



Check Point®  
SOFTWARE TECHNOLOGIES LTD.

# Check Point Software Blade Architecture



**3D**  
**SECURITY**

## DNEŠNÍ VÝZVY V OBLASTI BEZPEČNOSTI

Ochrana podnikové sítě v prostředí dnešních neustále se vyvíjejících hrozeb nebyla nikdy náročnější. Požadavky na infrastrukturu, konektivitu a výkon se neustále zvyšují. Nové, různorodé hrozby vedou k hledání nových dodavatelů bezpečnostních řešení a samostatných specializovaných produktů, které zvyšují složitost celkového systému bezpečnosti sítě. Současně je na IT oddělení vyvíjen tlak na snižování nákladů a komplexity a na lepší využití stávajícího hardwaru a zdrojů. Kombinace těchto požadavků často vede k zavádění neefektivních přístupů, které nefungují dobře, jsou nákladné a dlouhodobě neudržitelné.

V důsledku této situace hledají organizace a IT oddělení efektivnější řešení – takové, které by bylo jednoduché, flexibilní a které by zajistilo bezpečnost pro podnik jako celek. Součástí takového řešení by měla být i možnost přidávat bezpečnostní prvky podle potřeby, buď na úrovni sítě nebo v koncových zařízeních – aniž by bylo nutno řešit otázky výkonu, dostupnosti nebo náročných upgradů. Znamená to také schopnost investovat do bezpečnosti pouze v případě potřeby, bez nutnosti zavádět řešení dalších dodavatelů, instalovat na koncová zařízení agenty nebo pořizovat nová zařízení.

## STRATEGIE CHECK POINT 3D SECURITY

Strategie 3D Security společnosti Check Point přináší nové pojetí bezpečnosti: definuje ji jako třidimenzionální proces, který kombinuje bezpečnostní pravidla, uživatele (lidský faktor) a metody prosazování, přičemž výsledkem je silnější ochrana napříč všemi vrstvami bezpečnosti - včetně sítě, dat a koncových bodů. Chce-li organizace dosáhnout úrovně informační bezpečnosti potřebné pro 21. století, musí transformovat koncept bezpečnosti ze souhrnu samostatných bezpečnostních technologií v efektivní podnikový proces. Pomocí strategie 3D Security nyní mohou organizace vytvořit model bezpečnosti, který přesáhne pouhou technologii a zajistí integritu celé informační bezpečnosti.

Check Point 3D Security umožní organizacím předefinovat bezpečnost tak, že integruje tři dimenze bezpečnosti (pravidla, lidé, prosazování), jak jsou znázorněny na schématu dole, v jeden podnikový proces.

## ARCHITEKTURA CHECK POINT SOFTWARE BLADE

Klíčový nástroj pro realizaci strategie 3D Security představuje architektura Software Blade Architecture™ od společnosti Check Point, která umožňuje organizaci prosazovat stanovená bezpečnostní pravidla (politiky) a současně ohledně těchto pravidel školit uživatele. Architektura Software Blade je první a jedinou bezpečnostní architekturou, která poskytuje úplnou a flexibilní bezpečnost se snadnou správou, a to pro organizace libovolné velikosti.

Navic v případě, že se objeví nové hrozby a bezpečnostní potřeby, může architektura Check Point Software Blade rychle a flexibilně rozšířit bezpečnostní služby na vyžádání – aniž by se přidával nový hardware nebo zvyšovala složitost správy systému. Všechna řešení se spravují centrálně prostřednictvím jediné konzole, což redukuje složitost a operační režijní náklady. V dnešní době je vícevrstvá bezpečnost velmi důležitá, neboť jediné tak lze účinně bojovat s dynamickými hrozbami jako jsou škodlivé programy typu bot, trojské koně nebo pokročilé perzistentní hrozby (APT). Firewally dnes často působí jako multifunkční bezpečnostní brány, ale ne všechny organizace požadují stejný rozsah bezpečnosti. Pro organizace je důležité, aby byly při vytváření bezpečnostního systému flexibilní a aby měly nad svými bezpečnostními zdroji dokonalou kontrolu.

