



PRODUKTBESCHREIBUNG

Check Points DLP Software Blade ist eine einzigartige Lösung für Informationssicherheit, die nicht nur technologisch innovativ ist, sondern es auch ermöglicht, alle Prozesse im Unternehmen umfassend abzubilden. Mit dieser Lösung können Unternehmen nicht nur erkennen, dass Sicherheitsprobleme existieren, sondern auch vorbeugend/präventiv handeln. Check Points DLP Software Blade sorgt dafür, dass keine Daten unbeabsichtigt verloren gehen und Unternehmen ihre Daten aktiv schützen können.

DLP Software Blade

DIE HERAUSFORDERUNG

Ungewollter Datenverlust und der Missbrauch sensibler Informationen haben für die betroffenen Unternehmen meist gravierende Folgen und lassen daher keine Wahl: Moderne, IT-basierte Organisationen müssen adäquate Schutzmaßnahmen für ihre sensiblen Datenbestände treffen, also vor allem vertrauliche Mitarbeiter- und Kundendaten, rechtliche Dokumente und geistiges Eigentum vor unbefugter Nutzung schützen. Dieses Problem effektiv zu adressieren, ohne jedoch die Produktivität der Mitarbeiter zu bremsen oder die IT-Abteilung mit zusätzlichen Aufgaben zu überfrachten, stellt die Unternehmen vor eine besondere Herausforderung. Denn moderne Technologien haben sich weit entwickelt, doch schlussendlich sind sie nach wie vor nicht in der Lage, die Intentionen ihrer Benutzer zu verstehen. So hat bis heute der Versuch, sensible Daten durch die langwierige Entwicklung traditioneller DLP-Lösungen zu schützen zu wollen, nur geringe Erfolgsaussichten, sondern geht vielmehr mit aufwändiger Implementierung, mühsamer Administration und hohen Kosten einher.

ÜBERBLICK

Mit einer innovativen Kombination aus Technologie und Prozessen läutet Check Point jetzt eine neue DLP-Ära ein und bringt die Unternehmen aus der passiven Situation der Gefahrenerkennung heraus – hin zur aktiven Vermeidung von Datenverlust. Hierfür verbindet MultiSpect™, eine innovative Lösung für die Klassifizierung von Daten, Informationen zu Anwendern, Inhalten und Prozessen und trifft auf Basis dieser Kombination akkurate Entscheidungen über die Datennutzung. Darüber hinaus befähigt die neue UserCheck™-Technologie die Anwender, eventuelle Regelverletzungen in Echtzeit zu beheben. Check Points autodidaktische, netzwerkbasierte DLP-Lösung befreit IT- und Security-Verantwortliche von der Abwicklung von Störfällen und schult die Anwender im korrekten Umgang mit Daten-Policies – so werden sensitive Unternehmensdaten sowohl vor absichtlichem als auch im Besonderen vor versehentlichem Verlust geschützt.

CHECK POINT USERCHECK™

Check Point UserCheck befähigt den Anwender zur sofortigen Behebung von Fehlern und Störungen. Diese innovative Technologie informiert den Anwender über verdächtige Regelverletzungen und erlaubt sowohl eine sofortige Korrektur, als auch die schnelle Autorisierung legitimer Kommunikation. UserCheck ermöglicht dem Benutzer bei der Behandlung von Regelverletzungen eine Selbstregulierung. Optionen für das Senden, Verwerfen oder Überprüfen eines Problems erhöhen die Aufmerksamkeit im Umgang mit den Regeln für die Datennutzung und führen zu einer generellen Verbesserung der Datensicherheit. Die Meldung der Vorfälle in Echtzeit basiert entweder auf einem Pop-up aus einem Thin-Agent oder findet über das Versenden einer dedizierten Email an den Benutzer statt (Installation eines Agenten nicht erforderlich). Die Unternehmen profitieren hiervon auf mehrfache Weise:

