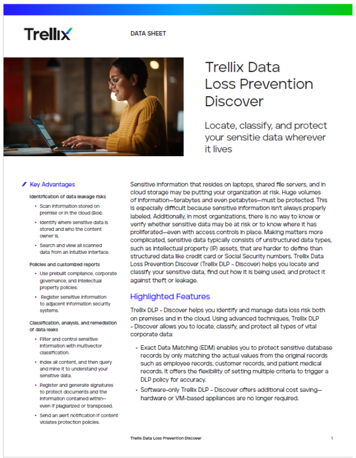
Trellix

carahsoft.

Trellix Data Loss Prevention - Discover

Locate, classify, and protect your sensitive data wherever it lives



Trellix DATA SHEET

Trellix Data Loss Prevention Discover

Locate, classify, and protect your sensitie data wherever it lives

Key Advantages

Identification of data leakage risks

- Scan information stored on premise or in the cloud (Box).
- Identify where sensitive data is stored and who the content owner is.
- Search and view all scanned data from an intuitive interface.

Policies and customized reports

- Use prebuilt compliance, corporate governance, and intellectual property policies.
- Register sensitive information to adjacent information security systems.

Classification, analysis, and remediation of data leaks

- Filter and control sensitive information with multivector classification.
- Index all content, and then query and mine it to understand your sensitive data.
- Register and generate signatures to protect documents and the information contained within—even if plagiarized or transposed.
- Send an alert notification if content violates protection policies.

Sensitive information that resides on laptops, shared file servers, and in cloud storage may be putting your organization at risk. Huge volumes of information—terabytes and even petabytes—must be protected. This is especially difficult because sensitive information isn't always properly labeled. Additionally, in most organizations, there is no way to know or verify whether sensitive data may be at risk or to know where it has proliferated—even with access controls in place. Making matters more complicated, sensitive data typically consists of unstructured data types, such as intellectual property (IP) assets, that are harder to define than structured data like credit card or Social Security numbers. Trellix Data Loss Prevention Discover (Trellix DLP - Discover) helps you locate and classify your sensitive data, find out how it is being used, and protect it against theft or leakage.

Highlighted Features

Trellix DLP - Discover helps you identify and manage data loss risk both on premises and in the cloud. Using advanced techniques, Trellix DLP - Discover allows you to locate, classify, and protect all types of vital corporate data:

- Exact Data Matching (EDM) enables you to protect sensitive database records by only matching the actual values from the original records such as employee records, customer records, and patient medical records. It offers the flexibility of setting multiple criteria to trigger a DLP policy for accuracy.
- Software-only Trellix DLP - Discover offers additional cost saving—hardware or VM-based appliances are no longer required.

Trellix Data Loss Prevention Discover 1

Thank you for downloading this Trellix data sheet. Master Government Aggregator® and Distributor for Trellix's Cybersecurity solutions available via GSA, NASPO, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Trellix's solutions, please check out the following resources and information:

For additional resources:
carah.io/TrellixResources

For upcoming events:
carah.io/TrellixEvents

For additional Trellix products:
carah.io/TrellixSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Trellix@carahsoft.com
855-462-2333

To purchase, check out the contract vehicles available for procurement:
carah.io/TrellixContracts

For more information, contact Carahsoft or our reseller partners:
Trellix@carahsoft.com| 855-462-2333

DATA SHEET

Trellix Data Loss Prevention Discover

Locate, classify, and protect your sensitie data wherever it lives

Key Advantages

Identification of data leakage risks

- Scan information stored on premise or in the cloud (Box).
- Identify where sensitive data is stored and who the content owner is.
- Search and view all scanned data from an intuitive interface.

Policies and customized reports

- Use prebuilt compliance, corporate governance, and intellectual property policies.
- Register sensitive information to adjacent information security systems.

