the Narrow classifier requires additional evidence, such as SSN related terms in proximity of the SSN.

In the case of False Positives or False Negatives, it is important to test policy settings in a non-production environment before rolling them out in your production environment. If a non-production environment isn't available you can select a test set of end users to add to a test policy as well.

Ultimately, a well monitored incident list and well maintained policy will lead to less False Positives and False Negatives.

**However, it's important to note that you cannot completely eliminate False Positives and False Negatives. In both cases, continued investigation for each instance is recommended in order to bring False Positives and False negatives into a reasonable threshold.**



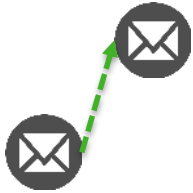


# DLP FORCEPOINT DLP BEST PRACTICES

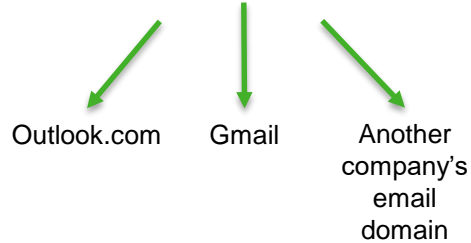


# DLP FORCEPOINT DLP BEST PRACTICES

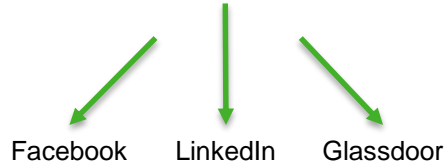
## External Controls



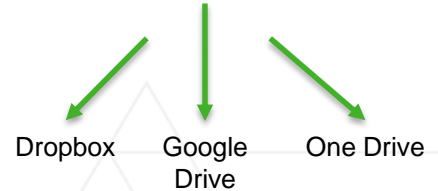
### Email (external)



### Web (Social)



### Web (Cloud Storage)



# DLP FORCEPOINT DLP BEST PRACTICES

## Slide notes

Determining how data is shared will allow your organization to implement the needed controls to ensure sensitive data is not shared inappropriately.

### **Example:**

A user working in the Marketing Department is part of a special project to develop new marketing materials for a new product that has not yet been publicly announced. To allow for extra work on the materials at home the user creates an account with Adobe Creative Cloud and uploads his work to the shared drive through a web browser. The data is uploaded over an https connection allowed through the Proxy and is not detected by existing DLP policies. The data is compromised on the Adobe servers and the marketing materials for the new product are made public prematurely.

### **The Best Practice in this case would be:**

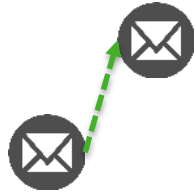
Organizations should create a comprehensive set of DLP policies that address all appropriate external channels that could potentially be utilized for sharing data. It's critical for an organization to evaluate and identify not only the common methods for sharing data but also those that present alternate methods such as social media, blogs, and SaaS applications, as part of the overall DLP plan.



# DLP FORCEPOINT DLP BEST PRACTICES

## Internal Controls

### Channels



Endpoint  
Email



Endpoint  
Printing



Endpoint  
Application



Endpoint  
Removable Media



Endpoint  
LAN



# DLP FORCEPOINT DLP BEST PRACTICES

## Slide notes

The typical implementation of data loss prevention is to prevent data from leaving the internal network. However, a good DLP strategy should include internal controls as well. Sensitive information should be controlled in a manner where those who are not authorized to view certain sensitive documents cannot receive those documents, even through internal channels. Internal data loss prevention controls also help prevent data leak from a careless, or potentially rogue employee.

### **Example:**

A member of the networking team has access to the document that contains information about the company's network. A member of the desktop support team requests this information to try to resolve a network issue that typically requires the assistance of a Network Engineer. The desktop support team member receives the file and places it on a file share that anyone in the company can access. The document that contains the information about the company's internal network is later compromised.

### **As a Best Practice in this scenerio:**

DLP policies that include internal channels and destinations, as well as removable media should have been configured.



