totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Check Point Endpoint Security

Single agent for endpoint security delivering total protection and simplified management

Contents

Executive summary 3
Meeting the challenge of securing endpoints 4
A new strategy: Unifying endpoint security 5
Performance benefits of unifying endpoint security 8
Check Point Endpoint Security 8
Conclusion/learn more 10

Executive summary

Any organization concerned about information security would discover that endpoints are the universal Achilles heel of risk. Endpoints bring three significant new risks. First, attacks increasingly bypass traditional perimeter-focused security and enter endpoints and the enterprise network through a variety of methods, such as interaction with malicious Web sites. Second, a large number of endpoints are mobile so they may be used both inside and outside the traditional perimeter of security controls. Finally, endpoints present a huge logistical challenge to IT staff who often must manage deployment of policies and controls for multiple security agents on each physical device.

Endpoints need proper security controls, or they face higher odds of falling to a vulnerability exploit. Successful exploits of vulnerabilities on endpoints can lead to stolen data, disruptions of business operations, and potential penalties for non-compliance with laws and regulations on security.

To respond to these challenges, enterprises are turning toward a new strategy that includes a broad set of technologies for endpoint security unified into a single agent with central control. This is the right strategy, but ensuring its success requires implementation of all controls covering major security risks to endpoints. In addition to functional scope, enterprises must also ensure that operational overhead for security controls on endpoints is negligible, that controls are invisible to end users, and that the entire solution can be cost effectively and efficiently managed from a central location. This white paper describes these risks and a unified solution called Check Point Endpoint Security™.

Meeting the challenge of securing endpoints

From an IT and security manager's perspective, technology infrastructure and data were easier to protect and safer before PCs, networking, and the Internet permeated organizations. During this transition, the network perimeter was the focus of security efforts as organizations sought to repel external digital attacks from penetrating into internal systems. Hackers and criminals learned how to exploit vulnerabilities with new types of attacks, which have resulted in demands for a corresponding maze of new security solutions. Conventional wisdom is to implement comprehensive protection with a layered approach to network and information security so potential vulnerabilities are not overlooked.

Now, experts urge attention toward a major new area of risk that needs its own layer of security—the endpoint. Endpoints are any computing devices attached to an organization's network including PCs, notebooks, handheld computing, or electronic devices with storage, I/O, and/or wireless connectivity, and IP-networked devices with programmable logic controllers used for industrial-control systems and critical infrastructure.

Endpoints are susceptible to a variety of attack vectors, especially vulnerabilities in common networking protocols that enable access through open or uncontrolled ports. Other exploits target programming errors in sizing software data buffers, whose overflow can corrupt the stack or heap areas of memory and allow execution of malicious code. Most PCs run on one of the Windows operating systems (OSes) from Microsoft, which makes them vulnerable to hackers focusing attacks on the hundreds of millions of devices using these platforms. But whatever the OS, all endpoints using IP are vulnerable to attack, and many fear endpoints are the new Achilles heel in the enterprise network.

Endpoints pose three major risks

Endpoints bring three significant new risks to enterprise IT. First, attacks increasingly bypass traditional perimeter-focused security and infiltrate enterprise networks via Web-based applications accessed by endpoints. Malicious Web pages can exploit browser vulnerabilities simply by being viewed. Most of these dangers such as cross-site scripting attacks pose risks to almost every browser. Web-based network access also poses other threats such as disclosure of cookies or local files, execution of local programs or malicious code, or complete takeover of vulnerable PCs.

The second risk is that a growing percentage of endpoints are mobile and may be used inside and outside the traditional perimeter of security controls. Laptops represent approximately 50 percent of overall PC shipments worldwide,[1] and that number continues to grow. Endpoints that do not run their own local security controls are exposed to danger when they are used outside the safety of perimeter-based controls.

Finally, endpoints present a huge logistical challenge to IT staff who must manage deployment of policy-based controls to each physical device. Deploying security software, installing updates and new signature files, and maintaining consistent policy and configurations are time-consuming tasks and difficult to do on a manual basis—especially for enterprises with thousands of mobile endpoints.

