Hillstone Data Loss Prevention (DLP)

The Hillstone Data Loss Prevention (DLP) system combines cutting-edge image and text recognition with behavioral analysis to safeguard sensitive data. It offers real-time monitoring and control over the transmission of critical information, effectively preventing the leakage of files like contracts, design documents, and source code across networks and endpoints. Hillstone DLP finds applications across diverse industries, including government, finance, and education. It proves particularly valuable in scenarios where data sensitivity and compliance requirements are paramount, offering users an efficient and cutting-edge data security solution.

Product Highlights

Multifaceted Security Policy

Hillstone DLP offers a comprehensive security management approach that covers organizational, user, data, and network perspectives. The goal is to effectively control the external transmission of critical data.

Precise Image and Text Recognition

Hillstone DLP significantly improves detection accuracy by up to 90% compared to traditional solutions. This is achieved through the utilization of natural language processing content recognition technology based on semantic signatures and Optical Character Recognition (OCR) technology for both text and image content.

Flexible Control Solutions

Hillstone DLP provides a range of control methods, including network auditing, network blocking, endpoint approval, and email control. Through comprehensive network auditing, the system systematically examines and evaluates data flow within the network. In situations where suspicious or unauthorized activities are detected, Hillstone DLP offers the capability to implement network blocking. Moreover, the endpoint approval feature ensures a granular level of control, allowing organizations to precisely manage file external transmissions. For email, the system can delete sensitive emails from a sender's outbox when outbound emails trigger blocking or approval policies, effectively preventing the unauthorized download of sensitive information. This enhances overall control over sensitive information.

Intelligent Behavioral Analysis

Through correlating and analyzing events, Hillstone DLP intelligently presents users' abnormal risk behaviors. It promptly identifies potential risks and assists in standardizing data access behavior, offering source-level protection for enterprise data security.

Features

AI-powered Content Inspection

- Support AI-powered content inspection, leveraging machine learning and natural language processing to analyze and identify thousands of semantic signatures
- Support manual adjustment of semantic similarity for desired clustering effects
- Support continuous machine learning on samples to refine data content recognition rules and enhance accuracy over time

Data Inspection

- Support rule matching using keywords, scripts, advanced semantics, dictionaries, data identifiers, and regular expressions. Dictionaries can be identified based on keyword count or weight, with the option to set negative weights. Chinese word segmentation is available for keywords, and a minimum regex hit count can be configured
- Support identifying various file formats, including common office software, compression software, network files, and image formats. Custom file formats are also supported, along with attributes like file type, size, and name
- Support structured and unstructured data fingerprint identification, including image fingerprint matching with customizable threshold settings
- Support the labeling and management of document types
- Support file fingerprinting with automatic updates from FTP, shared directories, and Git repositories at regular intervals
- Support identifying content within multi-layer compressed and nested files, and support configuring compression and nesting levels for thorough scanning
- Support content identification for individual files exceeding 50MB
- Support identification of text in images and stamps in documents

Data Classification and Grading

- Support the classification and grading of data

Network Data Protection

- Support capturing and analyzing network traffic to identify sensitive data
- Support monitoring and auditing sensitive data on network protocols such as HTTP, FTP, SMTP, POP3, IMAP, QQ, TIM, TELNET, SMB, etc.
- Support monitoring and identifying sensitive information in attachments uploaded through instant messaging software such as QQ, TIM, Feige, and FeiQ
- Support multi-dimensional configuration of network traffic monitoring based on IP, IP range, email address, URL, etc.

Endpoint User Monitoring

- Support recording endpoint user operations, including endpoint asset ownership, login account, time, operation, and sensitive data, etc.
- Support advanced queries with various combinations of conditions, including account, user, time, behavior, sensitive data, and application
- Support importing organizational structures through methods such as Active Directory (AD)
- Support configuring audit policies for operational behavior based on multiple dimensions such as organizational structure, user, email address, IP, etc., and support black and white-list policies

Endpoint Data Operation Monitoring

- Support monitoring content copy-paste and USB copying behaviors
- Support monitoring the copying or cutting of sensitive information files and pasting them into applications
- Support monitoring screen capture actions
- Support desktop screen capture for forensics