Classification, analysis, and remediation of data leaks

- Filter and control sensitive information with multivector classification.
- Index all content, and then query and mine it to understand your sensitive data.
- Register and generate signatures to protect documents and the information contained within—even if plagiarized or transposed.
- Send an alert notification if content violates protection policies.

Sensitive information that resides on laptops, shared file servers, and in cloud storage may be putting your organization at risk. Huge volumes of information—terabytes and even petabytes—must be protected. This is especially difficult because sensitive information isn't always properly labeled. Additionally, in most organizations, there is no way to know or verify whether sensitive data may be at risk or to know where it has proliferated—even with access controls in place. Making matters more complicated, sensitive data typically consists of unstructured data types, such as intellectual property (IP) assets, that are harder to define than structured data like credit card or Social Security numbers. Trellix Data Loss Prevention Discover (Trellix DLP - Discover) helps you locate and classify your sensitive data, find out how it is being used, and protect it against theft or leakage.

Highlighted Features

Trellix DLP - Discover helps you identify and manage data loss risk both on premises and in the cloud. Using advanced techniques, Trellix DLP - Discover allows you to locate, classify, and protect all types of vital corporate data:

- Exact Data Matching (EDM) enables you to protect sensitive database records by only matching the actual values from the original records such as employee records, customer records, and patient medical records. It offers the flexibility of setting multiple criteria to trigger a DLP policy for accuracy.
- Software-only Trellix DLP - Discover offers additional cost saving—hardware or VM-based appliances are no longer required.

Specifications

Content Types

Supports file classification of more than 300 content types, including:

- Box cloud storage
- Microsoft Office documents
- Adobe files
- Multimedia files
- Source code
- Design files
- Archives
- Encrypted files
- Built-in policies
- Intellectual property

Repositories Supported

- Common internet file system/ server message block (CIFS)
- Microsoft SharePoint
- Databases: Microsoft SQL, Oracle, DB2, MySQL Enterprise

- Fully deployable and manageable by Trellix ePolicy Orchestrator (Trellix ePO) software—it shares the same management extension and data loss prevention (DLP) policy as Trellix Data Loss Prevention Endpoint (Trellix DLP - Endpoint).
- Fully aligned with Trellix DLP - Endpoint classification capabilities.
- Compatible with Microsoft Windows 2008 R2, Windows 2012, Windows 2016 servers, and .
- Supports distributed deployments that leverage idle capacity on existing servers and may be deployed over a wide geographical area.
- Optical Character Recognition (OCR) recognizes and protects text in scanned images and forms. It allows customers to inspect embedded graphic files for sensitive content across network resources including files shares, SharePoint, and Databases.[1]

Preventing Loss of Sensitive Data

From source code to trade secrets to strategic business plans, IP and other information assets are critical to your brand, public reputation, and competitive edge. Protecting data during transmission is critical, but securing sensitive data before it is inappropriately accessed or moved and understanding where it resides should be your first line of defense.

Trellix DLP - Discover helps you protect your organization against data loss. Unlike legacy solutions that expect you to know exactly what content you want to protect, Trellix DLP - Discover provides comprehensive coverage for obvious information and helps you find the non-obvious.

Classify Complex Data

Trellix DLP - Discover empowers your organization to protect all kinds of sensitive data—from common, fixed-format data to complex, highly variable intellectual property. By combining the inputs from these object-classification mechanisms, Trellix DLP - Discover is able to build a highly accurate, multivector classification, which is used to filter and control sensitive information and to perform searches that identify hidden or unknown risks.
Object classification mechanisms include:

- **Multilayer classification:** Covers both contextual information and content in a hierarchical format
- **Document registration:** Generates signatures of information as it changes
- **Grammar analysis:** Detects

Document Registration

Documents can be registered from any CIFS repository. Signatures from registered documents can be used locally for detecting proliferation of sensitive material or be made available to other Trellix DLP Appliances.