# DLP FORCEPOINT DLP BEST PRACTICES

## Fingerprinting

Target only appropriate folders and files



## NLP Scripts

Name	Type	Classifier Type
<a href="#">10 Digit Account Number with support</a>	Predefined	Regular Expression
<a href="#">10-Digit Slovak and Czech Birth Numbers</a>	Predefined	Script
<a href="#">10K Form</a>	Predefined	Script
<a href="#">10K Form (Non Standard Fiscal Year)</a>	Predefined	Script
<a href="#">10Q Form</a>	Predefined	Script
<a href="#">10Q Form (Non Standard Fiscal Year)</a>	Predefined	Script
<a href="#">1st Magnetic Track</a>	Predefined	Script
<a href="#">1st Magnetic Track (Chinese cards)</a>	Predefined	Script
<a href="#">2nd Magnetic Track</a>	Predefined	Script
<a href="#">2nd Magnetic Track (Chinese cards)</a>	Predefined	Script
<a href="#">3rd Magnetic Track</a>	Predefined	Script
<a href="#">3rd Magnetic Track (Chinese cards)</a>	Predefined	Script
<a href="#">401(k) form terms</a>	Predefined	Dictionary
<a href="#">403(b) form terms</a>	Predefined	Dictionary
<a href="#">5-8 Digit Account Number with support</a>	Predefined	Regular Expression
<a href="#">5-9 Digit Account Number</a>	Predefined	Regular Expression
<a href="#">9 Digit Account Number with support</a>	Predefined	Regular Expression
<a href="#">9-Digit Slovak and Czech Birth Numbers</a>	Predefined	Script
<a href="#">Aadhaar Number</a>	Predefined	Script
<a href="#">account 5 to 8 digits</a>	Predefined	Regular Expression
<a href="#">Account and Password</a>	Predefined	Regular Expression
<a href="#">Account Number 5-9 digits, with Hebrew or ...</a>	Predefined	Regular Expression
<a href="#">Account Number 6-13 digits</a>	Predefined	Regular Expression
<a href="#">Account Number 6-13 digits near Account Nu...</a>	Predefined	Regular Expression
<a href="#">Account Number Terms Hebrew and English Support</a>	Predefined	Regular Expression
<a href="#">ActionScript source code</a>	Predefined	Script
<a href="#">Adult (Chinese)</a>	Predefined	Dictionary
<a href="#">Adult (Dutch)</a>	Predefined	Dictionary
<a href="#">Adult (English)</a>	Predefined	Dictionary
<a href="#">Adult (French)</a>	Predefined	Dictionary
<a href="#">Adult (German)</a>	Predefined	Dictionary
<a href="#">Adult (Italian)</a>	Predefined	Dictionary



# DLP FORCEPOINT DLP BEST PRACTICES

## Slide notes

When configuring Fingerprinting tasks you could choose to scan all files and folders. However, as a best practice you should only scan files and folders that contain information that actually need to be protected. Scanning all files and folders runs the risk of the crawler overloading system resources, which could result in incomplete scans and potential performance issues.

In addition to the targeted scan, you may consider fingerprinting only files that contain data that does not already fall into a pre-defined classification, such as CCN, PII, or PCI. Doing so will unnecessarily utilize resources. Typically, Fingerprinting is used to protect proprietary data.

When possible, use predefined scripts instead of Regular Expressions. The Forcepoint Natural Language Processing (NLP) scripts are more accurate because they not only analyze file content similar to a regex, but they analyze the *context* of the file content as well.



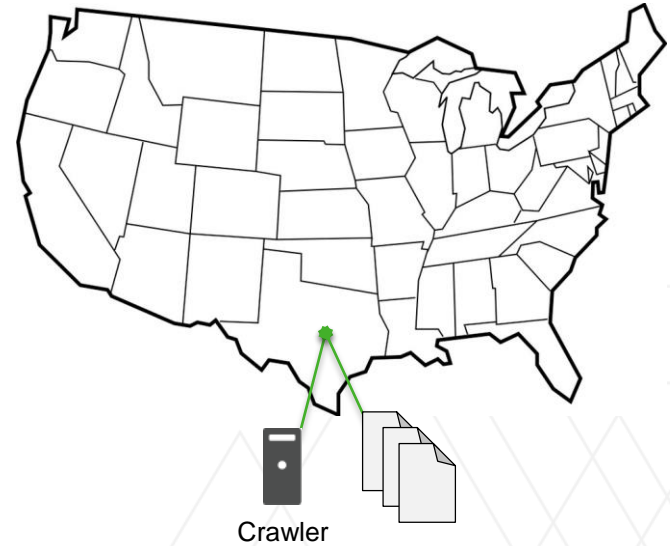
# DLP FORCEPOINT DLP BEST PRACTICES

## Discovery

✗



✓





# DLP FORCEPOINT DLP BEST PRACTICES

## Slide notes

While configuring your Discovery task ensure that you select a Crawler server that is closest to the files and folders you would like to scan. This is because there could be a large volume of files being scanned across the WAN, which could cause a bandwidth issue, OR bandwidth across the WAN could delay large scanning jobs. You must also consider the quantity and size of the documents that you are scanning as well as the complexity of the policy that enforces the scan.















