

Check Point Software Blade Architecture

Achieving the right balance between security
protection and investment

Contents

- Introduction 3
- Check Point Software Blade architecture overview 3
- What is a Software Blade? 4
- How are Check Point Software Blades deployed? 4
- Building a security solution using Software Blades 5
- Select a solution that can grow with your business 6
- What makes Check Point Software Blade Architecture different? 7
 - More Security 8
 - Flexibility 8
 - Simplicity 8
- Multi-core optimized security software 8
- Benefits of Software Blade architecture 9
 - Business Scenario 1: Consolidate security functions 10
 - Business Scenario 2: Open new branch office 12
- Blade functions 13
- Balancing security protection and investment 15



Introduction

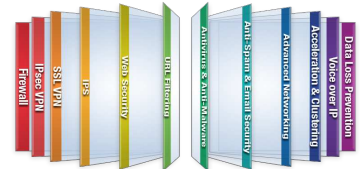
Protecting networks against today's constantly evolving threat environment has never been more challenging. Infrastructure, connectivity and performance requirements keep growing. New and varied threats are leading to more security vendors and point-products—including firewalls, intrusion prevention systems (IPS), Data Loss Prevention (DLP) and application control, just to name a few. All of this adds more and more complexity. Meanwhile, IT teams are under increasing pressure to reduce costs and complexity, and do more with existing hardware and resources. The combination of these challenges has led to ineffectual approaches that are increasingly inefficient, costly and unsustainable.

As a result, organizations and IT teams are looking for an effective solution—one that is more simple, flexible and easier to manage. This includes the freedom to add critical protection as needed, without worrying about performance, availability or forklift upgrades. It also means the ability to invest in security only as you need it, without having to introduce yet another security vendor and point appliance.

Check Point Software Blade Architecture Overview

The Check Point Software Blade Architecture is the first and only security architecture that delivers total, flexible and manageable security to companies of any size. It enables organizations to easily and efficiently tailor their network security infrastructure to meet critical and targeted business security needs—all while maintaining network performance service level agreements (SLAs). What's more, as new threats and needs emerge, Check Point's Software Blade Architecture quickly and flexibly extends security services on-demand—without the addition of new hardware or management complexity. All solutions are centrally managed through a single console that reduces complexity and operational overhead

Check Point Software Blades deliver lower total cost-of-ownership (TCO), faster return-on-investment (ROI), and cost-efficient protection to meet any network security need—today and in the future.



softwareblades
from Check Point

Independent.

Modular.

Centrally managed.



What is a Software Blade?

A Software Blade is a security building block that is independent, modular and centrally managed—allowing organizations to customize a security configuration that targets the right mix of protection and investment. Software Blades can be quickly enabled and configured on any gateway or management system with a simple click of a mouse—no hardware, firmware, or driver upgrades required. And as needs evolve, additional software blades can be easily activated to extend security to an existing configuration on the same security hardware.

How are Check Point Software Blades deployed?

Software Blades can be deployed on Check Point UTM-1™, Power-1™, and IP Appliances and open servers. New Software Blades can be easily added to your existing hardware platform by simply ‘turning on’ their functionality in Check Point’s centralized, easy-to-use management console. No additional hardware, firmware or drivers are necessary. This enables organizations to deploy security dynamically—as needed—with lower total cost of deployment.

The Firewall Blade—with Check Point’s award-winning FireWall-1® technology—is always included.

