Trellix Data Loss Prevention

TRELLIX DATA LOSS PREVENTION

is a suite of products that protects against data loss by identifying and securing data within your network and offline. Trellix DLP policies help you understand the types of data on your network, how the data is accessed and transmitted, and if the data contains sensitive or confidential information.

KEY FEATURES:

Trellix DLP provides comprehensive protection for all potential leaking channels, including removable storage devices, the cloud, email, instant messaging, web, printing, clipboard, screenshot, and file-sharing applications.

Compliance enforcement — Ensure compliance by addressing day-to-day user actions, such as emailing, cloud posting, and downloading to removable media devices.

Advanced protection — Apply fingerprinting, classification, and file tagging to secure sensitive, unstructured data, such as intellectual property and trade secrets.

User education — Provide real-time feedback through educational pop-up messages to help shape corporate security awareness and culture.

Centralized management — Integrate with Trellix ePO software to streamline policy and incident management.

Scanning and discovery — Scan files and databases stored on local endpoints, shared repositories, or the cloud to identify sensitive data.

Trellix DLP products

TRELLIX DEVICE CONTROL

Controls the use of removable media on endpoints. Trellix Device Control contains a subset of the protection rules in Trellix DLP Endpoint for Windows and Mac.

KEY FEATURES:

- Controls what data can be copied to removable devices, or controls the devices themselves. It can block devices completely or make them read-only.
- Provides protection for USB drives, smartphones, Bluetooth devices, and other removable media.
- Prevents executables on removable media from running. Exceptions can be made for required executables such as virus protection.

TRELLIX DLP ENDPOINT

Agent-based solution that inspects user actions. It scans data-in-use on endpoints and blocks or encrypts unauthorized transfer of data identified as sensitive or confidential. The Endpoint Discovery feature scans local file system and email storage files and applies rules to protect sensitive content.

KEY FEATURES:

- Trellix DLP Endpoint includes all Trellix Device Control features.
- Classification engine applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied.
- Protection rules apply the classification criteria and other definitions to protect the sensitive content.
- Protects against data loss from: clipboard software, cloud applications, email, network shares, printers, screenshots, application file access, web posts, removable storage, local file system files
- The Trellix DLP Endpoint discovery crawler runs on the local endpoint, searches local file system and email storage files and applies policies to protect sensitive content.

TRELLIX DLP PREVENT

Works with your web proxy or MTA server to protect web and email traffic.

KEY FEATURES:

- Trellix DLP Prevent interacts with your email and web traffic, generates incidents, and records the incidents for subsequent case review.
- Proactively enforces policies for all types of information sent over email or web.
- Enforces policies for the information you know is sensitive and the information you might not know about.
- Filters and controls sensitive information to protect against known and unknown risks.
- Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use.
- Supports Optical Character Recognition (OCR) for scanning images attached to emails.

TRELLIX DLP DISCOVER

Scans network file, Box, SharePoint, and database repositories to identify and protect sensitive data by copying or moving the files, or by applying an RM policy. Registration scans extract fingerprint information from file repositories for file classification and store the signatures in a registered documents database.

KEY FEATURES:

- Detects and classifies sensitive content.
- Creates registered document signature databases.
- Moves or copies sensitive files.
- Integrates with Microsoft Rights Management Service to apply protection to files.
- Automates IT tasks, such as finding blank files, determining permissions, and listing files that changed within a specified time range.
- Supports Optical Character Recognition (OCR) for classification, remediation, and registration scans of file-based repositories.