- Vollständige Prävention – ermöglicht einen praktikablen Weg von reiner Problemerkennung hin zu aktiver Problemverhinderung
- Autodidaktisches System – erfordert kein IT-/Security-Personal für die Behandlung von Störmeldungen und schult gleichzeitig die Anwender im geeigneten Umgang mit den Datensicherheitsregeln des Unternehmens



UserCheck ermöglicht dem Anwender die sofortige Korrektur von Regelverletzungen

DIE WICHTIGSTEN VORTEILE

- **Verhindert den Verlust geschäftskritischer Informationen**
Die neue UserCheck-Technologie erlaubt den Anwendern die sofortige Korrektur eventueller Regelverstöße
- **Kombiniert Technologie und Prozesse zu funktionierendem DLP**
Die innovative Datenklassifizierungs-Engine MultiSpect bietet unvergleichliche Präzision, indem sie Informationen zu Anwendern, Inhalten und Prozessen verbindet.
- **Einfacher Einsatz für sofortigen Schutz vor Datenverlust**
Vorkonfigurierte Policies und die umfassende Unterstützung verschiedenster Dateiformate und Datentypen sorgen für den Schutz von sensiblen Daten – vom ersten Tag an.

PRODUKT-FEATURES

- Check Point UserCheck
- Check Point MultiSpect
- Netzwerkweiter Schutz
- Zentrales Policy-Management
- Schneller und flexibler Einsatz



Check Point MultiSpect™

Check Point MultiSpect ist durch die Kombination von Benutzer-, Inhalts- und Prozessinformationen die optimale Engine zur automatisierten Datenklassifikation. So liefert Check Point DLP eine außerordentlich hohe Präzision bei der Identifizierung sensibler Daten, wie zum Beispiel Personenidentifikationsinformationen (PII), Compliance-relevante Daten (HIPAA, SOX, PCI Daten etc.) und vertrauliche Geschäftsdaten. Hierfür bietet die MultiSpect-Technologie ein äußerst leistungsfähiges, dreischichtiges Prüfsystem:

- Datenklassifikation und -korrelation anhand verschiedener Parameter, sowie die Prüfung und Durchsetzung verschiedener Protokolle – untersucht Datenströme und setzt die Policies in den meistgenutzten TCP-Protokollen wie SMTP, FTP, HTTP und Webmail durch; gleicht Muster ab und klassifiziert Dateien für die Identifikation von Inhaltstypen, und zwar unabhängig von anhängenden Erweiterungen oder Dateikompressionen.
- Erkennen und Schutz sensibler Formate – Datei-/Formatabgleich (auf Basis vordefinierter Templates/Dokumentvorlagen)
- Identifikation von unkonventionellem Geschäftskommunikationsverhalten – sofort nutzbare und vielfach bewährte „best practice“ Policies

Darüber hinaus steht für die Erstellung individueller Datentypen eine offene Skriptsprache zur Verfügung. Diese außergewöhnlich hohe Flexibilität bietet praktisch unbegrenzte Unterstützung für den Schutz sensibler Datenbestände.

Netzwerkübergreifender Schutz

Check Points DLP-Lösung baut auf einem neuen, netzwerkbasieren Software Blade auf, das als dedizierte Appliance und zukünftig auch auf jedem bestehenden Check Point-Gateway mit Software Blades eingesetzt werden kann. Das Check Point DLP Software Blade ist eine fortschrittliche Data Loss Prevention-Lösung für Daten, die über Netzwerke übertragen werden. Sie bietet eine breite Abdeckung für unterschiedliche Datentransporttypen wie SMTP, HTTP und FTP, einschließlich s.g. Deep Application Awareness für den Schutz von Datenströmen. Die erstellten DLP-Policies definieren pro Regel, pro Netzwerksegment, pro Gateway und pro Benutzergruppe was verhindert werden soll und wie dies geschehen soll.