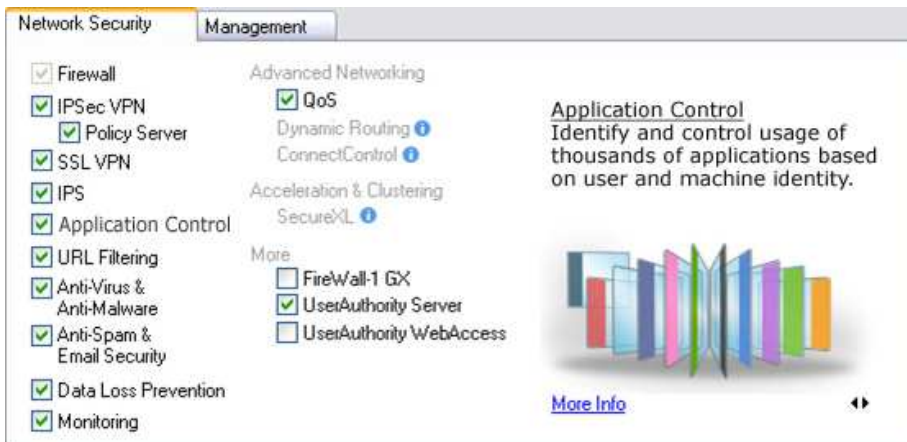


Figure 1. Check Point Security Gateway R70—SmartDashboard

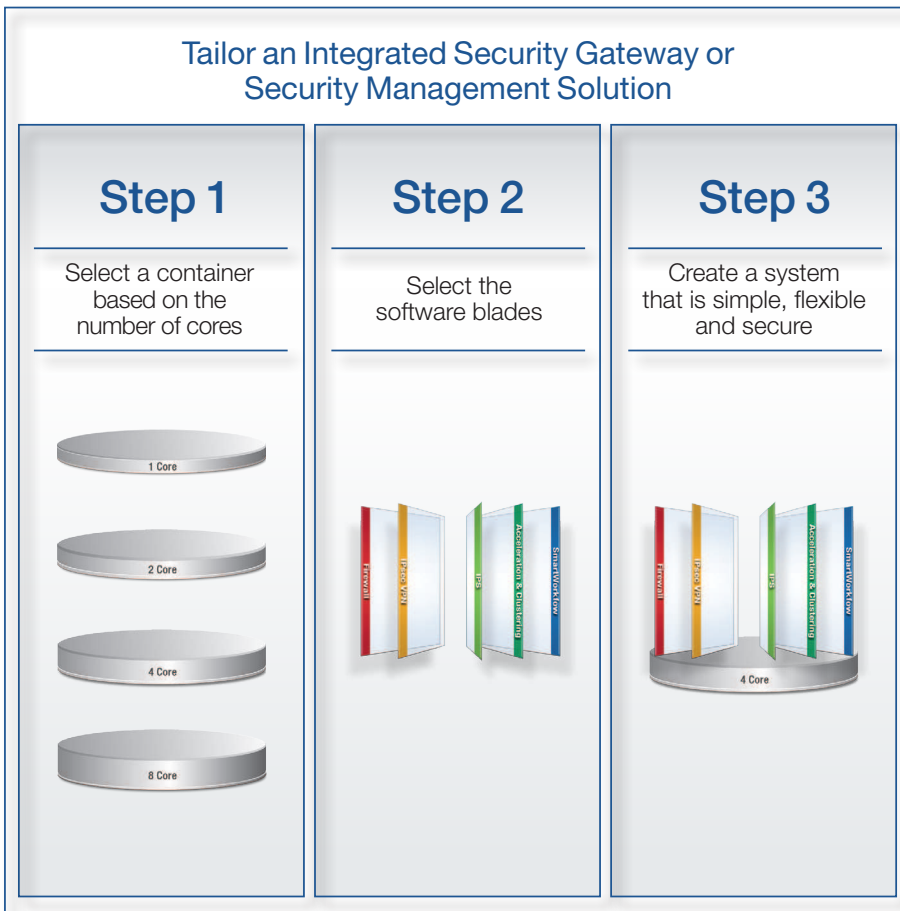
Key Benefits

- Simplicity
- Manageability
- More Security
- Lower TCO
- Guaranteed performance
- Lower carbon footprint



Building a security solution using Software Blades

Check Point's Software Blade Architecture allows for simple and efficient customization of tailored systems for your business. Or, choose from a full selection of predefined, turn-key solutions. Extend your security solution with a click of a mouse. Easily add new security Software Blades with Check Point's flexible, easy-to-use management console.



Select a solution that can grow with your business

Whether designing a solution for an enterprise headquarters or data center, branch office, or mid-size business, Check Point's Software Blade Architecture provides unmatched configuration flexibility. The result is a complete gateway or management system configured precisely to your specific business needs.



What makes Check Point Software Blade Architecture different?

