Trellix

DATASHEET

Trellix Data Loss Prevention - Monitor

Safeguard vital data

Protecting customer and employee personal privacy data—Social Security numbers, credit card numbers, or other personal information—is on everyone's mind today. Accidental disclosure of data due to employee error, lost laptops, and misplaced USB devices are security challenges for nearly every organization. To compound matters, data can be leaked or end up in the wrong hands when it's transmitted and shared through web applications like Google Gmail, Yahoo! Mail, instant messaging, and Facebook. Trellix Data Loss Prevention - Monitor (Trellix DLP - Monitor) is a high-performance data loss prevention solution that can analyze all internet communications and determine if information is going where it shouldn't. It helps you minimize the workload for your security team, meet compliance requirements, and safeguard intellectual property and other vital assets.

Key Advantages

- **Fully unified with Trellix ePolicy Orchestrator (Trellix ePO) software:** Share common policies, incident and case management with Trellix DLP - Endpoint.
- **High-performance and scalable:** Cluster up to eight appliances with 6 Gbps scanning bandwidth. Comprehensive analysis: Detect more than 300 unique content types over any port and any applications.
- **Comprehensive analysis:** Detect more than 300 unique content types over any port and any applications.
- **Convenient built-in policies:** Provide a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use.

Monitor, Track, and Report on Data in Motion

No matter what your business, you need the visibility to identify sensitive information over any application, any protocol, any port, and in any form—with a high degree of accuracy.

With Trellix DLP - Monitor, you can gather, track, and report on the data in motion across your entire network—in real time—to find what and how information travels between your users and other organizations. A high-performance, purpose-built appliance that uniquely detects more than 300 content types traversing any port or protocol, Trellix DLP - Monitor can help you uncover threats to your data and take action to protect your organization against data loss. In addition, through user notification, Trellix DLP - Monitor can educate your users on data loss violations to change behaviors without effort.

Scan and Analyze Information in Real Time

Integrated into the network using a SPAN or tap port, Trellix DLP - Monitor performs real-time scanning and analysis of network traffic. With more than 150 pre- built rules, ranging from compliance to acceptable use to intellectual property, Trellix DLP - Monitor matches entire and partial documents—including fine-grained plagiarism—to its comprehensive set of rules. This enables you to detect anomalies in network traffic, no matter how large or small.

Discover Risks Not Previously Considered

Through detailed classification, indexing, and storage of all network traffic—not just information that matches its real-time rules—Trellix DLP - Monitor allows you to quickly leverage historical information to understand what data is sensitive, how it is being used, who is using it, and where it is going. Additionally, you can perform granular investigation and historical inspection of information to detect risk events and data exposure that may not have been previously considered. And when deployed in conjunction with Trellix DLP - Discover, you can also identify where data is stored on your network and who owns it.

View Incident Reports to Inform Action

Once traffic is scanned, analyzed, and classified by its classification engine, Trellix DLP - Monitor stores all the pertinent information in a proprietary database. Using an intuitive search interface, you can view comprehensive reports of your information, who is sending it, where it is going, and how it is being sent—so you can determine what, where, and how informationis leaking. With this knowledge, you can take action to address these threats by applying a range of actions to ensure

Specifications

- **System throughput:** Classify content at up to 800 Mbps, without sampling.
- **Network integration:** Integrates passively into the network using either a SPAN port or a physically inline network tap (optional).
- **Clustering capability:** Cluster up to eight appliances at up to 6 Gbps performance.
- **Supports file classification of more than 300 content types, including:**
  - Office documents
  - Multimedia files
  - P2P
  - Source code
  - Design files
  - Archives
  - Encrypted files
- **Includes protocol handlers for:**
  - FTP
  - HTTP
  - IMAP
  - IRC
  - LDAP
  - POP3
  - SMB
  - SMTP
  - Telnet

compliance with regulations and protect sensitive data.

Classify All Types of Data

Trellix DLP - Monitor empowers your organization to scan all kinds of sensitive data—from common, fixed- format data to complex, highly variable intellectual property. By combining these object-classification mechanisms, Trellix DLP - Monitor builds a highly accurate, detailed classification engine that filters sensitive information and performs 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:** Includes signatures of information as it changes
- **Grammar analysis:** Detects grammar or syntax of anything from text documents to spreadsheets to source code
- **Statistical analysis:** Tracks how many times a signature, grammar, or biometric match occurred in a particular document or file
- **File classification:** Identifies content types regardless of the extension applied to the file or compression

Forensic and Rule Tuning Capability

Unique capture technology enables you to leverage your own historical data to implement a much faster, efficient deployment—no more guessing, months of trial and error, or business disruption. This makes it easy to fine-tune DLP rules (including classification tuning) for accuracy based on your ever-changing business needs. Capture technology can also aid in forensic investigation by acting as a digital recorder and by replaying after-the- fact DLP incidents for thorough investigation. Capture technology is available either as a virtual environment, or as a 2U 16TB storage array connected to a NDLP 6600 appliance via a SAS cable.

Form Factor and Appliance Options

Trellix DLP - Monitor is available as a hardware appliance with the option of a virtual appliance.

Visit Trellix.com to learn more.