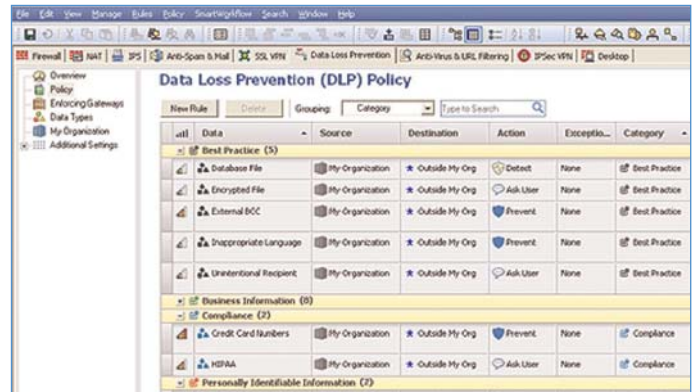
Zentrales Policy-Management

Das DLP Blade wird mit Check Point Security Management™ zentral und über ein benutzerfreundliches Interface verwaltet. Das zentralisierte Management ermöglicht eine besonders wirksame Nutzung und gute Kontrolle der Sicherheitsregeln. Zudem erlaubt es dem Anwenderunternehmen den Einsatz eines einzigen Repositories für Benutzer- und Gruppendefinitionen, Netzwerkobjekte, Zugriffsrechte und Sicherheitsregeln über die gesamte Sicherheitsinfrastruktur hinweg. Für die gesamte, verteilte Umgebung werden automatisch einheitliche Zugriffsregeln durchgesetzt, was von praktisch überall aus den sicheren Zugriff ermöglicht.

Die Nutzung einer einheitlichen Policy über verschiedene Gateways hinweg kontrolliert die Durchsetzungsaktionen pro Policy, wie zum Beispiel „erkennen“ (nur aufzeichnen) oder „Quarantäne“ (Selbstbehandlung bei Regelverstoß). Das Policy Management bietet folgende Features und Optionen:

- Festlegen von Datentyp(en) und Benutzergruppe(n) – auch unter Nutzung von Active Directory und LDAP
- Zulassen von Ausnahmen – zugelassene Benutzer
- Datenverkehrsweg – Durchsetzen von Outbound-Verkehr oder Datenverkehr zwischen Abteilungen
- Vordefinierte Policies und Datentypen für Inhalte
- Abgestufte Anwendung bestimmter Policies für unterschiedliche Benutzergruppen

- Integrierte Logging- und Event-Korrelation
- Anpassung von interner Quarantäne
- Granulare Schutzkontrolle – einfach zu nutzende Schutzprofile erlauben Administratoren die Definition von Aktivierungsregeln für Signaturen und Schutzmaßnahmen, die den Sicherheitsanforderungen der jeweiligen Netzwerkkumgebung entsprechen
- Vordefinierte Standardprofile und empfohlene Profile – vielfach bewährte, schnell und einfach zu nutzende Profile, die auf optimierte Sicherheit und Performance abzielen



Einfaches Erstellen dedizierter DLP-Regeln verhindert Datenverlust

Event Management

Um nicht die sprichwörtliche Nadel im Heuhaufen suchen zu müssen, ermöglicht SmartEvent für DLP dem Unternehmen genau das zu überwachen und festzuhalten, was tatsächlich wichtig ist. Das Event Management bietet folgende Funktionen und Optionen:

- Grafische Darstellung und Auswertung von DLP Events, historisch und in Echtzeit
- Einfache Korrelation von Vorfällen
- Grafische Darstellung von Vorfällen auf einer Zeitachse
- Einfach konfigurierte, individuelle Ansichten
- Management-Workflow von Events/Vorfällen

Weitere Detailinformationen hierzu bietet das Check Point-Datenblatt zu SmartEvent Blade.

Schneller und flexibler Einsatz

Organisationen jeder Größe können vom ersten Tag an mit Hilfe vorkonfigurierter Templates geschützt werden. Die Lösung bietet eine breite Palette bereits hinterlegter Policies und Regeln, die z. B. den generellen Anforderungen an gesetzliche Auflagen, dem Schutz geistigen Eigentums und einer akzeptable Nutzbarkeit entsprechen.

