CHECK POINT DATA LOSS PREVENTION

PREVENT DATA LOSS

Benefits

- Save time and reduce costs when you enable our integrated DLP on any Check Point firewall
- Deploy our pre-defined policy in monitor mode in just a few minutes
- Track and control the movement of sensitive data in your organization
- Stay compliant with regulations and industry standards
- Educate users on proper data handling policy

Features

- Two options for securing data; Content Awareness and a more full-featured DLP
- Choose from 60+ or 700+ pre-defined data content types for PII, PCI, HIPAA and more
- Customize pre-defined data types or create new ones as needed
- Customizable, multi-language user notifications
- Inspect and control SMTP, FTP, HTTPS webmail and Exchange traffic

In today's world of increasing data loss events and data privacy regulations, organizations have little choice but to take action to protect sensitive data. The risk of exposure of confidential employee and customer data, legal documents, and intellectual property is high.

How do you protect data without impeding employee productivity or overloading your IT staff? Technology has evolved, but is still ultimately ineffective in understanding users' intentions. Even more difficult is the long initial learning curve inherent in traditional DLP products where administrative and CAPEX costs are high.

INTEGRATED NETWORK DATA LOSS PREVENTION

Check Point simplifies DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative data classification technologies combine user, content and process information to make accurate decisions, while UserCheck™ empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies — protecting sensitive corporate information from both intentional and unintentional loss.

Empower Users

Check Point UserCheck empowers users to remediate incidents in real time. This innovative technology alerts users of suspected breaches for instant remediation and allows quick authorization of legitimate communications. UserCheck improves security and raises awareness of data use policies by empowering users to self-administer incident handling-with options to send, discard or review the issue. Notifications occur in real-time via a pop-up from a thin agent, via a dedicated email sent to the end-user or in a browser redirect (no need to install agent).

Accurate Data Classification

Innovative Check Point data classification technologies deliver exceptionally high accuracy in identifying sensitive data including Personally Identifiable Information (PII), compliance-related data (HIPAA, SOX, PCI, etc.) and confidential business data. This is achieved through multi-parameter data classification and correlation.

Multi-protocol inspection and enforcement inspects content flows and enforces policies in the most widely used TCP protocols including: SMTP, FTP, HTTP and webmail. Pattern matching and file classification allows for the identification of content types regardless of the extension applied to the file or compression.

Track Data Movement

Prevent Unintentional Data Loss

Easy to Deploy and Manage

Rapid and Flexible Deployment

Organizations of any size can be protected from the start with pre-configured templates for immediate data loss prevention. A wide range of built-in policies and rules are included for common requirements, including regulatory compliance, intellectual property and acceptable use. Check Point DLP can be installed on any Check Point firewall, saving time and reducing costs by leveraging existing security infrastructure.

Central Policy Management

DLP is centrally managed with Check Point Security Management via a user-friendly interface. Centralized management offers unmatched leverage and control of security policies and enables organizations to use a single repository for user and group definitions, network objects, access rights and security policies across their entire security infrastructure.

Inspect SSL/TLS Encrypted Traffic

Check Point DLP is an in-line, advanced data loss prevention solution for data transmitted over networks. Scan and secure SSL/TLS encrypted traffic passing through the firewall. When traffic is passed through, the security gateway decrypts the traffic with the sender's public key, inspects and protects, then re-encrypts, sending the newly encrypted content to the receiver.

Central Event Management

Separating the needle from the haystack, SmartEvent monitors and reports only what is important. Event management includes real-time and historical graphing and reporting, incident correlation and configuring custom views of DLP events.

TWO DLP OPTIONS TO CHOOSE FROM

Check Point Content Awareness and DLP are two ways to secure organization data. Content Awareness is for customers who want basic data control features while DLP is for customers who want very granular control with the ability to use dictionary matches, scan file repositories, match by template, add watermarks to files and create their own data types using the cpcode scripting language. Here is a summary of the differences between the light-weight Content Awareness and the more full-featured DLP option.

Content Awareness in the Unified Policy	Full- featured Data Loss Prevention
▪ Content Awareness is part of the first-match Unified Policy rulebase where you add rules as needed ▪ Can be used as a policy layer in the Unified Policy ▪ Directional (inbound and outbound) control of data in each policy rule ▪ Over 60 pre-defined data content types ▪ Pattern and keyword matching ▪ File attribute-based matching ▪ Virtual System support ▪ IPv6 support	▪ DLP has a dedicated multi-match rulebase already defined and ready to use in detect mode ▪ Over 700 pre-defined data content types ▪ Pattern, keyword matching, and dictionaries ▪ File attribute-based matching ▪ Advanced inspection based on structured content ▪ Similarity to commonly-used templates ▪ Use open scripting language to create specific data-types ▪ Scan internal Exchange communications ▪ Scan data in shared directories ▪ Whitelist files and repositories ▪ Add visible or invisible watermarks to business documents ▪ Quarantine files and send a notification of potential breaches to the owner of the data