## CO JE TO SOFTWARE BLADE?

Software Blade je samostatná bezpečnostní aplikace či modul, například firewall, VPN (Virtual Private Network), IPS (Intrusion Prevention System) nebo Application Control, který je nezávislý, modulární a centrálně spravovaný. Organizace tak mohou skladbu bezpečnostních prvků přizpůsobit a vytvořit si takovou kombinaci, která bude vyhovovat potřebám jejich ochrany i finančním možnostem. Software Blade lze rychle aktivovat a konfigurovat na libovolné bráně nebo management systému pomocí jednoduchého kliknutí myši – nevyžaduje se žádný hardware, firmware nebo upgrade ovladačů. Když se bezpečnostní potřeby změní, lze snadno aktivovat další Software Blade a rozšířit bezpečnost na existující konfiguraci na stejném bezpečnostním hardwaru.

### Strategie Check Point 3D Security



**Policy**

**Bezpečnostní pravidla,**  
která podporují obchodní  
potřeby a promění bezpečnost  
v podnikový proces.



**People**

**Uživatelé**  
jsou zapojeni do definování  
pravidel, školení a nápravy  
bezpečnostních incidentů.



**Enforcement**

**Prosazování,**  
konsolidace a kontrola všech  
vrstev bezpečnosti - sítě,  
aplikací, obsahu a uživatelů.

Rozšiřujte své řešení bezpečnosti pomocí jediného kliknutí myši. Nové bezpečnostní moduly Software Blades můžete přidávat ve flexibilní, snadno použitelné management konzoli Check Point.

## KLÍČOVÉ PŘÍNOSY

### ■ Lepší bezpečnost

Řešení s více vrstvami ochrany a konsolidovaná platforma pro podnikovou bezpečnost představuje unikátní kombinaci integrované bezpečnosti sítě a koncových bodů spojenou s komplexní ochranou proti malwaru.

### ■ Jednoduchost

Snadná administrace, maximální flexibilita a jednoduchá aktivace bezpečnostních prvků eliminuje složitost systému bezpečnosti; jeho provoz a údržba je celkově jednodušší.

### ■ Snadný management

Aktivace jedním kliknutím myši umožňuje rychlou implementaci bezpečnostních služeb. Centralizovaný management modulů Software Blades zvyšuje produktivitu a efektivnost.

### ■ Kompletní bezpečnost

Rozsáhlá knihovna více než třiceti Software Blades poskytuje bezkonkurenční integrované bezpečnostní řešení, které umožňuje realizovat správnou úroveň bezpečnosti na všech vrstvách sítě.

### ■ Nižší TCO

Řešení poskytuje lepší bezpečnost, možnosti rozšiřování a konsolidace, což snižuje celkové náklady na vlastnictví (TCO) v porovnání s tradičními řešeními na bázi produktů od různých dodavatelů až o 50 %.

### ■ Maximalizace výkonu

Kompletní škála výkonových variant zařízení - od 190 Mb/s až po 1 Tb/s. Umožňuje poskytování zdrojů při garantované úrovni služeb.

### ■ Úspory prostoru a ekologičnost

Poskytuje "Green IT" úspory na základě možnosti konsolidace více samostatných řešení a zařízení do jedné integrované brány, což redukuje nároky na prostor ve stojanu (rack space), chlazení, kabeláž a spotřebu elektrické energie.

## JAK SE CHECK POINT SOFTWARE BLADES IMPLEMENTUJÍ?

Software Blades lze implementovat na specializovaných zařízeních (appliance) Check Point a na otevřených serverech. Nové Software Blades se pak na vaši stávající hardwarovou platformu přidávají jednoduše pomocí „zapnutí“ jejich funkčnosti na centrální, snadno ovladatelné management konzoli Check Point. Není potřeba žádný další hardware, firmware nebo ovladače. Organizace tedy mohou implementovat bezpečnost dynamicky – podle potřeby – a s podstatně nižšími náklady na implementaci.

The screenshot displays the SmartDashboard interface for the Firewall blade. At the top, there are two tabs: "Network Security (13)" and "Management (0)". The "Network Security" tab is active, showing a list of features with checkboxes. The "Firewall" blade is highlighted, and its configuration details are shown on the right. The "Firewall" section includes a description: "World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box." Below the description is an illustration of a multi-colored bar chart and a "More Info" link. The "Advanced Networking & Clustering" section includes "Dynamic Routing", "SecureXL", and "QoS". A "More Blades" link is also visible.

