



PRODUCT DESCRIPTION

Check Point DLP Software Blade™ is the only solution that combines technology and processes to make DLP work, helping businesses move data loss from detection to prevention by pre-emptively protecting sensitive information from unintentional loss.

DLP Software Blade

OUR CHALLENGE

In today's world of increasing data loss events, organizations have little choice but to take action to protect sensitive data. Confidential employee and customer data, legal documents, and intellectual property are being exposed. Organizations are challenged with effectively addressing this without impeding employee productivity or overloading IT staff. Technology is evolving, but ultimately ineffective in understanding user intentions. Even more difficult is trying to protect sensitive data without the long deployments, painful administration and high costs often associated with traditional DLP products.

OVERVIEW

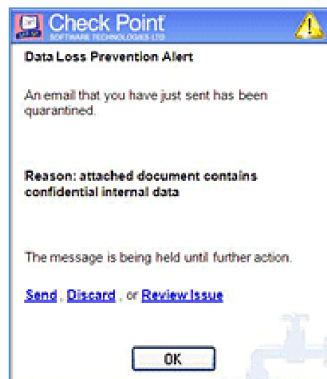
Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users 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.

Check Point UserCheck™

Check Point UserCheck empowers users to remediate incidents in real time. This innovative technology alerts users of suspected breaches, allowing for instant remediation, and allows quick authorization of legitimate communications.

UserCheck empowers users to self-administer incident handling, with options to send, discard or review the issue, improving security by raising awareness of data use policies. Real-time notification based either on a pop-up from a thin agent or via a dedicated email sent to end user (no need to install agent). Organizations benefit in several ways:

- Full prevention—enables a practical move from detection to prevention
- Self-educating system—doesn't require IT / security personnel in incident handling while educating the users on proper data sharing policies



UserCheck empowers users to remediate incidents in real time.

KEY BENEFITS

- **Prevents data loss of critical business information**
UserCheck technology empowers users to remediate incidents in real time
- **Combines technology and processes to make DLP work**
Innovative MultiSpect data classification engine combines users, content and process that delivers unrivaled accuracy
- **Easy deployment for immediate data loss prevention**
Protect sensitive data from day-1 with pre-configured policies and the broadest support for file formats and data types

PRODUCT FEATURES

- Check Point UserCheck
- Check Point MultiSpect
- Network-wide Protection Coverage
- Central Policy Management
- Rapid and Flexible Deployment



DLP Software Blade

Check Point MultiSpect™

Check Point's innovative MultiSpect data classification engine combines users, content and process into accurate decisions. Check Point DLP delivers exceptionally high accuracy in identifying sensitive data including personally identifiable information (PII), compliance-related data (HIPAA, SOX, PCI data, etc.), and confidential business data. This is achieved through the MultiSpect technology, a strong 3-tier inspection engine:

- 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, HTTPS, and TLS as well as webmail and Microsoft Exchange
- Pattern matching and file classification for identifying content types regardless of the extension applied to the file or compression method used
- Recognize and protect sensitive forms—file/form matching (based on predefined templates)
- Identify unconventional business communication behavior—Out-of-the-box best practice policies

In addition, an open scripting language is available for creating custom data types. This unique flexibility provides virtually unlimited support for protecting sensitive data.

Network-wide Protection Coverage

Check Point's DLP solution is based on an in-line network-based Software Blade which runs on any existing Check Point gateway. The Check Point DLP Software Blade is an advanced data loss prevention solution for data transmitted over networks with wide coverage of traffic transport types (SMTP, HTTP, HTTPS, TLS, FTP) with deep application awareness protecting data in-motion. DLP policies are created to define what to prevent and how to prevent, per policy, per network segment, per gateway and per user-group.

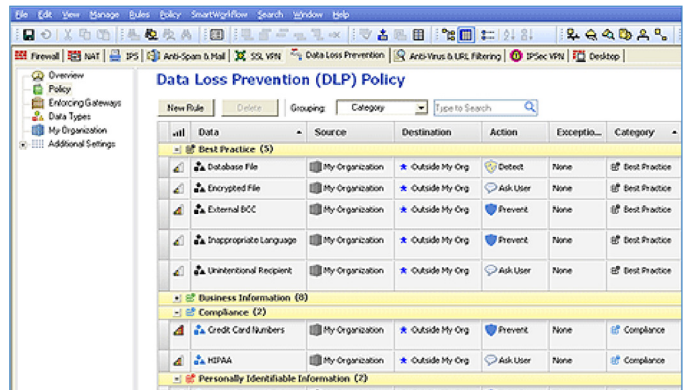
Central Policy Management

The DLP blade is managed centrally with Check Point Security Management™ through 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. Unified access policies are enforced automatically throughout the distributed environment, empowering them to securely provision access from anywhere.

Unified policy deployment across multiple gateways controls enforcement actions per policy; i.e. Detect (log only), or Quarantine (self-incident handling). Policy management includes the following features and options:

- Selection of data type(s) and user group(s)—also using Active Directory
- Enable exceptions—allowed users
- Traffic direction—enforce on outbound or inter-departmental traffic

- Pre-defined policies and content data types
- Incremental exposure of specific policies per different user groups
- Integrated Logging and Event correlation
- Customization of internal quarantine
- Granular protection control—easy-to-use protection profiles allow administrators to define signature and protection activation rules that match the security needs of your network assets
- Predefined default and recommended profiles—provide immediate and easy use out-of-the-box with profiles tuned to optimize security or performance



Easily create dedicated DLP rules to prevent data loss.