# DLP TROUBLESHOOTING DLP ISSUES



# DLP TROUBLESHOOTING DLP ISSUES

## Common Errors

ERROR: Failed to deploy Endpoint Server <server FQDN>. Reason: Endpoint initialization failed.  
Reason: Failed to create policy deployment XML: **Error while transforming**

Name	Status	Deployment Results
 TRITON AP-DATA Server on triton-mon.cashton.local	 Warning	At least one child element was not deployed successfully
 Endpoint Server triton-mon.cashton.local	 Failure	Failed to deploy Endpoint Server triton-mon.cashton.local. Reason: Endpoint initialization failed. Reason: Failed to create policy deployment XML: Error while transforming
 Policy Engine triton-mon.cashton.local	 Success	All configuration settings were committed successfully
 Forensics Repository triton-mon.cashton.local	 Success	All configuration settings were committed successfully
 Primary Fingerprint Repository triton-mon.cashton.local	 Success	All configuration settings were committed successfully
 Crawler triton-mon.cashton.local	 Success	All configuration settings were committed successfully



# DLP TROUBLESHOOTING DLP ISSUES

## Slide notes

### **Error while transforming**

This error can be triggered as a result of an improper change of the Service Account password. The Service Account password is used to decrypt data when the Deploy action is in progress. If the password is set improperly this results in mismatched keys between the current password and the files that are encrypted by the previous password.



# DLP TROUBLESHOOTING DLP ISSUES

## Common Errors

ERROR: Failed to deploy Endpoint Server <server FQDN>. Reason: Endpoint initialization failed.  
Reason: Failed to create policy deployment XML: **Error while transforming**

### Changing the TRITON AP-DATA Service Account Password

<https://support.forcepoint.com/KBArticle?id=Changing-the-TRITON-AP-DATA-service-account-password>

### Unable to Deploy Endpoint Server: Error while Transforming

<https://support.forcepoint.com/KBArticle?id=000013199>



# DLP TROUBLESHOOTING DLP ISSUES

## Slide notes

To reset the Service Account password correctly, follow the steps outlined in the “**Changing the TRITON AP-DATA Service Account Password**” KB article.

If you are already experiencing this error, follow the steps outlined in the “**Unable to Deploy Endpoint Server: Error while Transforming**” KB article.



# DLP TROUBLESHOOTING DLP ISSUES

## Common Errors

**ERROR Exception - FileDelete: apr\_file\_remove on C:\Program Files (x86)\ Websense\Data Security\ResourceResolver\ResourceResolverServerUse\GeoIpDBTmpUse\_3548575613.cpy.dat failed: The process cannot access the file because it is being used by another process.**

```
2016-11-03 13:57:02,243 workschedulerwebService      Error [Th:Thread-207] validateCredentials Error: Error code:[-711]. Error Message:[], msg:
2016-11-03 15:16:44,391 utils.SystemLogging          Error [Th:Thread-216] Failed to post a SystemLog. Code: -1, Error: (10061, 'connection refused').
2016-11-03 15:17:47,720 utils.SystemLogging          Error [Th:SchedulingThread] Failed to post a SystemLog. Code: -1, Error: (10061, 'Connection refused').
2016-11-03 15:17:53,174 win32FileBrowser            Error [Th:Pool Job Fingerprint Regression 1] Error while retrieving file: \[REDACTED]\Fingerprinting\ [REDACTED].Excelx File for MON
TC002.xlsx (offset 0, length 8674), Error (32, 'CreateFile', 'The process cannot access the file because it is being used by another process.')
```



# DLP TROUBLESHOOTING DLP ISSUES

## Slide notes

Another commonly reported error is the “**process cannot access the file because it is being used by another process**” error. This error is triggered by third party antivirus scanners when they actively scan directories and files that are used by the Endpoint client. Active antivirus scanners, as well as backup utilities, place file locks on files while scanning or backing up. When a file lock is active no other application, including the Endpoint Client, can access these files.