Network Security (13)	Management (0)
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Application Control
<input checked="" type="checkbox"/> IPSec VPN	<input checked="" type="checkbox"/> URL Filtering
<input type="checkbox"/> Policy Server	<input checked="" type="checkbox"/> Data Loss Prevention
<input type="checkbox"/> Mobile Access	Advanced Networking & Clustering:
<input checked="" type="checkbox"/> IPS	<input checked="" type="checkbox"/> Dynamic Routing
<input checked="" type="checkbox"/> Anti-Bot	<input checked="" type="checkbox"/> SecureXL
<input checked="" type="checkbox"/> Anti-Virus	<input checked="" type="checkbox"/> QoS
<input checked="" type="checkbox"/> Anti-Spam & Email Security	
<input checked="" type="checkbox"/> Identity Awareness	
<input checked="" type="checkbox"/> Monitoring	

### Check Point Security Gateway – panel SmartDashboard

*Firewall Software Blade je vždy součástí řešení.*

Prizpůsobte bezpečnostní řešení vašim specifickým obchodním podmínkám.

## ZVOLTE ŘEŠENÍ BEZPEČNOSTNÍ BRÁNY, KTERÉ BUDE RŮST S VAŠÍM PODNIKÁNÍM

Architektura Software Blade od Check Point vám poskytuje bezkonkurenční flexibilitu – ať navrhujete řešení pro centrálu společnosti nebo datové centrum, pro pobočky společnosti nebo pro podnik střední velikosti. Výsledkem bude vždy efektivně fungující brána nebo management systém konfigurované přesně podle specifických potřeb vašeho podniku.

### Tři volby při budování řešení bezpečnostní brány

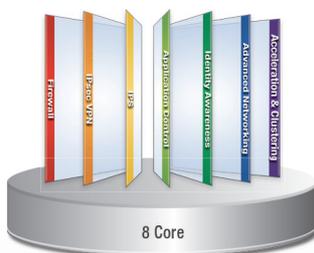
#### Volba 1

Balíky na bázi zařízení  
Check Point Appliance



#### Volba 2

Kontejnery  
a předdefinované systémy



#### Volba 3

Individuální sestava  
Software Blades - A la carte



## SIZING VAŠEHO SYSTÉMU

Jak určit, jak výkonné zařízení zvolit? Check Point zavedl novou benchmark metriku SecurityPower™, která zákazníkům umožní vybrat správné bezpečnostní zařízení (appliance) tak, aby bylo schopno zvládnout reálný síťový provoz, více pokročilých bezpečnostních Software Blades a typickou bezpečnostní politiku. Pomocí aplikace SecurityPower mohou zákazníci rychle určit, které zařízení bude nejlépe vyhovovat jejich současným síťovým bezpečnostním potřebám a které zároveň bude schopno podporovat předpokládaný budoucí nárůst provozu a další bezpečnostní Software Blades.

Určete, které Software Blades  
budete na bezpečnostní  
bráně provozovat

Zadejte rychlost sítě

Vyberte umístění  
bezpečnostní brány  
(perimetr nebo LAN)

A screenshot of the SecurityPower configuration interface. It shows a 'Define your Network Requirements' section with two main steps. Step 1, 'Choose Blade Combination', includes checkboxes for Firewall, Identity Awareness, VPN, IPS, Application Control, DLP, URL Filtering, and Anti Virus. Step 2, 'Define Performance Requirements', includes fields for Gateway Throughput (1700 Mbps) and Number of users (100). It also has radio buttons for Gateway Location: Perimeter / DMZ (selected), Internal, and Both. An 'Advanced settings' dropdown is visible at the bottom.