Das Check Point DLP Software Blade kann als dedizierte Appliance und zukünftig auch auf jedem Check Point Security Gateway (basierend auf Check Point-Appliances oder Open Server-Plattformen) installiert werden. Der sehr einfache und schnelle Einsatz innerhalb bestehender Check Point-Installationen führt unter Nutzung der existierenden Security-Infrastruktur zu einer erheblichen Zeit- und Kostenersparnis. Neben dem DLP Software Blade steht somit eine umfassende Palette leistungsstarker und hoch skalierbarer DLP-1 Appliances zur Verfügung, die für jede Art von Anforderung an die Netzwerksicherheit eine Lösung bieten.



SPEZIFIKATIONEN

APPLIANCE –
TECHNISCHE SPEZIFIKATIONEN

Performance	DLP-1 2571	DLP-1 9571
Anzahl Benutzer	1.000	5.000
Messages/Stunde	70.000	350.000
Durchsatz	700 Mbps	2,5 Gbps
Schnittstellen		
Integrierte Schnittstellen	6 Kupfer 1 GbE	10 Kupfer 1 GbE
Optionale Schnittstellen	Built-in 4-Port, Kupfer, Bypass Card	LOM, 2x4 1 GbE Fiber, 2x4 1 GbE Kupfer, 2x2 10 GbE Modular 4-Port, Kupfer, Bypass Card
Speicher		
Speichergröße	500 GB	2x2 TB (Gespiegelt – RAID 1)
Physikalische Spezifikationen		
Größe	1U	2U
Maße (Standard)	17,4 x 15 x 1,73 in.	17 x 20 x 3,46 in.
Maße (metrisch)	443 x 381 x 44 mm	431 x 509,5 x 88 mm
Gewicht	6,5 kg (14,3 lbs)	16,5 kg (36,3 lbs)
Leistung		
Redundante Netzteile (Hot-Swappable)	Nein	Ja
Eingangsleistung	100~240V; 50 ~ 60 Hz	
Maximale Spannungsversorgung	250W	400W
Maximaler Stromverbrauch	77,5W	200,7W
Betriebsumgebung/Einsatzbereich	Temperatur: 5° bis 40° C; Luftfeuchtigkeit: 10% - 85%, nichtkondensierend, Höhe: 2.500 m	
Compliance	UL 60950; FFC Part 15, Subpart B, Klasse A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; CNS 13438 Klasse A (Test durchlaufen; Landes-/ Länderfreigabe ausstehend); KN22KN61000-4 Serie, TTA; IC-950; ROHS	

SOFTWARE – TECHNISCHE SPEZIFIKATIONEN

Das DLP Software Blade ist eine Softwarelösung, die auf der Software Blade-Architektur basiert. Für den Einsatz auf Open Servern ist die Kompatibilität mit einer breiten Palette derzeit verfügbarer und in Kürze zu Verfügung stehender Hardwareplattformen getestet. Weitere Informationen hierzu finden Sie in der Hardware-Kompatibilitätsliste.

Minimale Hardwarevoraussetzungen für die Installation des DLP Software Blade

Empfohlene Systemvoraussetzungen für Open Server	< 1.000	< 5.000
CPU Kerne	2	8
RAM Größe	4 GB	4 GB
Speichergröße	250 G	500 G
NICs	2 / 3 bei L2-Inlinebetrieb	