Check Point Software Blade architecture is different because it allows IT to customize a modular security solution on a single, common platform that can easily be extended or modified as needs change. The architecture also delivers a high level of flexibility without sacrificing performance. Security gateway performance can be guaranteed when multiple blades are deployed by enabling performance thresholds. Thresholds, set by IT personnel, control the provisioning of system resources—such as CPU cycles and system memory—to the IPS Software Blade.

In this example, IPS inspection can be disabled if the resource usage exceeds defined thresholds. This enables the security gateway to maintain a high level of performance even when under heavy load.

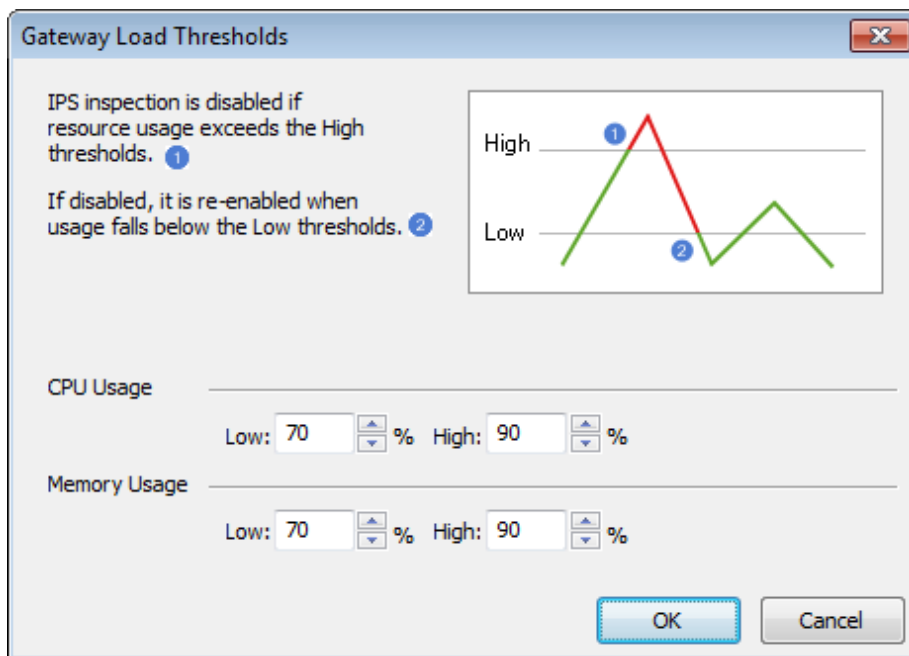


Figure 2. Setting usage thresholds to guarantee performance

This solution supports an unlimited number of system configurations, which makes it easy for organizations to customize and upgrade their security infrastructure by consolidating functions or increasing performance. For example, since all security functions are controlled by a single security management system, IT administrators don't have to master various GUIs, learn new interfaces or figure out how different vendor solutions interact with each other.



More Security

There's no need to cobble together different solutions from various vendors because the Check Point Software Blade Architecture is a comprehensive solution comprised of best-of-breed technologies for both security gateway and management functionality. It provides the right level of security at all enforcement points and network layers, which effectively reduces the risk of exposure to security threats.

Flexibility

When organizational needs change, Check Point offers the ultimate flexibility, as all Software Blades can be easily activated or transferred from one hardware platform to another. Because Software Blades are completely portable, organizations can easily:

- Consolidate multiple security functions on a single platform
- Change the combination of security functions on a particular gateway
- Offload some functions to a second gateway

Simplicity

It's simple to activate new security functions via the central Software Blade management system, as illustrated in Figure 1. This capability reduces the number of administrative tasks associated with updating, monitoring, event analysis, and reporting.

Multi-core optimized security software

Designed specifically to leverage the latest multi-core processors, Check Point Software Blade Architecture integrates CoreXL™ technology, which increases deep-packet inspection throughput needed for intrusion detection in an integrated security gateway. Using intelligence built into the director core, CoreXL distributes the load equally among the cores running the Check Point security gateway, as shown in Figure 3.

CoreXL is designed to use as many cores as are available (4, 8, 16, and so on), enabling it to scale on higher-capacity systems without changes. The Check Point security gateway migrates easily to new systems with more cores and allows companies to increase performance without changing solutions.