# Zjednodušte management bezpečnosti pomocí jednoho pohledu.

## PŘEDDEFINOVANÉ A INDIVIDUÁLNÍ (A LA CARTE) SOFTWARE BLADE SYSTÉMY A KONTEJNERY

Systémy a kontejnery Software Blade jsou dodávány se všemi službami nutnými pro provoz prostředí Software Blade Check Point a obsahují snadno použitelné administrátorské rozhraní. Existují tři druhy systémů a kontejnerů Software Blade:

### PRO BEZPEČNOSTNÍ BRÁNY

Systémy Software Blade pro bezpečnostní brány jsou k dispozici jako balíky včetně specializovaného zařízení (appliance package), jako předdefinované bezpečnostní balíky (predefined security bundle) bez vazby na zařízení nebo jako individuální výběr bezpečnostních funkcí podle vlastní volby (a la carte) a zahrnují:

- SecurePlatform™ - specializovaný operační systém pro rychlou a snadnou implementaci
- CoreXL™ - akceleraci na vícejádrových procesorech pro hloubkovou inspekci paketů a maximální výkon

#### Kroky při vytvoření integrované bezpečnostní brány na míru vašim potřebám

1. Vyberte kontejner na základě počtu jader CPU ve vašem zařízení (appliance)
2. Vyberte požadované Gateway Software Blades
3. Vytvořte systém, který je jednoduchý, flexibilní a bezpečný

### PRO BEZPEČNOST KONCOVÝCH BODŮ

Zvolte si ze šesti Endpoint Security Software Blade a vytvořte individuální řešení dle vašich potřeb:

- Zaveďte pouze ty prvky bezpečnosti koncových bodů, které v současnosti potřebujete.
- Kdykoliv v budoucnu můžete z centrální management konzole dodat další prvky.

#### Kroky při vytvoření integrovaného řešení bezpečnosti koncových bodů na míru vašim potřebám

1. Vyberte kontejner na základě počtu počítačů
2. Vyberte požadované Endpoint Software Blades
3. Centrálně nainstalujte Endpoint Software Blades

### PRO MANAGEMENT BEZPEČNOSTI

Kontejnery Software Blade pro management bezpečnosti jsou dodávány předdefinované a zahrnují:

- Vestavěnou službu aktualizace, která udržuje software v aktuálním stavu
- Integrované funkce pro zálohování, obnovu a přechod na vyšší verze.

#### Kroky při vytvoření integrovaného management řešení na míru vašim potřebám

1. Vyberte kontejner na základě počtu jader CPU ve vašem zařízení (appliance) nebo open serveru
2. Vyberte požadované Management Software Blades
3. Začněte provádět centrální management vašich bezpečnostních bran a koncových bodů

# Chraňte vaši síť před bezpečnostními hrozbami s využitím konceptu více bezpečnostních vrstev.

## SOFTWARE BLADES PRO BEZPEČNOSTNÍ BRÁNY



**Check Point Firewall Software Blade** staví na technologii s řadou ocenění, která se poprvé objevila jako součást řešení FireWall-1 společnosti Check Point a představuje nejsilnější úroveň bezpečnosti bran zohledňující identitu uživatelů (identity awareness) ve své třídě. Firewally společnosti Check Point, které využívá 100 % společností z prestižního seznamu Fortune 100 a celosvětově přes 170000 zákazníků, prokázaly od uvedení FireWall-1 na trh v roce 1994 svoji vedoucí pozici v odvětví a schopnost nepřetržitě inovace.



**Check Point IPsec VPN Software Blade** poskytuje bezpečnou konektivitu do podnikových sítí pro vzdálené a mobilní uživatele, podnikové pobočky a obchodní partnery. Tento Software Blade integruje funkce pro řízení přístupu, autentizaci a šifrování, a tak zajišťuje bezpečnost síťových připojení přes veřejný Internet.



**Check Point Mobile Access Software Blade** poskytuje jednoduchý bezpečný vzdálený přístup k podnikovým aplikacím přes Internet, prostřednictvím chytrých telefonů nebo PC. Řešení umožňuje vzdálený přístup kategorie enterprise přes SSL VPN pro jednoduché bezpečné mobilní připojení k e-mailu, kalendářům, kontaktům a podnikovým aplikacím.



**Check Point Intrusion Prevention System (IPS) Software Blade** kombinuje špičkové funkce pro ochranu proti průnikům (IPS) s vynikajícím výkonem za mnohem nižší cenu než tradiční samostatná IPS řešení. IPS Software Blade zajišťuje komplexní a proaktivní prevenci průniků - vše s výhodami v oblasti implementace a správy, které poskytuje unifikované a rozšiřitelné řešení firewall nové generace.



