



POPIS PRODUKTU

Check Point DLP Software Blade™ je jediným řešením DLP (Data Loss Prevention), které kombinuje technologii a procesy tak, že výsledkem je skutečně účinná prevence úniku dat. Organizace mohou nejen detekovat ztrátu dat, ale proaktivně chránit citlivé informace před neúmyslnými ztrátami.

DLP Software Blade

VÁŠ PROBLÉM

Vzhledem k množství se případům ztráty dat dnes organizace nemají na výběr: musí podnikat opatření k tomu, aby svá citlivá data chránily. Dochází totiž k únikům důvěrných dat o zaměstnancích a klientech, různých právních dokumentů a také duševního vlastnictví. Organizace musí tento problém vyřešit tak, aby se nenarušila produktivita zaměstnanců a současně aby nebyly kladeny neúměrné nároky na pracovníky IT. Technologie se v tomto oboru vyvíjí, avšak její častou slabou stránkou bývá, že nedokáže zohlednit skutečné záměry uživatelů. Ještě obtížnější jsou snahy chránit citlivá data bez dlouhých implementací, náročné administrace a vysokých nákladů spojených s tradičními produkty DLP.

PŘEHLED

Check Point přináší do řešení prevence ztráty dat (DLP) revoluční přístup: kombinuje technologii a procesy tak, že podniky mohou přejít od pasivní detekce k aktivní prevenci ztráty dat. Inovativní technologie pro klasifikaci dat MultiSpect™ spojuje informace o uživateli, obsahu a procesech, takže lze přijímat přesná, správná rozhodnutí. Díky technologii UserCheck™ zase mohou uživatelé v reálném čase provádět nápravu incidentů. Řešení DLP od Check Point osvobozuje pracovníky IT a síťové bezpečnosti od nutnosti řešit jednotlivé incidenty a uživatele vede k používání správných metod a pravidel práce s daty. Výsledkem je účinná ochrana citlivých podnikových informací před úmyslnými i neúmyslnými úniky.

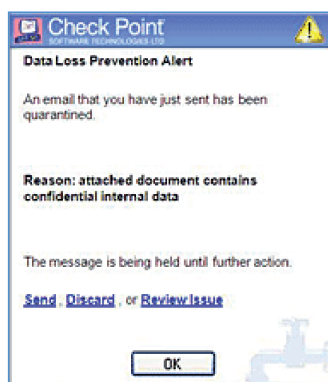
Technologie Check Point UserCheck™

Check Point UserCheck™ uživatelům umožňuje provádět nápravu incidentů v reálném čase. Tato inovativní technologie upozorňuje uživatele na podezřelou situaci, kdy mohou provést okamžitou nápravu a mohou také rychle autorizovat legitimní komunikace.

S technologií UserCheck mají uživatelé možnost sami zpracovávat jednotlivé incidenty, přičemž mají k dispozici volbu potvrdit odeslání zadržené komunikace, zrušit ji nebo zrevidovat. Dochází tak k celkovému zlepšení bezpečnosti, protože se zvyšuje povědomí uživatelů o politikách (pravidlech) použití dat. Oznámení o incidentu dostává uživatel buď formou vyskakovacího okna z tenkého agenta, nebo prostřednictvím dedikovaného e-mailu poslaného koncovému uživateli (pak není potřeba instalovat agenty).

Organizace získávají přínosy v několika směrech:

- Plošná prevence – umožňuje praktický přesun od detekce k prevenci.
- Samovzdělávací systém – nevyžaduje přímou účast pracovníků IT/bezpečnosti na zpracování incidentů a současně vzdělává uživatele ohledně správných pravidel sdílení dat.



Technologie UserCheck™ umožňuje uživatelům provádět nápravu incidentů v reálném čase.

KLÍČOVÉ PŘÍNOSY

- **Prevence úniku kritických obchodních informací**
Nová technologie UserCheck umožňuje uživatelům řešit DLP incidenty v reálném čase.
- **Kombinace technologie a procesů tak, že DLP účinně funguje**
Inovativní MultiSpect engine pro klasifikaci dat kombinuje informace o uživateli a obsahu a poskytuje tak bezkonkurenční přesnost detekce DLP incidentů.
- **Snadná implementace umožňuje okamžitou prevenci ztráty dat**
Ochrana citlivých dat může začít okamžitě po instalaci produktu díky předkonfigurovaným politikám a široké podpoře pro souborové formáty a datové typy.