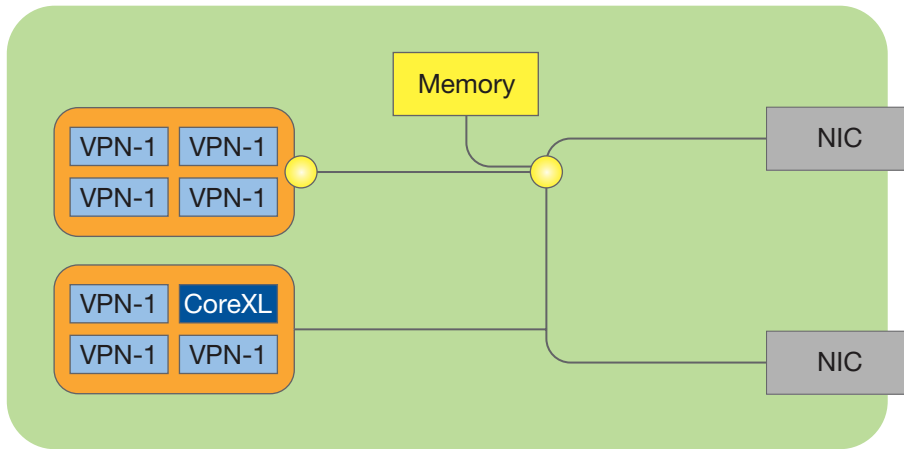


Figure 3. Check Point CoreXL intelligently balances security duties across multiple cores

Benefits of the Software Blade Architecture

Check Point Software Blade Architecture facilitates straightforward configuration and policy changes, including the ability to add new security applications to an existing platform or migrate security functions to another platform in a seamless manner, with no downtime. Software Blades can be added, swapped, or removed as needed. When configuration changes are made, the Software Blade container carries out all the necessary adjustments. This simplifies the task of consolidating and adding performance to existing Check Point security solutions and enables organizations to deploy security dynamically.

This solution offers unmatched benefits to organizations responding to changing business and security needs, as shown in Table 1. The Check Point Software Blade Architecture provides industry-leading security threat protection that is easy to manage and has a lower TCO than one-size-fits-all or multi-vendor solutions. These benefits are discussed in more detail in the next two business scenarios.

Table 1. Key benefits of the Check Point Software Blade Architecture

Features	Benefits
Simple deployment and upgrades	Responds to business-environment changes
New security functions run on existing platforms	Reduces TCO (total cost of ownership)
Comprehensive set of security modules	Combats evolving threats
Central management via Web-based GUI	Keeps things simple and manageable



Business Scenario 1: Consolidate security functions

Situation: Business growth has resulted in sprawling security infrastructure that spans many organizations and locations, as shown in Figure 4. The current configuration increases cost and risk because IT administration must support several generations of multi-vendor equipment based on custom hardware and dedicated management software.

IT requirements:

- A standardized security platform that reduces operational expense-related change and configuration management of security systems
- The flexibility to implement global and/or local policy management
- Central visibility into security effectiveness: incident logging and tracking, system health checks, user monitoring and compliance audits and reporting
- Common hardware that runs all security functions and maximizes the potential cost savings from reducing hardware footprint, rack space, cabling and utility costs
- System configurations tuned for locations, which avoids the overhead and cost from unused security functions