**Check Point Application Control Software Blade** poskytuje nejsilnější aplikační kontrolu a bezpečnost pro organizace všech velikostí. Umožňuje IT oddělením vytvářet granulární bezpečnostní politiky - na bázi uživatelů nebo skupin - s cílem identifikace, blokování nebo omezení užití více než 240.000 Web 2.0 aplikací a widgetů.



**Check Point Identity Awareness Software Blade** poskytuje detailní přehled o uživateli, skupinách a počítačích a umožňuje vynikající řízení přístupu prostřednictvím tvorby přesných bezpečnostních politik na bázi identit. Díky centralizovanému managementu a monitorování lze politiky spravovat z jedné unifikované konzole.



**Check Point DLP Software Blade** kombinuje technologii a procesy tak, že vytváří zcela nový koncept prevence ztráty dat (Data Loss Prevention, DLP), který podnikům pomáhá preventivně chránit citlivé informace před neúmyslnými úniky, vzdělává uživatele ohledně pravidel správného zacházení s daty a umožňuje jim provádět nápravu bezpečnostních incidentů v reálném čase.



**Check Point URL Filtering Software Blade** se integruje s modulem Application Control a umožňuje jednotné prosazování a management veškerých aspektů webové bezpečnosti. Filtrování na bázi URL poskytuje optimalizovanou webovou bezpečnost prostřednictvím plné integrace v rámci bezpečnostní brány s cílem zabraňovat jejím obcházení přes externí proxy; integrace prosazování politik s modulem Application Control přináší plnou Web a Web 2.0 ochranu; UserCheck zmocňuje a vzdělává uživatele v reálném čase ohledně bezpečnostních pravidel použití Webu.



**Check Point Anti-Bot Software Blade** detekuje počítače infikované škodlivými programy typu bot, zabráňuje škodám programy bot pomocí blokování komunikace botů s C&C (command-and-control servery) a je nepřetržitě aktualizován z ThreatCloud™, první celosvětové sítě pro boj s kyberzločinem.

## SOFTWARE BLADES PRO BEZPEČNOSTNÍ BRÁNY (pokračování)



**Check Point Antivirus Software Blade** obsahuje pokročilý antivir, který blokuje přichozí škodlivé soubory. Využívá real-time virové signatury a ochrany na bázi anomálií zasílané ze sítě ThreatCloud™, první celosvětové sítě pro boj s kyberločinem. Takto je Antivirus Software Blade schopen detekovat a blokovat malware již v bezpečnostní bráně, předtím, než by mohl být infikován počítač uživatele.



**Check Point Anti-Spam and Email Security Software Blade** poskytuje komplexní ochranu messagingové infrastruktury organizace. Multidimenzionální přístup chrání e-mailovou infrastrukturu, poskytuje vysoce přesnou ochranu proti spamu a brání organizaci před širokou škálou virových a malwarových hrozeb přicházejících v rámci elektronické pošty. Nepřetržité aktualizace zajišťují, že jsou veškeré hrozby zachyceny předtím, než se mohou rozšířit.



**Check Point Web Security Software Blade** poskytuje sadu pokročilých funkcí pro detekování a prevenci útoků namířených proti webové infrastruktuře. Web Security Software Blade zajišťuje komplexní ochranu v případě používání Webu pro obchodování a komunikace.



**Check Point Advanced Networking and Clustering Software Blade** zjednodušuje implementaci a management síťové bezpečnosti v rámci složitých a vysoce vytížených sítí; současně maximalizuje síťový výkon a bezpečnost v multi-Gbps prostředích. Tento blade je kombinací Check Point Acceleration and Clustering Software Blade a Advanced Networking Software Blade, a je ideální volbou pro prostředí největších podnikových sítí a datových center, kde jsou kritickými faktory výkon a dostupnost.



**Check Point Acceleration and Clustering Software Blade** poskytuje sadu pokročilých technologií SecureXL a ClusterXL, které ve své kombinaci maximalizují výkon a bezpečnost v prostředích vyžadujících velmi vysoký výkon. Pracují s technologií CoreXL, která je zahrnuta do blade kontejnerů, a vytvářejí základ tzv. Open Performance Architecture, která poskytuje průchodnost potřebnou pro datacentrové aplikace a nejvyšší úroveň bezpečnosti pro ochranu proti dnešním hrozbám na úrovni aplikací.