This type of error can trigger for many Endpoint files and appear in many Endpoint logs, depending on the action being executed when the error is generated. For example, in the screenshot you’ll see the same error as in the text box above it, except instead of it being triggered for a Resource Resolver file it is triggered for a file that is being fingerprinted.





# DLP TROUBLESHOOTING DLP ISSUES

## Common Errors

ERROR Exception - FileDelete: apr\_file\_remove on C:\Program Files (x86)\ Websense\Data Security\ResourceResolver\ResourceResolverServerUse/GeoIpDBTmpUse\_3548575613.cpy.dat failed: **The process cannot access the file because it is being used by another process.**



**Download Process Monitor (981 KB)**

**Run now** from [Sysinternals Live](#).



# DLP TROUBLESHOOTING DLP ISSUES

## Slide notes

If you receive errors similar to these examples, or if you suspect that an active virus scanner may be causing a problem, you may run Process Monitor to confirm your suspicion.

You can scan a filtered directory or file with Procmon to discover what is writing to or reading from the directory or file. Some executables to look out for include executable from:

- Sophos
- McAfee
- Trend



# DLP TROUBLESHOOTING DLP ISSUES

## Common Errors

### For Windows Endpoints

<https://support.forcepoint.com/KBArticle?id=v8-0-Excluding-Websense-Endpoints-from-Antivirus-Scanning>

### For Servers and Mac Endpoints

[http://www.websense.com/content/support/library/deployctr/v83/dic\\_av\\_exclude.aspx](http://www.websense.com/content/support/library/deployctr/v83/dic_av_exclude.aspx)

Below are the list of AV Exclusions required

#### Endpoint Installation Folder:

C:\Program Files\Websense\Websense Endpoint  
C:\Program Files(x86)\Websense\Websense Endpoint  
Custom folder location defined by the customer

#### DLLs:

C:\windows\system32\QIPCAP.dll  
C:\windows\system32\QIPCAP64.dll  
C:\windows\system32\QIPOverlay.dll

#### SYS files:

C:\windows\system32\drivers\cwnep.sys  
C:\windows\system32\drivers\qip.sys  
C:\windows\system32\drivers\qiptdi.sys  
C:\windows\system32\drivers\rnetcore.sys  
C:\windows\system32\drivers\WNetCore.sys  
C:\windows\system32\drivers\WFPRedir.sys  
C:\windows\system32\drivers\WsOMFlt.sys

For all endpoint clients, exclude:

- Endpoint processes: **wepsvc.exe** and **dserui.exe**

For TRITON AP-ENDPOINT DLP, also exclude:

- **EndpointClassifier.exe** and **kvoop.exe**



# DLP TROUBLESHOOTING DLP ISSUES

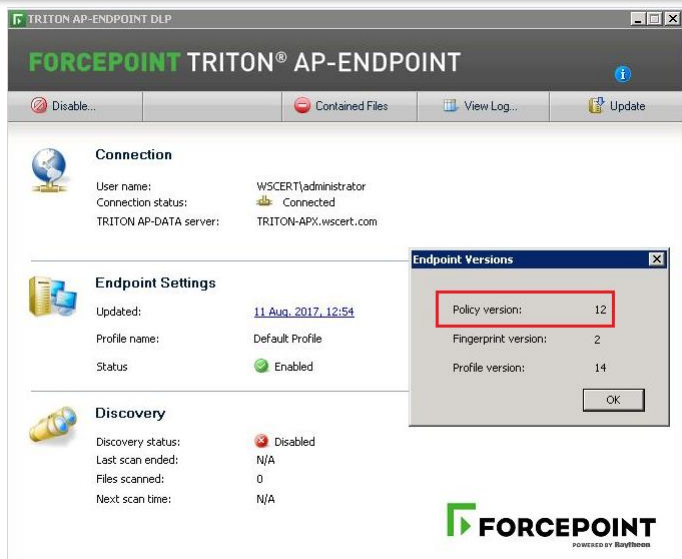
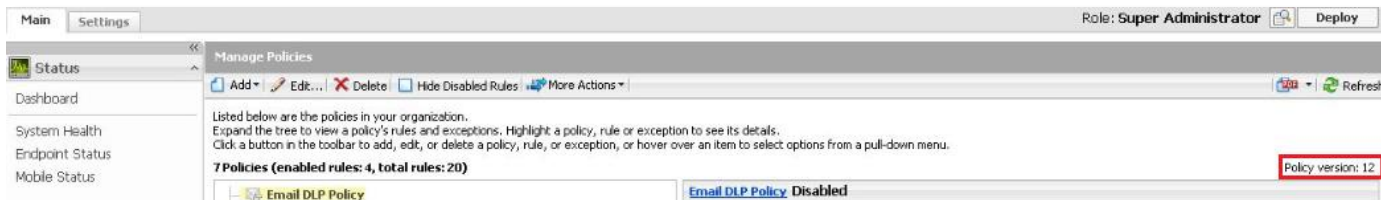
## Slide notes