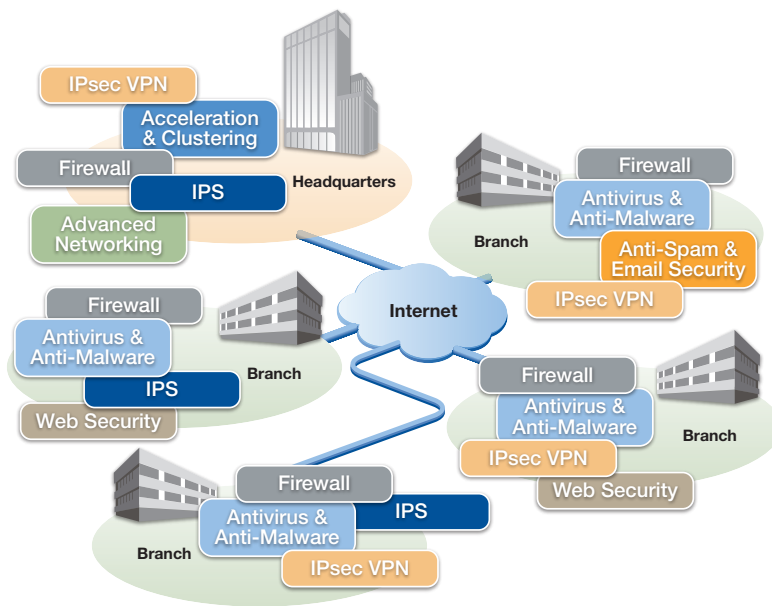


Figure 4. Organizational infrastructure before consolidation



Solution: Check Point Software Blade configurations, as shown in Figure 5 and described in Table 2, are customized for each business location. The same Check Point container software runs at every location, simplifying management and policy proliferation and cutting validation time. Employing a single hardware platform, each location runs the security function it needs, which optimizes cost/performance. IT can easily move functions around, from location to location, and leverage their existing infrastructure. The result is one deployment project, multiple configurations and a single system-management function.

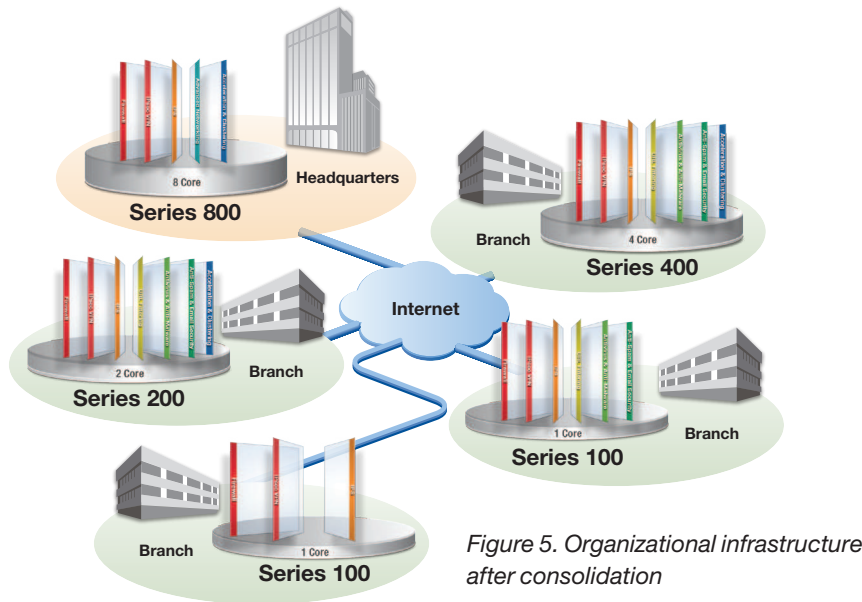


Table 2. Check Point Security Gateway Systems

Series	Software Blades	Description
100	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware	<ul style="list-style-type: none"> Entry-level security gateway for small or branch offices Limited to 50 users and recommended for up to 8 ports
200	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	<ul style="list-style-type: none"> Limited to 500 users and recommended for up to 12 ports Comprehensive XTM (eXtensible Threat Management) security gateway with high performance capabilities for mid-sized companies and offices
400	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	<ul style="list-style-type: none"> High-performance security gateway for offices of any size Unlimited number of users and recommended for up to 16 ports
800	Firewall, VPN, IPS, Advanced Networking, Acceleration & Clustering	<ul style="list-style-type: none"> The highest-performance security gateway designed for the most demanding performance environments Ideal for large campuses and data centers



Business Scenario 2: Open new branch office

Situation: Business is expanding and additional branch offices must be supported. Today, existing branch offices are outfitted with inflexible solutions that can't scale and don't protect infrastructure investment. Security solutions at branch offices look nothing like what's deployed at headquarters, but they need the same level of protection as the corporate network since they are subjected to the same Internet threats.