**Check Point Advanced Networking Software Blade** obsahuje řadu pokročilých síťových funkcí jako je dynamické směrování, podpora multicastingu, prioritizace QoS (Quality of Service), ISP redundance nebo vyrovnávání aplikační zátěže (application load balancing). Tyto funkce ve své kombinaci optimalizují výkon sítě a uživatelů, například tím, že kriticky důležitým aplikacím a uživatelům přiřazují vysokou prioritu. V důsledku toho se udržuje vysoká produktivita a spokojenost uživatelů při práci online.



**Security Gateway Virtual Edition** chrání dynamická virtualizovaná prostředí a externí sítě, jako jsou např. privátní nebo veřejné cloudy, před interními i externími hrozbami tím, že zabezpečuje virtuální počítače a aplikace. Tento Software Blade se spravuje z jednotného rozhraní, což poskytuje konzistentní a efektivní management.



**Voice Over IP** Bezpečnostní produkty Check Point umožňují implementovat aplikace VoIP, jako je IP telefonie nebo videokonference, aniž by tím vznikly nové bezpečnostní hrozby nebo bylo potřeba přepracovat design vaší sítě. Vzhledem k tomu, že červi a útoky DoS (odmítnutí služby) specifické pro VoIP dokážou zcela zablokovat telefonické služby na bázi IP, nabízí Check Point dynamické řešení, které je schopno rozpoznat a zablokovat známé i nové hrozby, jež by mohly narušit vaši obchodní kontinuitu.

## SOFTWARE BLADES PRO MANAGEMENT BEZPEČNOSTI



**Check Point Network Policy Management Software Blade** poskytuje komplexní centralizovaný management síťových bezpečnostních politik pro bezpečnostní brány Check Point a Software Blades, a to prostřednictvím SmartDashboard – jednotné konzole, která umožňuje řídit i ty nejsložitější instalace.



**Check Point Endpoint Policy Management Software Blade** zjednodušuje správu bezpečnosti koncových bodů tak, že sjednocuje veškeré funkce pro bezpečnost koncových bodů do jedné konzole. Stanovené bezpečnostní politiky lze monitorovat, spravovat a prosazovat z jednoho kontrolního panelu, až na úroveň uživatelů a jednotlivých počítačů, vše pomocí několika kliknutí myši.



**Check Point SmartEvent Software Blade** je jednotné řešení pro správu a analýzu bezpečnostních událostí, které poskytují v reálném čase informace potřebné pro účinnou správu hrozeb. Administrátoři jsou schopni rychle identifikovat kritické bezpečnostní události, zastavit hrozby přímo z obrazovky události, dodat za provozu potřebné ochranné prvky k potlačení útoku, a to vše z jedné konzole.



**Check Point Logging & Status Software Blade** provádí real-time monitorování bezpečnostního statusu a aktivit prostřednictvím sledování logů (protokolů) a dodává kompletní vizualizovaný obraz o změnách na bezpečnostních branách, tunelech a vzdálených uživateli.



**Check Point SmartWorkflow Software Blade** poskytuje hladký a automatizovaný proces pro správu změn bezpečnostních politik, který pomáhá administrátorům zredukovat počet chyb a zdokonalit shodu s definovanými procesy. Aplikace prosazuje v praxi formální proces pro editování, kontrolu, povolování a monitorování změn politik z jedné konzole; výsledkem je ucelená správa politik po celou dobu jejich životního cyklu.



**Check Point SmartProvisioning Software Blade** umožňuje centralizovanou administraci a poskytování zařízení Check Point. Za použití profilů mohou administrátoři automatizovat konfiguraci zařízení a snadno rozšiřovat změny v nastaveních na mnoho různých geograficky distribuovaných zařízení, a to prostřednictvím jedné bezpečnostní management konzole.