TRELLIX DLP MONITOR

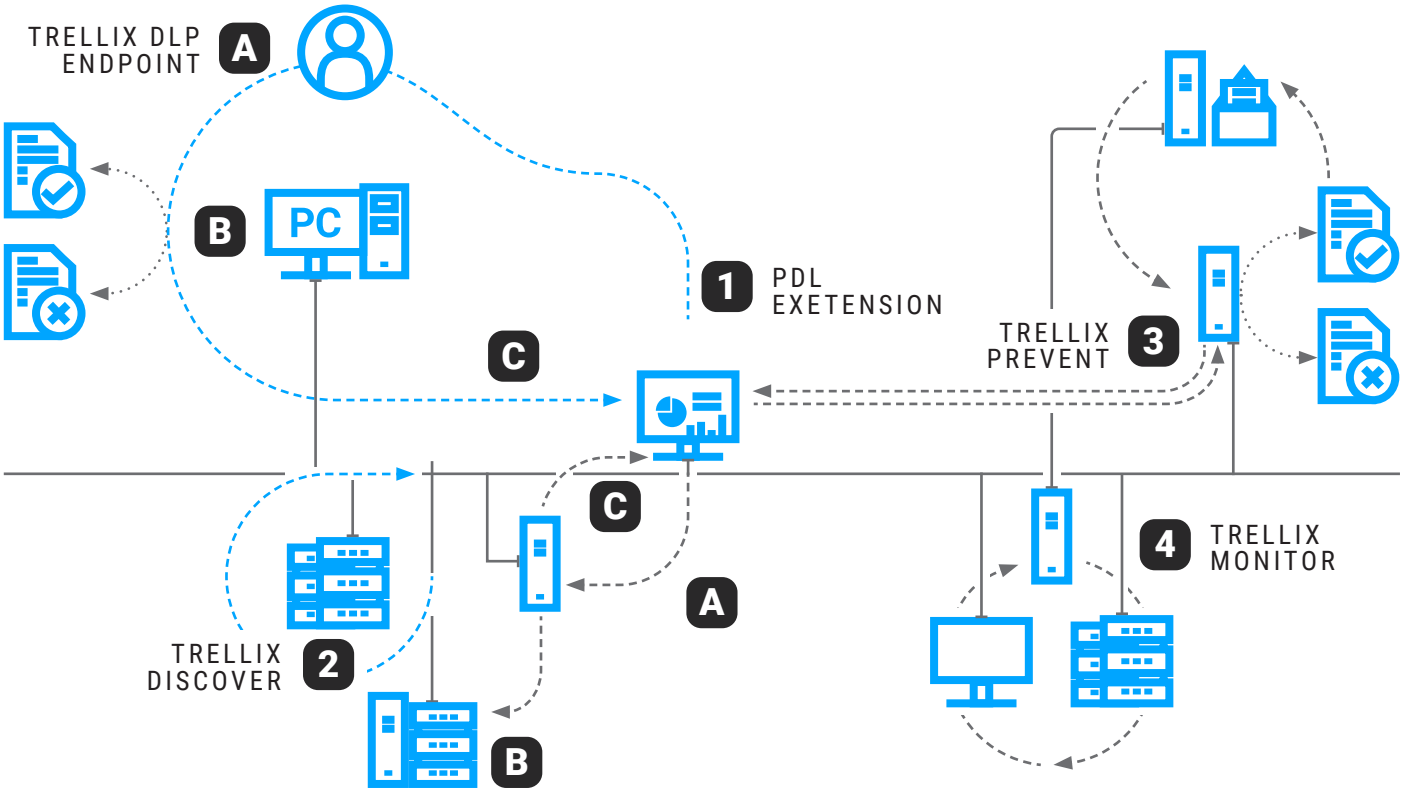
Passively scans unencrypted network traffic for potential data loss incidents.

KEY FEATURES:

- Analyzes the traffic of well-known TCP protocols to identify users or devices that send a high volume of unknown traffic, which might indicate a violation of company policy.
- Analyzes points of data loss without impacting your network to help you plan your data loss prevention strategy.
- Supports protocols that are not proxied by other email or web gateways.
- Monitors network traffic for devices that do not have Trellix DLP installed.
- Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use.
- Supports Optical Character Recognition (OCR) for scanning images attached to web posts or images found in other network traffic.

TRELLIX DLP PREVENT AND TRELLIX DLP MONITOR APPLIANCES THAT HAVE THE DLP CAPTURE FEATURE ENABLED ALSO:

- Capture content to analyze later for keywords, user activity, or file name to identify potential data loss incidents missed by active email protection, web protection, or network communication protection rules.
- Allow complete customization of email, web, or network communication protection rules for testing using the DLP Capture database.



THE FOLLOWING DIAGRAM SHOWS A SIMPLIFIED NETWORK WHERE ALL TRELLIX DLP PRODUCTS AND TRELLIX EPO ARE DEPLOYED.

1. **Administrators create policies in Trellix ePO** and deploy them to Trellix DLP Endpoint clients.
   a. Users create, save, and copy files or emails.
   b. Trellix DLP Endpoint client applies policies and either blocks or allows user actions.
   c. Applying the policies creates incidents that are sent to DLP Incident Manager for reporting and analysis.
2. **Trellix DLP Discover scans files from local** or cloud repositories and local databases, collecting file metadata.
   a. Trellix DLP Discover receives classifications and policies from Trellix ePO to apply during classification or remediation scans.
   b. DLP Server software creates registered documents databases for use in policies for Trellix DLP Discover, Trellix DLP Prevent, and Trellix DLP Monitor.
   c. Incidents from remediation scans are sent to DLP Incident Manager for reporting and analysis.
3. **Trellix DLP Prevent receives email from MTA servers and web traffic from web proxy servers.** It analyzes the email messages and web traffic, applies the Trellix DLP policies, and sends incidents and evidence to DLP Incident Manager.
4. **Trellix DLP Monitor analyzes network traffic, then creates incidents or saves evidence for the supported protocols.** It applies network communication protection rules, web protection rules, or email protection rules.