IT requirements:

- One-stop shopping for all branch office connectivity and security functions to reduce cost and complexity
- All security policies provisioned from and managed at a central Security Operations Center, which minimizes deployment effort and enforces consistency with enforcement of security policy
- The ability to scale as needs change, such as adding more security, performance or features (e.g., IPS, acceleration, clustering, VoIP security)

Solution: Check Point Software Blades are deployed in branch offices and central headquarters. The turnkey Check Point solution includes everything branch offices need to provide immediate connectivity and security for all branch office IT assets (e.g., network, servers, PCs, laptops). Organizations can manage policy centrally from headquarters—no local expertise required—or management responsibilities can be delegated to local administrators if desired.

The Check Point Provisioning Management Software Blade enables easy deployment and provisioning of security services for branch offices. This capability provides centralized administration and provisioning of Check Point security devices via a single management console. Using profiles, a network administrator can easily deploy security policy or configuration settings (e.g., DNS, hosts, domain, routing and interface settings) to multiple, geographically distributed devices.

The Provisioning Software Blade also provides centralized backup management and a repository of device configurations, so administrators can easily apply existing configurations to new devices. Managed devices fetch their assigned profiles from a centralized management server, enabling one profile change to update hundreds of devices, each acquiring the new common properties, while maintaining its own local settings. By automating device configuration, the Provisioning Software Blade reduces administrative overhead, reduces errors, and ensures security consistency across the network.



Blade functions

Software Blades, shown below, enable organizations to efficiently and quickly tailor security gateway and management functionality to specific and changing security needs. New blades are quickly licensed as needed without the addition of new hardware. Security Gateway, Security Management and Endpoint Security Software Blades available today are listed in Figure 6, 7 and 8.