Reporting

The powerful analytics engine for incident and search result views allows you to customize summary views based on any two contextual pivot points. List and detail views, as well as summary views with trending, are available. Multiple customizable prebuilt and customizable reports are provided with the system.

grammar or syntax of anything from text documents to spreadsheets to source code

- **Statistical analysis:** Tracks how many times a signature, pattern, or keyword match occurred in a particular document or file
- **File classification:** Identifies content types regardless of the extension applied to the file or compression
- **Document Classification:** Discover rules for CIFS, Box, and SharePoint now support the reaction Classify File As. This reaction embeds the classification ID into file formats that support embedded classifications.

Determining What Information to Protect

To identify information and proliferation risks, Trellix DLP - Discover can be configured to scan specific repositories and identify data for explicit protection. Additionally, all data crawled by Trellix DLP - Discover is indexed and made accessible through an intuitive interface, allowing you to quickly search for data that may be sensitive in order to understand who owns the content and where it is stored.

Defining Policies for Protection

Once you know what information to protect, Trellix DLP - Discover can help you accurately protect that information. Trellix DLP - Discover provides intuitive and unified policy creation, reporting, and management to give you more control over your information protection strategy for data at rest. Key benefits of the policies, rules, and classifications in Trellix DLP - Discover include:

- Numerous built-in policies for a simple out-of-box experience
- Powerful rule-construction engine, from simple structured data (credit cards, Social Security numbers) to complex information (intellectual property)
- Simplified rule creation and validation by transferring search result analysis to a protection rule
- Integration with adjacent information security vectors to ensure consistent protection
- Exclusion of public documents and common text to prevent benign information from generating incidents

Software Specifications

Trellix DLP - Discover is available as a software version. Below are the minimum system requirements.

Hardware requirements

- CPU: Intel Core 2 64-bit
- RAM: 4 GB minimum
- Disk space: 100 GB minimum

Supported Platforms

- Windows Server 2008 R2 Standard, 64-bit
- Windows Server 2012 Standard, 64-bit
- Windows Server 2012 R2 Standard, 64-bit
- Windows Server 2016 Standard, 64-bit

Supported Virtualization Systems

- VMware vSphere using vCenter server versions 6.0, 6.5, or 6.7
- vCenter Server 5.0 Update 2

Trellix ePO software and agents

- Trellix ePO 5.3.3, 5.9.1, and 5.10
- Trellix agent 5.0.6, 5.5, 5.5.1

Scan Your Network for Violations

After policies are defined, Trellix DLP - Discover can be instructed to routinely scan network resources for policy violations. Flexible scheduling options are available to perform continuous, daily, weekly, or monthly scans.

Trellix DLP - Discover automatically scans all accessible resources, including laptops, desktops, servers, document repositories, portals, and file transfer locations for policy violations. You can define scan groups based on IP addresses, subnets, ranges, or network paths. You can also focus scan operations based on specific parameters, such as scanning only "My Documents" for all users and not system folders, or looking for files owned by specific users or of a certain type or size.

Review and Remediate Violations

Trellix DLP - Discover eliminates or minimizes proliferation of sensitive material through integrated incident workflow and case management. If Trellix DLP - Discover finds content that violates protection policies, it generates incidents and sends notifications. Incidents created by Trellix DLP - Discover can be added to the case management framework, which allows you to involve specialists from numerous organizations within the company to take action on the violation. Additionally, risk dashboards provide easy ways for security personnel to see the profile of policy violations and generate reports based on any data-at- rest parameter of interest.

Capture and Analyze Stored Data

In addition to scanning network resources to detect policy violations, Trellix DLP - Discover also indexes all content found at rest in the network and provides you with the ability to query and mine this information to understand your sensitive data. Trellix DLP - Discover lets you quickly understand your sensitive data, how it is used, who owns it, where it is stored, and where it has proliferated.

1. Integrated with DLP - Discover—no separate server required. An add-on feature to Trellix Total Protection for DLP sku.

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.