**Check Point Monitoring Software Blade** prezentuje kompletní obraz o výkonu sítě a bezpečnosti, což umožňuje rychle reagovat na změny v modelech provozu bezpečnostních událostí. Tento Software Blade centrálně monitoruje různá zařízení Check Point a upozorňuje na změny na bezpečnostních branách, koncových bodech, tunelech, vzdálených uživateli a bezpečnostních aktivitách.



**Check Point Management Portal Software Blade** umožňuje přístup k managementu bezpečnosti pomocí prohlížeče, což mohou využít externí pracovníci, např. pracovníci podpory nebo auditoři, a přitom se zachovává centralizovaná kontrola prosazování bezpečnostních politik. Lze prohlížet bezpečnostní politiky, stav všech produktů Check Point a aktivitu administrátorů, a také editovat, tvořit a modifikovat interní uživatele.



**Security Management and Multi-Domain Security Management (Provider-1™)** poskytuje další úroveň bezpečnosti a kontroly na základě segmentace managementu bezpečnosti do několika virtuálních domén. Podniky všech velikostí mohou snadno vytvořit virtuální domény na bázi geografického rozmístění, obchodních jednotek nebo bezpečnostních funkcí, a tak posílit bezpečnost a zjednodušit management.



**Check Point User Directory Software Blade** využívá LDAP servery k získání identifikačních a bezpečnostních informací o síťových uživateli, a tak eliminuje rizika související s manuálním udržováním a synchronizací redundantních datových úložišť a umožňuje centralizovanou správu uživatelů v rámci celého podniku.



**Check Point SmartReporter Software Blade** zvyšuje rozsah informací o bezpečnostních hrozbách na základě centralizace bezpečnostních výkazů o stavu sítě, bezpečnosti a aktivitách uživatelů do výstižných reportů, předdefinovaných nebo s možností přizpůsobení dle požadavků. Snadné generování reportů a jejich automatická distribuce šetří čas a peníze, a umožňuje tak organizaci maximalizovat bezpečnostní investice..

## SOFTWARE BLADES PRO BEZPEČNOST KONCOVÝCH BODŮ



**Check Point Firewall & Compliance Check Software Blade** chrání koncové body na základě kontroly příchozího a odchozího provozu a zajišťování shody s bezpečnostními politikami, pomocí centralizovaného managementu z jedné konzole. Definovatelné zóny a bezpečnostní úrovně chrání systémy koncových bodů před neautorizovaným přístupem. Integrovaná technologie pro utajení činí koncové body neviditelnými pro útočníky. Tento software blade lze snadno spravovat pomocí unifikovaného Endpoint Security Management.



**Check Point Full Disk Encryption Software Blade** poskytuje automatickou bezpečnost pro všechny informace na pevném disku koncových bodů včetně uživatelských dat, souborů operačního systému a dočasných nebo vymazaných souborů. Vícefaktorová pre-boot autentizace ověřuje identitu uživatelů a tím maximální ochranu dat, šifrování pak zabraňuje ztrátě dat při odcizení.



**Check Point Media Encryption Software Blade** umožňuje centrálně prosazovatelné šifrování výměnných paměťových médií typu USB flash disk, zálohovací pevné disky, CD nebo DVD, což dále posiluje ochranu dat. Kontrola portů umožňuje management všech portů koncových bodů plus centralizované logování aktivit portů pro účely auditování a shody s nařízením.



**Check Point Remote Access VPN Software Blade** poskytuje uživatelům bezpečný hladký přístup k podnikové síti a zdrojům při cestování nebo práci na dálku. Privátnost a integrita citlivých informací jsou zajištěny na základě vícefaktorové autentizace, skenování shody systému koncového bodu s nastavenými pravidly a šifrování všech přenášených dat.



**Check Point Anti-Malware & Program Control Software Blade** účinně detekuje a odstraňuje z koncových bodů malware pomocí jednoho skenu. Viry a další škodlivé programy typu spyware, keystroke loggers, trójské koně nebo rootkits se identifikují za použití signatur, blokování podezřelého chování a heuristické analýzy. Funkce pro kontrolu programů umožňují provozovat na koncových bodech pouze povolené programy. Tento software blade lze snadno spravovat pomocí unifikovaného Endpoint Security Management.