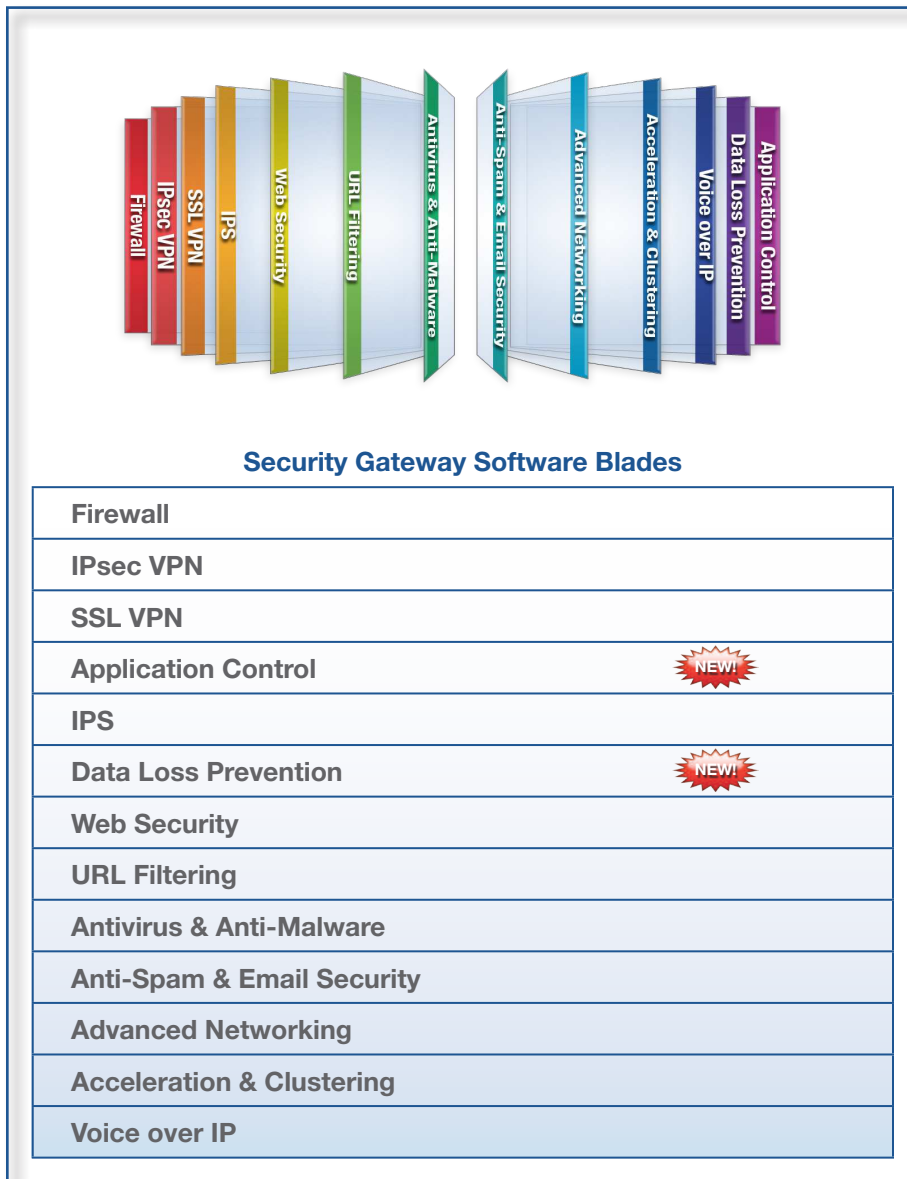


Figure 6.



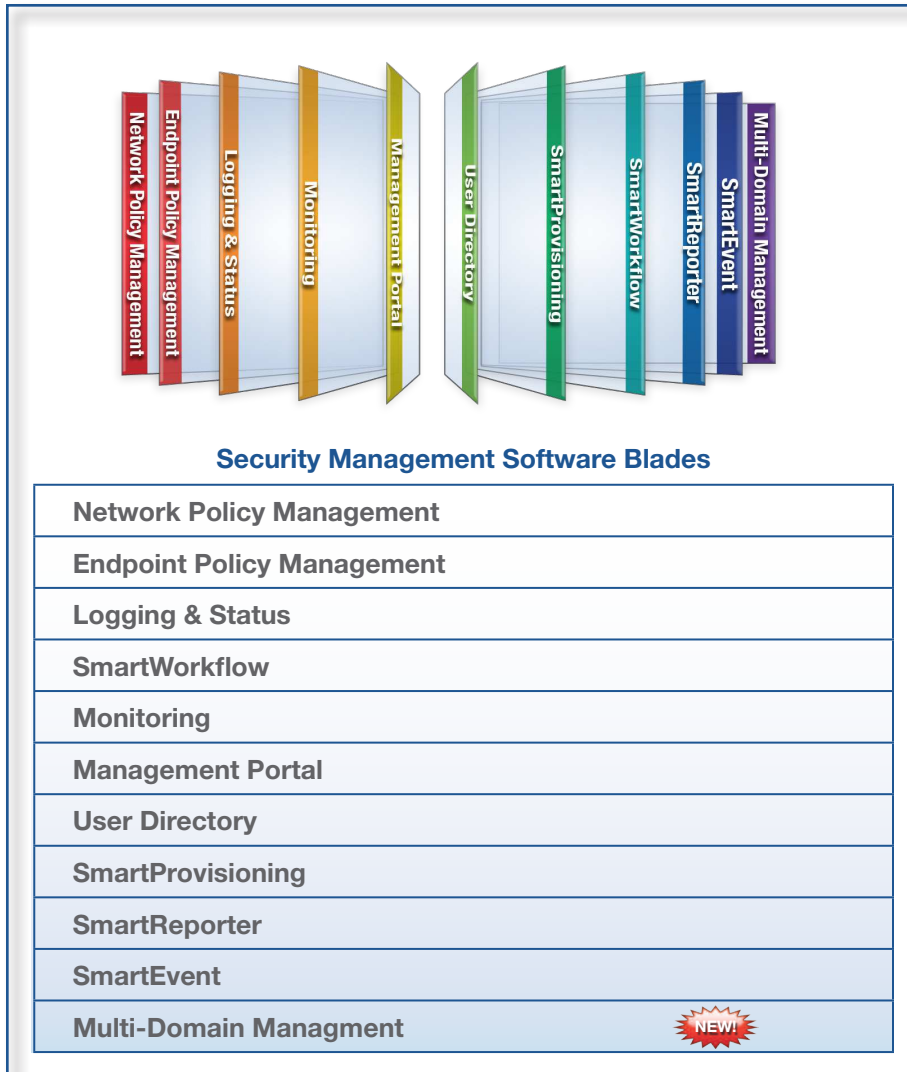


Figure 7.