Endpoint Data Egress Monitoring

- Support monitoring behavior such as network transmission, network sharing (uploading and downloading), as well as copying from and to shared resources to applications
- Support monitoring Instant Messaging (IM) applications like QQ, TIM, and WeChat, auditing or blocking the content entered into the input fields

Endpoint Screen Watermarking

- Support the automatic loading of watermarks on the screen when opening sensitive files. The watermark content includes built-in IP, MAC, device name, username, and organizational structure, with customizable options for content, rotation angle, and transparency
- Support file printing actions, allowing the addition of customizable watermarks to the printed files

Endpoint Peripheral Control

- Support the restriction of user access to USB drives, external hard drives, flash drives, CD/DVD drives, printers, Bluetooth devices, mobile portable devices, etc
- Support control over USB drives from specific manufacturers

Endpoint Application Monitoring

- Support monitoring of data operations for specified endpoint applications.• Support application blacklists and whitelists. Applications on the whitelist can access sensitive files without any intervention, while those on the blacklist triggering access to sensitive files can be audited or blocked
- Support preventing attempts to bypass blacklists and whitelists by modifying process names
- Support monitoring processes of third-party and in-house developed applications

Endpoint Offline Protection

- Support offline protection for active endpoint policies
- Support encryption and local storage of endpoint events and logs during offline mode, with automatic upload to the server upon reconnection

Endpoint Safe Mode Protection

- Support normal operation in Windows Safe Mode, preventing employees from bypassing controls while attempting to leak sensitive information using Safe Mode

Endpoint Approval

- Support approval for external file transmission, allowing employees to choose individual or batch sensitive files for temporary external sharing
- Configurable options include setting valid external transmission periods and the number of allowed transmissions, with support for a two-tier approval process

Endpoint System Compatibility

- Compatible with Windows 7, Windows 8, Windows 10, Windows Server 2008 and newer versions

Email Protection

- Support 163/263 Enterprise Cloud Mail
- Support automatic saving of sensitive attachments for forensics; allows discarding non-sensitive ones
- Support flexible, multi-level, and customizable email approval workflows
- Supports detection of "drip-feed" data leakage (multiple small outbound transmissions)
- Support monitoring and display of key email statistics (total, sensitive, percentage) on the server details page
- Support deletion of sensitive emails from the sender's outbox to prevent unauthorized downloads when policies are triggered

Policy Management

- Support creating policy groups, and support unified or separate deployment of policies for different product modules including Hillstone network DLP and endpoint DLP
- Support response actions including auditing, alerting, blocking, labeling with classification, sending emails, logging to syslog servers, adding comments, setting status, setting attributes, restricting data retention, uploading files, and uploading event log files
- Support configuring different response actions for various leakage methods/ protocols and monitoring positions within a single policy
- Support setting the retention period for events generated by policies, automatically deleting events after the specified period
- Support configuring automated response policies

Drip Leak Detection

- Support the configuration of policies for drip leak to detect gradual data leaks over a specified period

Event Audit and Correlation Analysis

- Support advanced query conditions, including time range, module, event ID, event type, triggered policy, discovery time, triggered document, severity level,

Features (Continued)

server/endpoint, triggering IP address, department, external sender, leakage method, and other dimensions for combined queries

- Support fuzzy searches for events, allowing for the quick identification of leakage events by searching for specific sensitive information such as name, ID number, phone number, etc., that were uniquely identified within the events

Log Retention

- Support the timely and complete upload of risk event logs to a centralized management platform
- Support online preview of event attachments, with customizable watermarks for added security against sensitive information re-disclosure
- Support encrypted storage for event log
- Support retrieval of sensitive files from the management platform

Report Management

- Support analysis and statistics across dimensions such as event type, quantity, severity, department, trend, policy ranking, external transmission ranking, etc.
- Support various built-in report templates with information including organizational name, reporting time, reporter, security risk quantity, monitored time, time trend graphs, etc.
- Support sorting and summarization based on specific conditions
- Support the scheduling and delivery of weekly email reports

Permission Management

- Support role-based permission management, allowing flexible assignment of system roles
- Support multi-level permission management for administrators, with the ability to manage organizational scope and customize roles

Log Management

- Support sending event logs to third-party log collection servers through Syslog

Backup and Restore

- Support the backup and restoration of database information and policies

Version:EX-08.01-DLP-3.0R6-0324-EN-01