Event Management

Separating the needle from the haystack, SmartEvent for DLP allows you to monitor and report only what is important. Event management includes the following features and options:

- Real-time and history graphing and reporting of DLP events
- Easy incident correlation
- Graphical incident timeline
- Easily configured custom views
- Event / incident management workflow

For more details, see SmartEvent Software Blade.



Rapid and Flexible Deployment

Organizations of any size can be protected from day one with pre-configured templates. A wide range of built-in policies and rules are included for common requirements, including regulatory compliance, intellectual property, and acceptable use.

The Check Point DLP Software Blade can be installed on any Check Point Security Gateway (based on Check Point appliances or open server platforms). Deploy easily and rapidly on existing Check Point Security Gateways saving time and reducing costs by leveraging existing security infrastructure. In addition, a full range of powerful and highly scalable DLP-1 appliances are available to align with any network security requirements.



APPLIANCE TECHNICAL SPECIFICATIONS

		
	DLP-1 2571	DLP-1 9571
Performance		
Number of Users	1000	5000
Messages / Hour	70,000	350,000
Throughput	700 Mbps	2.5 Gbps
Interfaces		
Built-in Interfaces	6 Copper 1 GbE	10 Copper 1 GbE
Optional Interfaces	Built-in 4-Port, Copper, Bypass Card	LOM, 2x4 1 GbE Fiber, 2 x 4 1 GbE Copper, 2 x 2 10 GbE Modular 4-Port, Copper, Bypass Card
Storage		
Storage Size	500GB	2 x 2 TB (Mirrored – RAID 1)
Physical Specifications		
Enclosure	1U	2U
Dimensions (standard)	17.4 x 15 x 1.73 in.	17 x 20 x 3.46 in.
Dimensions (metric)	443 x 381 x 44mm	431 x 509.5 x 88mm
Weight	6.5kg (14.3 lbs)	16.5 kg (36.3 lbs)
Power		
Dual, Hot-Swappable Power Supplies	No	Yes
Power Input	100 ~ 240V; 50 ~ 60Hz	
Power Supply Spec (Max)	250W	400W
Power Consumption (Max)	77.5W	200.7W
Operating Environment Range	Temperature: 5° to 40° C, Humidity: 10%-85% non-condensing, Altitude: 2,500m	
Compliance	UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; CNS 13438 Class A (test passed; country approval pending); KN22KN61000-4 Series, TTA; IC-950; ROHS	

SOFTWARE TECHNICAL SPECIFICATIONS

DLP Software Blade is a software solution based on the Software Blade architecture. For deployment on open servers, it is tested for compatibility with a wide variety of currently shipping and pre-release hardware platforms. Please see the Hardware Compatibility List.

	Minimum Hardware Requirements for Installing DLP Software Blade	
Open Server Recommended Requirements	< 1000 users	< 5000 users
CPU Cores	2	8
RAM Size	4GB	4GB
Storage Size	250G	500G
NICs	2	2



TECHNICAL SPECIFICATIONS

Inspection	
Inspection Options	<ul style="list-style-type: none"> Over 500 pre-defined data content types Pattern, keyword matching, and dictionaries Multi-parameter data classification and correlation Advanced inspection based on structured content Similarity to commonly-used templates File attribute-based matching Use open scripting language to tailor and create specific data-types
File Types	Inspection of content for more than 600 file types
Protocols	HTTP, HTTPS, TLS, SMTP, FTP
Supported Regulations	PCI-DSS, HIPAA, PII and more
Non-regulated Data Types	<ul style="list-style-type: none"> Intellectual property data Financial and legal terms National ID numbers International Bank Account Numbers (IBAN)
Multi-language Support	Detection of content in multiple languages including single and double-byte fonts (UTF-8)
Enforcement	
Types	<ul style="list-style-type: none"> Ask User (self prevent with UserCheck)—places message in quarantine, send notification to end user, request self-remediation Prevent—block message from being sent and notify the end-user Detect—log incidents
UserCheck	<ul style="list-style-type: none"> Enabled and customized per policy with individual editable notification to end-user (multi-language) Self learning—prevents recurring incident management within same mail thread Two notification methods—email reply (no need for agent installation), or system tray pop-up (requires thin agent installation)
Enforcement Features	<ul style="list-style-type: none"> Policy exceptions per user, user group, network, protocol, or data type Send notification of potential breaches to owner of data asset (e.g. CFO for financial documents) Log all incidents—with option to correlate events and audit incidents
View Incident	<ul style="list-style-type: none"> Granular administrator permissions provide control over who can see DLP data Sensitive data in DLP event logs can be masked (e.g. only the last four digits of credit card numbers are shown) An audit log is created each time a captured message is viewed
Log All Emails	All outgoing Emails (including non-incidents) are logged for sender, recipients and subject
Policy Management	
Central Management	<ul style="list-style-type: none"> Integrated with SmartCenter Dashboard Simple and intuitive policy creation Easy data content type creation Powerful data content type categorization and search options
Event Management	<ul style="list-style-type: none"> Additional integrated functionality within SmartEvent Log reporting and real-time timeline monitoring Pie-chart with violation distributions per user or per network
Deployment	
Installation Options	<ul style="list-style-type: none"> Software Blade running on all Check Point security gateways Dedicated appliance
Network Deployment Options	<ul style="list-style-type: none"> Inline connectivity Connect to layer 2 mirrored port/ SPAN port
Installation Wizard	Simple wizard that assists in first stage operation of the DLP blade including connectivity to Active Directory and different initial required configurations

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com