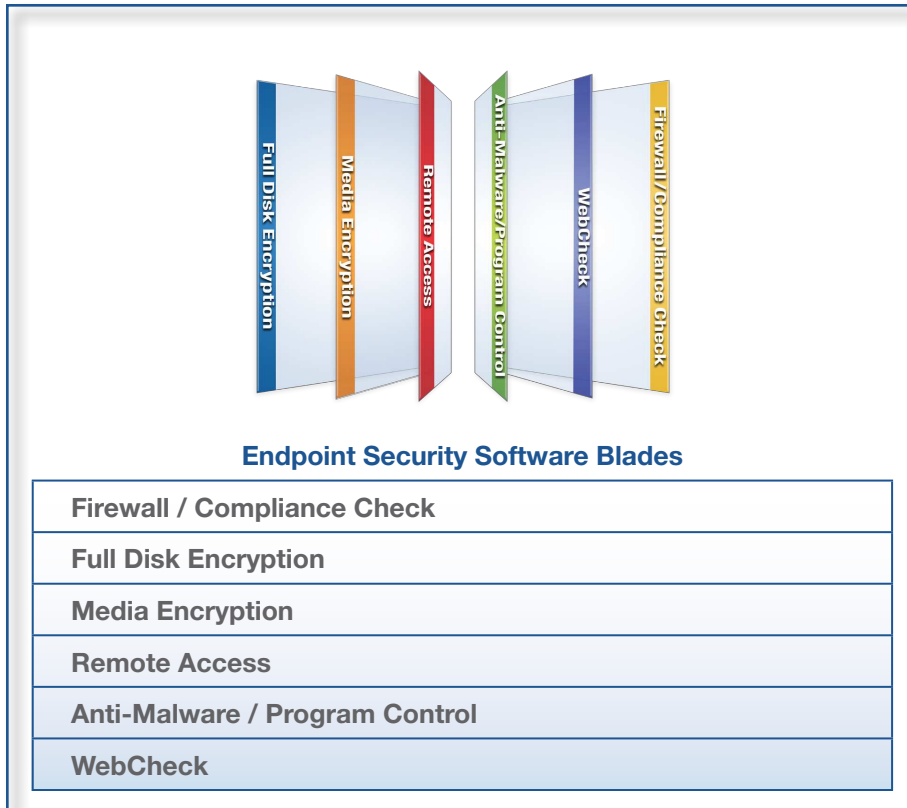


Figure 8.

Balancing security protection and investment

The continued evolution of security software and general-purpose servers delivers more flexibility for better security function consolidation and reuse. With Check Point Software Blade architecture, enterprises can buy the right amount of protection at the right price. Software Blades compliment existing Check Point firewall protection solutions, further securing networks without degrading gateway performance.

To learn more about Check Point Software Blade architecture, please visit <http://www.checkpoint.com/products/softwareblades/architecture/>



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Soleim 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
URL: <http://www.checkpoint.com>

©2003–2010 Check Point Software Technologies Ltd. All rights reserved. Check Point, Abra, AlertAdvisor, Application Intelligence, Check Point DLP, Check Point Endpoint Security, Check Point Endpoint Security On Demand, the Check Point logo, Check Point Full Disk Encryption, Check Point Horizon Manager, Check Point Media Encryption, Check Point NAC, Check Point Network Voyager, Check Point OneCheck, Check Point R70, 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, DLP-1, DynamicID, Endpoint Connect VPN Client, 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, Software Blade, IQ Engine, MailSafe, the More, better, Simpler Security logo, 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, the puresecurity logo, Safe@Home, Safe@Office, Secure Virtual Workspace, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, 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, SofaWare, Software Blade architecture, the softwareblades logo, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, 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-1, Web Intelligence, ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm DataLock, ZoneAlarm Extreme Security, ZoneAlarm ForceField, ZoneAlarm Free Firewall, ZoneAlarm Pro, ZoneAlarm Internet Security Suite, ZoneAlarm Security Toolbar, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, 7,165,076, 7,540,013 and 7,725,737 and may be protected by other U.S. Patents, foreign patents, or pending applications.