VLASTNOSTI A FUNKCE PRODUKTU

- Technologie Check Point UserCheck
- Technologie Check Point MultiSpect
- Zajištění ochrany v kontextu celé sítě
- Centrální správa politik
- Rychlá a flexibilní implementace



Technologie Check Point MultiSpect™

Inovativní engine pro klasifikaci dat MultiSpect kombinuje informace o uživateli, obsahu a procesech, výsledkem čehož je neporovnatelně přesnější detekce DLP incidentů. Řešení Check Point DLP se vyznačuje vysokou mírou přesnosti při identifikování citlivých dat, včetně osobních identifikačních informací (PII), dat týkajících se shody s legislativou (HIPAA, SOX, PCI atd.) a důvěrných obchodních dat. Toho je dosaženo právě díky technologii MultiSpect, silnému 3-úrovňovému inspekčnímu enginu s těmito charakteristikami:

- Multiparametrová klasifikace a korelace dat.
- Multiprotokolová inspekce a prosazování - provádí inspekci datových toků a prosazuje politiky v nejvíce používaných TCP protokolech, jako je SMTP, FTP, HTTP, HTTPS a TLS, a také webmailu a Microsoft Exchange.
- Porovnávání vzorů (pattern matching) a klasifikace souborů za účelem identifikace obsahu bez ohledu na přípony použité pro soubor nebo na použitou metodu komprese.
- Rozpoznání a ochrana citlivých formulářů - porovnání souborů/formulářů (na základě předdefinovaných šablon).
- Identifikace nezvyklého chování obchodních komunikací - použití předdefinovaných osvědčených politik (Best Practices).

Kromě toho je k dispozici otevřený skriptovací jazyk pro tvorbu specifických zákaznických datových typů. Tato jedinečná flexibilita poskytuje prakticky neomezenou podporu pro ochranu citlivých dat.

Ochrana pokrývající celou síť

DLP řešení Check Point je založeno na in-line softwarovém bladu, který funguje na jakékoliv stávající Check Point bráně. Check Point DLP Software Blade představuje pokročilé řešení prevence ztráty dat pro data přenášená v rámci sítě (data-in-motion) s širokým pokrytím typů přenosových protokolů a sofistikovaným rozpoznáváním aplikací (SMTP, HTTP, HTTPS, TLS, FTP). DLP politiky, které definují, co se má chránit a jak se to má chránit, jsou vytvářeny podle síťových segmentů, podle bezpečnostních bran a podle uživatelských skupin.

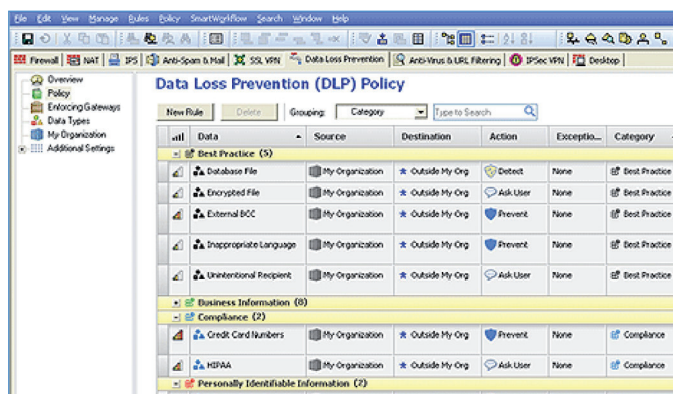
Centrální správa politik

Softwarový blade DLP se spravuje centrálně pomocí produktu Check Point Security Management™, který má uživatelsky příjemné rozhraní. Centralizovaná správa nabízí vynikající správu bezpečnostních politik, neboť umožňuje organizacím používat jedno úložiště pro definice uživatelů a skupin, síťových objektů, přístupových práv a bezpečnostních politik napříč celou bezpečnostní infrastrukturou. Unifikované přístupové politiky se aplikují automaticky v rámci distribuovaného prostředí, takže lze na jejich základě zajistit bezpečnost při přístupu odkudkoliv.

Jednotná správa politik v rámci všech bezpečnostních bran nabízí nastavení vynucovacích akcí na úrovni „detekce“ (pouze zápis do protokolu) nebo „karantény“ (samoobslužné zpracování incidentu). Správa politik zahrnuje tyto funkce a vlastnosti:

- Výběr datového typu (typů) a uživatelské skupiny (skupin) – také s využitím Active Directory.
- Definice výjimek – povolení pro vybrané uživatele.
- Směr provozu – prosazuje pravidla u odchozího nebo interního provozu.