You may also review the “**Excluding TRITON AP-ENDPOINT from Antivirus Scanning**” and “**Excluding Forcepoint files from antivirus scans**” KB articles for a list of files to exclude from your AV scanner, for future reference.



# DLP TROUBLESHOOTING DLP ISSUES

## Common Errors



# DLP TROUBLESHOOTING DLP ISSUES

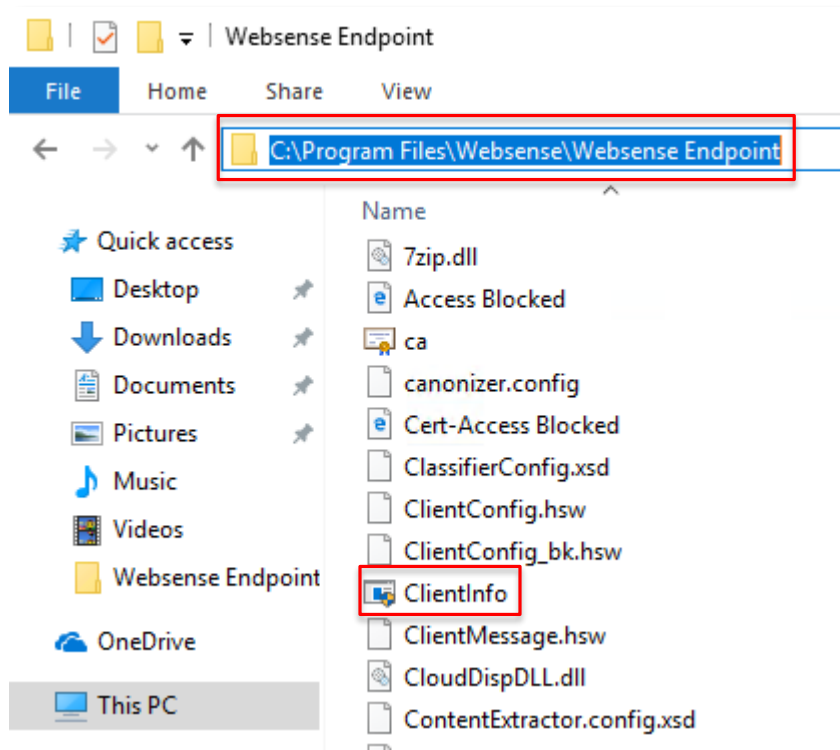
## Slide notes

Occasionally, you may notice that some end users may not be adhering to a recent policy change. The first item to check is the database version on the server side and the client side. The end user should be able to do a manual update from the Endpoint Client. If the policy version does not update that may indicate a network issue between the client and server. If this issue occurs for a roaming users the user may need to establish a VPN connection in order to pull down the policy update.



# DLP TROUBLESHOOTING DLP ISSUES

## Collecting clientinfo.log



## Other useful information to provide to Support

- Endpoint version
- Operating system version
- Browser type
- Browser version
- Whether the issue exist in another browser or version



# DLP TROUBLESHOOTING DLP ISSUES

## Slide notes

If end users encounter issues with the DLP Endpoint Client, collecting the clientinfo.log file is a recommended first step. If you need to open a support case for the issue, attach the clientinfo.log to the case. Also ensure that you provide the following information.

- Endpoint version
- Operating system version
- Browser type
- Browser version
- Whether the issue exist in another browser or browser version

These additions to the case will reduce the time it takes for Technical Support to request it after the case is already opened.





QUESTIONS? THANK YOU!



**FORCEPOINT**

POWERED BY **Raytheon**

Protecting the human point.

[mcswebinar@forcepoint.com](mailto:mcswebinar@forcepoint.com)

