CHECK POINT DATA LOSS PREVENTION SOFTWARE BLADE

CHECK POINT DLP SOFTWARE BLADE

Check Point Data Loss Prevention (DLP) Software Blade™ combines technology and processes to revolutionize DLP, helping businesses to pre-emptively protect sensitive information from unintentional loss, educating users on proper data handling policies and empowering them 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 deliver 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.

INSIGHTS

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

September 2015

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:

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

Fingerprint Sensitive Files

DLP scans file repositories of sensitive files and match when a file from this repository (or part of it) leaves the organization. With files matching, sensitive files are prevented from leaving the organization.

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.

COMPLETE DATA SECURITY SOLUTION

The DLP Software Blade is part of a complete data security solution to secure data at rest, data in use and data in transit. Most corporate laptops and PCs store proprietary data on their hard drives, and many users regularly work outside of a secure corporate environment. A data breach from a lost, stolen or compromised laptop can result in costly fines, lawsuits and lost revenue. Our Endpoint Full Disk Encryption secures the entire hard drive. Endpoint Media Encryption and Port Control secure removable media. Capsule Docs enables organizations to seamlessly protect documents, ensuring access for authorized users only. Remote Access VPN provides secure access to corporate resources when traveling or working remotely. Finally, ensure your data security policy meets regulatory requirements with our Compliance Software Blade.

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.

- ✓ 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

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

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.

TECHNICAL SPECIFICATIONS

Inspection	
Inspection Options	✓ Over 600 pre-defined data content types ✓ Pattern, keyword matching, and dictionaries ✓ Multi-parameter data classification and correleation ✓ 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 800 file types
Protocols	HTTP, HTTPS, TLS, SMTP, FTP
Supported Regulations	PCI-DSS, HIPAA, PII and more
Non-regulated Data Types	✓ 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)
File repository scans	Scan data in shared directories
Dormument watermarks	Add visible or invisible watermarks to business documents
Enforcement	
Types	✓ 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 events.
UserCheck™	✓ Enabled and customized per policy with individual editable notification to end-user (multi-language) ✓ Self learning – prevents recurring incident management within same mail threat ✓ Two notification methods – email reply (no need for agent installation), or system tray pop-up (requires thin agent installation)
Enforcement Features	✓ 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	✓ 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	✓	Integrated with SmartCenter Dashboard
	✓	Simple and intuitive policy creation
	✓	Easy data content type creation
	✓	Powerful data content type categorization and search options
Event Management	✓	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	✓	Software blade running on all Check Point security gateways
	✓	Dedicated appliance
Network Deployment Options	✓	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 US
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 | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com