- Předdefinované politiky a typy obsahu.
- Inkrementální uplatnění konkrétních politik u různých uživatelských skupin.
- Integrovaná korelace logů a událostí.
- Zákaznické přizpůsobení parametrů interní karantény.
- Granulární řízení ochrany – snadno použitelné profily ochrany umožňují administrátorům definovat pravidla signatur a aktivace ochrany, které odpovídají bezpečnostním potřebám konkrétní sítě a síťových zařízení.
- Předdefinované standardní a doporučené profily – umožňují okamžité a snadné použití profilů vyladěných pro optimalizaci bezpečnosti nebo výkonu.



Snadno lze vytvořit dedikovaná pravidla DLP pro prevenci úniku dat.

Správa událostí

SmartEvent pro DLP dokáže najít jehlu v kupce sena: umožní vám monitorovat a prezentovat pouze to, co je důležité. Správa událostí zahrnuje tyto funkce a vlastnosti:

- Tvorba grafů a výkazů o událostech DLP, v reálném čase i historicky.
- Snadná korelace incidentů.
- Grafické znázornění časového postupu událostí.
- Snadno konfigurovatelné zákaznické pohledy.
- Workflow správy událostí a incidentů.

Podrobnější údaje naleznete v informacích o produktu SmartEvent Software Blade.



Rychlá a flexibilní implementace

S využitím předkonfigurovaných šablon může být organizace libovolné velikosti chráněna okamžitě po nainstalování produktu. V produktu je zahrnuto široké spektrum vestavěných politik a pravidel, které odpovídají běžným požadavkům v oblasti datové ochrany, včetně např. shody s legislativními požadavky, ochrany duševního vlastnictví a přípustného použití dat.

Softwarový blade Check Point DLP lze nainstalovat na jakoukoliv bezpečnostní bránu Check Point (provozovanou na zařízení Check Point nebo otevřených serverových platformách). Snadná a rychlá implementace bladu DLP na existující bezpečnostní bráně Check Point šetří čas a redukuje náklady, neboť umožňuje využít stávající bezpečnostní infrastrukturu. Kromě toho je k dispozici několik typů dedikovaných výkonných zařízení DLP-1, která jsou vysoce škálovatelná a vyhoví jakýmkoliv síťovým bezpečnostním požadavkům.



TECHNICKÁ SPECIFIKACE ZAŘÍZENÍ

		
Výkon	DLP-1 2571	DLP-1 9571
Počet uživatelů	1 000	5 000
Počet zpráv/hodinu	70 000	350 000
Propustnost	700 Mb/s	2,5 Gb/s
Rozhraní		
Vestavěná rozhraní	6 x 1GbE metalické	10 x 1GbE metalické
Volitelná rozhraní	Vestavěná 4portová bypass karta metalická	LOM, 2 x 4 1GbE optická, 2x 4 1GbE metalická, 2x 2 10GbE modulární 4portová bypass karta metalická
Úložiště		
Velikost úložiště	500 GB	2 x 2 TB (zrcadlený – RAID 1)
Fyzické parametry		
Provedení – výška	1U	2U
Rozměry (palce)	17,4 x 15 x 1,73“	17 x 20 x 3,46“
Rozměry (mm)	443 x 381 x 44 mm	431 x 509,5 x 88 mm
Hmotnost	6,5 kg	16,5 kg
Napájení		
Duální napájecí zdroje vyměnitelné za chodu	Ne	Ano
Napájení	100 – 240 V, 50 – 60 Hz	
Příkon (max.)	250 W	400 W
Spotřeba el. energie (max.)	77,5 W	200,7 W
Provozní prostředí	Teplota: 5 – 40 °C, vlhkost vzduchu: 10 – 85 % nekondenzující, nadmořská výška: 2500 m	
Soulad s normami	UL 60950, FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; CNS 13438 Class A; KN22KN61000-4 Series, TTA; IC-950; ROHS	

TECHNICKÁ SPECIFIKACE PLATFORMY PRO SOFTWARE

DLP Software Blade je softwarové řešení založené na architektuře Software Blade. Pro účely implementace na otevřených serverech bylo řešení testováno na kompatibilitu se širokou škálou v současnosti dodávaných a ohlášených hardwarových platform. Bližší informace najdete v seznamu kompatibilních zařízení (Hardware Compatibility List).