**Check Point WebCheck Endpoint Software Blade** chrání podnik proti rostoucímu počtu webových hrozeb. Známé a neznámé hrozby, jako jsou drive-by downloads, phishing stránky nebo zero-day útoky, jsou izolovány pomocí technologie virtualizace prohlížeče a současně pomocí pokročilé heuristiky zabraňuje uživatelům v přístupu na nebezpečné weby. Tento software blade lze snadno spravovat pomocí unifikovaného Endpoint Security Management.

Centrálně spravovaná komplexní bezpečnost koncových bodů, která je pro práci koncových uživatelů zcela transparentní.

# Kontaktujte Check Point a diskutujte o Check Point Software Blade Architecture:

[www.checkpoint.com/contactus](http://www.checkpoint.com/contactus)

**Telefonicky v USA: 1-800-429-4391 volba 5 nebo  
1-650-628-2000**



## CONTACT CHECK POINT

### Worldwide Headquarters

5 Ha'Soleim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)

### Czech Office

IBC Building, Pobřežní 3/620, 186 00 Praha 8, Tel.: +420 222 311 495, email: [info\\_ee@checkpoint.com](mailto: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](http://www.arrowecs.cz)  
Arrow ECS, a.s. | Tvorkovských 5, 709 00 Ostrava - Mariánské Hory | tel.: +420 597 488 811 | [www.arrowecs.cz](http://www.arrowecs.cz)

©2003–2012 Check Point Software Technologies Ltd. Všechna práva vyhrazena. Check Point, AlertAdvisor, Application Intelligence, Check Point 2200, Check Point 4000 Appliances, Check Point 4200, Check Point 4600, Check Point 4800, Check Point 12000 Appliances, Check Point 12200, Check Point 12400, Check Point 12600, Check Point 21400, Check Point 6100 Security System, Check Point Anti-Bot Software Blade, Check Point Application Control Software Blade, Check Point Data Loss Prevention, Check Point DLP, Check Point DLP-1, Check Point Endpoint Security, Check Point Endpoint Security On Demand, logo Check Point, Check Point Full Disk Encryption, Check Point GO, Check Point Horizon Manager, Check Point Identity Awareness, Check Point IPS, Check Point IPSec VPN, Check Point Media Encryption, Check Point Mobile, Check Point Mobile Access, Check Point NAC, Check Point Network Voyager, Check Point OneCheck, Check Point R75, Check Point Security Gateway, Check Point Update Service, Check Point WebCheck, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, DefenseNet, DynamicID, Endpoint Connect VPN Client, Endpoint Security, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IP Appliances, IPS-1, IPS Software Blade, IPSO, R75, Software Blade, IQ Engine, MailSafe, logo More, Better, Simpler Security, Multi-Domain Security Management, MultiSpect, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, logo puresecurity, Safe@Home, Safe@Office, Secure Virtual Workspace, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, SecurityPower, Series 80 Appliance, SiteManager-1, Smart-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, SmartEvent, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartReporter, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SmartWorkflow, SMP, SMP On-Demand, SocialGuard, SofaWare, Software Blade Architecture, logo softwareblades, SSL Network Extender, Stateful Clustering, Total Security, logo totalsecurity, TrueVector, UserCheck, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Edge, VPN-1 MASS, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VE, VPN-1 VSX, VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Antivirus + Firewall, ZoneAlarm DataLock, ZoneAlarm Extreme Security, ZoneAlarm ForceField, ZoneAlarm Free Firewall, ZoneAlarm Pro Firewall, ZoneAlarm Internet Security Suite, ZoneAlarm Security Toolbar, ZoneAlarm Secure Wireless Router, Zone Labs a logo Zone Labs jsou ochranné známky nebo registrované obchodní značky společnosti Check Point Software Technologies Ltd. nebo jejich dceřiných společností. Společnost ZoneAlarm je součástí společnosti Check Point Software Technologies, Inc. Company. Všechny ostatní názvy produktů zde uvedené jsou ochrannými známkami nebo registrovanými obchodními značkami jejich příslušných vlastníků. Produkty popisované v tomto dokumentu jsou chráněny patenty USA č. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, 7,165,076, 7,540,013, 7,725,737 a 7,788,726 a mohou být chráněny jinými patenty v USA nebo v jiných zemích nebo může být o patent zažádáno.