TECHNISCHE SPEZIFIKATIONEN

Überprüfung der Daten und Inhalte	
Prüfoptionen	<ul style="list-style-type: none"> • Mehr als 250 vordefinierte Datentypen • Abgleich von Mustern, Schlüsselwörtern und Verzeichnissen • Datenklassifizierung und Korrelation anhand verschiedener Parameter • Fortschrittliche, auf strukturiertem Inhalt basierte Inspektion • Ähnlichkeit mit allgemein genutzten Templates • Attribut-basierter Dateiabgleich • Offene Skriptsprache für die Anpassung und Erstellung spezifischer Datentypen
Dateitypen	Inhaltliche Prüfung von mehr als 600 Dateitypen
Protokolle	HTTP, SMTP, FTP
Unterstützte Regularien	PCI-DSS, HIPAA, PII u.a.
Nicht regulierte Datentypen	<ul style="list-style-type: none"> • Geistiges Eigentum, Schutz- und Urheberrechte • Finanzielle und rechtliche Bestimmungen • Nationale ID-Nummern • Internationale Bankkontonummern (IBAN)
Unterstützung verschiedener Sprachen	Erkennung von Inhalten in verschiedenen Sprachen, einschließlich Single Byte- und Double-Zeichensätze (UTF-8)
Umsetzung der Richtlinien	
Typen	<ul style="list-style-type: none"> • Ask User (autodidaktische Prävention mit UserCheck) – stellt Nachrichten in Quarantäne, schickt Benachrichtigung an den Endanwender, fordert zur selbstständigen Fehlerbeseitigung auf • Prevent – blockiert das Senden von Nachrichten und informiert den Endbenutzer • Detect – protokolliert Störfälle
UserCheck	<ul style="list-style-type: none"> • Kundenspezifisch und pro Policy aktiviert, mit individuell editierbarer Benachrichtigung an den Endanwender (mehrsprachig) • Autodidaktisch – verhindert wiederholte Beschäftigung mit der gleichen Fehlermeldung • Zwei Benachrichtigungsmethoden – Email- bzw. Browser-Nachricht (Installation eines Agenten nicht erforderlich) oder System-Tray Pop-up (erfordert Thin Agent-Installation)
Funktionen für die Regeldurchsetzung	<ul style="list-style-type: none"> • Regelausnahmen pro Anwender, Benutzergruppe, Netzwerk, Protokoll oder Datentyp • Senden von Benachrichtigungen über potentielle Regelverletzungen an Verantwortliche für die jeweiligen Datenbestände (z. B. an CFO für Finanzdokumente) • Dokumentation aller Vorfälle – mit optionaler Eventkorrelation und Störfallrevision
Überprüfung von Vorfällen	Ein Administrator mit DLP-Befugnis (ein dediziertes Passwort) kann die tatsächlich gesendete Nachricht einschließlich Dateianhängen einsehen. Jede Überprüfung einer Nachricht wird protokolliert.
Dokumentation aller Emails	Zu allen gesendeten Emails (einschließlich störungsfreier Nachrichten) werden der Sender, Empfänger und der Betreff festgehalten.
Policy Management	
Zentrales Management	<ul style="list-style-type: none"> • Integriert mit SmartCenter Dashboard • Einfache und intuitive Policy-Erstellung • Einfache Datentypenstellung • Leistungsstarke Datentypkategorisierungs- und Suchoptionen
Event Management	<ul style="list-style-type: none"> • Zusätzliche, integrierte Funktionalität innerhalb von SmartEvent • Log-Reporting und Echtzeitüberwachung von Zeitvorgaben • Tortendiagramm zur Verteilung und Häufigkeit von Regelverletzungen pro Anwender oder pro Netzwerk
Einsatz	
Installationsoptionen	<ul style="list-style-type: none"> • Software Blade, lauffähig auf allen Check Point Security Gateways • Dedizierte Appliance
Einsatzoptionen im Netzwerk	<ul style="list-style-type: none"> • Inline Connectivity • Verbindung mit auf Layer 2 gespiegelten Port/SPAN Port
Installationsassistent	Einfaches Wizard, das die ersten Schritte der Inbetriebnahme des DLP Blade unterstützt, einschließlich der Connectivity zum Active Directory/ LDAP sowie verschiedene, zu Beginn erforderliche Konfigurationen

KONTAKT CHECK POINT

Central Europe: Fraunhofer Straße 7, 85737 Ismaning, Deutschland | Tel: 49-89-999-819-0 | Tel: 49-89-999-819-499 | Email: info@checkpoint.com
 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

www.checkpoint.com/contactus • Tel. Deutschland: 49-89-999819-0 • Tel. Österreich: 43-1-99460-6701 • Tel. Schweiz: 41-44-316-64-44