	Minimální hardwarové požadavky pro instalaci DLP Software Blade	
Doporučené požadavky otevřeného serveru	do 1 000 uživatelů	do 5 000 uživatelů
Jádra CPU	2	8
Velikost RAM	4GB	4GB
Velikost úložiště	250G	500G
Počet síťových rozhraní	2	2



TECHNICAL SPECIFICATIONS

	Inspekce
Charakteristiky inspekce	<ul style="list-style-type: none"> • Přes 500 předdefinovaných typů datového obsahu. • Vzorce (pattern), klíčová slova a slovníkovy. • Multiparametrová klasifikace a korelace dat. • Pokročilá inspekce na bázi strukturovaného obsahu. • Detekce podobnosti s interně používanými šablonami. • Porovnávání na bázi souborových atributů. • Otevřený skriptovací jazyk pro přizpůsobení a tvorbu specifických datových typů.
Typy souborů	Inspekce obsahu pro více než 600 typů souborů
Protokoly	HTTP, HTTPS, TLS, SMTP, FTP
Podporované regulace	PCI-DSS, HIPAA, PII a další
Neregulované datové typy	<ul style="list-style-type: none"> • Data duševního vlastnictví. • Finanční a právní termíny. • Národní ID čísla. • Mezinárodní čísla bankovních účtů (IBAN).
Národní jazyková podpora	Detekce obsahu v mnoha jazycích, včetně jedno a dvoubajtových fontů (UTF-8)
	Prosazování politiky
Typy	<ul style="list-style-type: none"> • „Ask User“ (prevence pomocí UserCheck) – umísťuje zprávy do karantény, zasílá oznámení koncovému uživateli, vyžaduje nápravu uživatelem. • „Prevent“ – blokuje zprávy, aby nebyly odeslány, a zasílá oznámení koncovému uživateli. • „Detect“ – protokoluje incidenty.
UserCheck	<ul style="list-style-type: none"> • Aktivovaný a přizpůsobený podle politiky s individuálně editovatelným oznámením pro koncového uživatele (národní jazyková podpora). • Sebevzdělávání – zabraňuje opakující se správě incidentů v rámci stejného e-mailového vlákna. • Dvě metody oznamování – e-mailová odpověď (není potřeba instalovat agenta) nebo systémové vyskakovací okno (vyžaduje instalaci tenkého agenta).
Funkce prosazování	<ul style="list-style-type: none"> • Výjimky z politiky na uživatele, skupinu uživatelů, síť, protokol nebo datový typ. • Zasílání oznámení o potenciálních narušeních bezpečnosti vlastníkovi datových zdrojů (např. finanční ředitel u finančních dokumentů). • Protokolování všech incidentů – s možností korelovat události a auditovat incidenty.
Prohlížení incidentů	<ul style="list-style-type: none"> • Granulární administrátorská oprávnění poskytují kontrolu nad tím, kdo může data DLP prohlížet. • Senzitivní data v logu událostí DLP lze maskovat (např. se zobrazují pouze poslední čtyři číslice z čísel kreditních karet). • Při každém prohlížení zachycené zprávy se vygeneruje zápis do auditovacího protokolu.
Protokolování všech e-mailů	Všechny odcházející e-maily (včetně e-mailů neoznačených jako incidenty) se protokolují podle odesílatele, příjemce a předmětu.
	Správa politik
Centrální správa	<ul style="list-style-type: none"> • Integrovaná se SmartCenter Dashboard. • Jednoduchá intuitivní tvorba politik. • Snadná tvorba typu datového obsahu. • Výkonné funkce pro kategorizaci typů datového obsahu a vyhledávání.
Správa událostí	<ul style="list-style-type: none"> • Dodatečná integrovaná funkcionalita v rámci SmartEvent. • Vykazování protokolu a monitorování časového postupu událostí v reálném čase. • Koláčové grafy zohledňující porušení bezpečnosti podle uživatelů nebo podle sítě.
	Implementace
Možnosti instalace	<ul style="list-style-type: none"> • Softwarový blade (Software Blade DLP) nainstalovaný na libovolnou bezpečnostní bránu Check Point. • Dedikované zařízení.
Síťová implementace	<ul style="list-style-type: none"> • In-line konektivita. • Připojení k L2 zrcadlenému portu/SPAN portu.
Instalační průvodce	Jednoduchý průvodce, který pomáhá v prvním stadiu provozu DLP bladu včetně připojení na Active Directory a nastavení různých počátečních konfiguračních parametrů.

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

Czech Office

IBC Building, Pobrežní 3/620, 186 00 Praha 8, Tel.: +420 222 311 495, email: info_ee@checkpoint.com


 Arrow ECS, a.s. | Nagano Office and Technology Park, | Nagano III, U Nákladového nádraží 10, 130 00 Praha 3 | tel: +420 266 109 211 | www.arrowecs.cz
 Arrow ECS, a.s. | Tvorkovských 5, 709 00 Ostrava - Mariánské Hory | tel.: +420 597 488 811 | www.arrowecs.cz