[1] Source: 451 Group

A new strategy: Unifying endpoint security

Prudent IT security managers view endpoints as vulnerable "islands" of risk, especially when they are used as mobile devices outside enterprise network-perimeter controls. The way to prevent exploitation of vulnerabilities on endpoints is to deploy a comprehensive layer of endpoint security on each PC.

Enterprises have typically deployed some standalone point solutions for endpoint security such as a personal firewall or antivirus software. This approach quickly becomes a management nightmare in organizations with hundreds or thousands of PCs. For example, each time a software update is available for individual endpoint agents, IT must execute a rigorous engineering test cycle to qualify the release for performance and compatibility before pushing the update out to endpoints. Because it is not uncommon for enterprises to have three or more endpoint security agents on each device, implementation can become very time-consuming and costly.

A new strategy is to unify endpoint security with functionality on each PC that is centrally deployed and managed by IT security specialists on a single console. Unification of security functionality allows for simplified deployment and management, which lowers the overall cost of operations. With a unified agent approach, IT will only have to run test cycles for one agent and will have the assurance that each function within that agent is compatible. However, to achieve strong endpoint security, an enterprise should carefully consider functions in a particular unified endpoint solution. Only a comprehensive set of security controls can provide an enterprise with complete endpoint security.

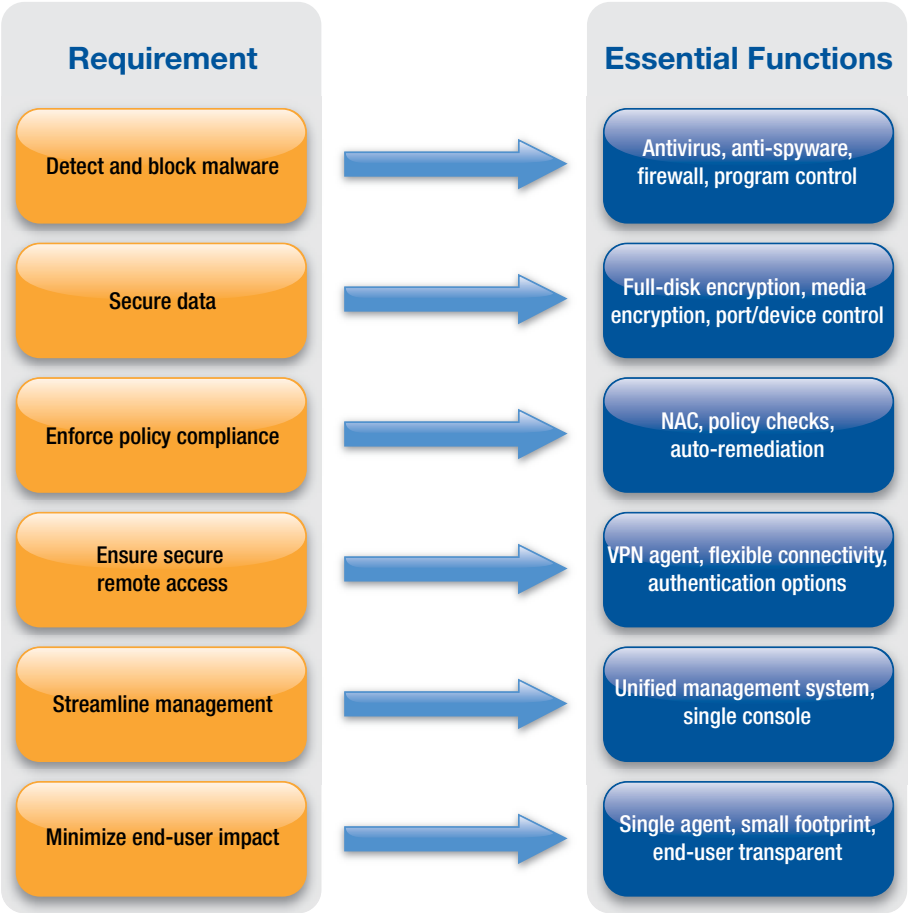
At a minimum, for unified endpoint security, organizations should consider requiring steps to:

- Detect and block malware
- Secure data
- Enforce policy compliance
- Ensure secure remote access
- Streamline management
- Minimize end-user impact

1. Detect and block malware

Detection of malware and blocking it from execution on endpoints is typically fulfilled by deploying separate point products for firewall, antivirus, and anti-spyware. Each of these security applications provides vital, unique functionality toward the collective requirement of detecting and blocking malware.

A firewall with program control is the most important of these security controls because it provides core manipulation of inbound and outbound traffic. Only a firewall can block unwanted traffic such as malicious code, control which applications are allowed network access, and make endpoints "stealthy" by having them appear invisible to hackers. As a matter of product heritage, some endpoint security suites are built around antivirus, but the firewall is best suited as the first line of defense due to its ability to control traffic to and from the endpoint PC.



Essential requirements for unified endpoint security

Antivirus is used to identify and stop infiltration of viruses. A quality antivirus application uses a combination of detection techniques, such as signature matching and heuristics. The former technique spots viruses by matching files against a database of previously identified malicious code. Heuristics identify viruses by matching file delivery and code behavior against known threats.

Anti-spyware stops infiltration of worms, Trojans, adware, and keystroke loggers. It provides real-time protection against spyware installation on endpoints and the detection and removal of spyware that was previously installed.

For all these measures, it is important for administrators to have central control and visibility over endpoints to ensure compliance with endpoint security policy. For example, that means having the ability to schedule scans at regular intervals on PCs and view reports on the compliance level of PCs, the percentage of PCs that had a full virus scan in the past week, and the number of PCs that are currently infected.

2. Secure data

Securing data on endpoints is critical since it's so easy to steal or lose a laptop PC or other mobile device. Once it falls into unauthorized hands, clear-text data

on the endpoint is immediately available for access and exploitation. Controls to secure endpoint data include full-disk encryption, media encryption, and port/device control.

Encryption is the process of making data unreadable to anyone except those who have special knowledge, usually requiring a key to decrypt the data and render it readable again. Encryption may be applied to an individual file, a folder, an entire disk, or other type of storage media. In the past, encryption has been cumbersome to execute on endpoints and hindered system performance. Newer encryption solutions have solved these issues and been deployed globally on millions of endpoints.

Port/device control is a relatively new technology that allows enterprises to centrally control the use of individual ports on an endpoint. One practical benefit is preventing unauthorized transfer of protected data from an endpoint to a personal storage device such as a USB memory stick. Port control also prevents the transfer of malware from external storage devices onto an endpoint—and on toward the enterprise network.

3. Enforce policy compliance

Enforcing policy compliance makes an endpoint comply with security policy before it is granted access to the network. At a basic level, this requirement does a policy check on each endpoint for security policy and enforcement rules created by administrators. For example, compliance may require each endpoint to have the most current version of antivirus software, critical patches, the latest applications, or assurance that the endpoint is not running prohibited programs. Failing a policy check will block network access for an endpoint.

Heterogeneous enterprise networks require policy compliance to work with gateways and authentication systems from multiple vendors. Policy compliance in a unified endpoint security scheme should support industry-standard 802.1x authentication to enable network access control (NAC) in multivendor environments. It should also support auto-remediation for automatic retrieval and installation of updates on noncompliant endpoints. Another requirement is on-demand compliance, which enforces security policy on unmanaged endpoints without the need for IT to install agent software, provides session confidentiality for those devices, and detects and disables spyware. As an example, when an employee accesses the corporate network via an SSL VPN gateway from a PC located at an Internet cafe or airport kiosk, IT has to be able to ensure that these machines are safe to access the network. IT also has to ensure session confidentiality so nothing is left behind after an employee ends a remote access session.

4. Ensure secure remote access

The prevalence of mobile computing makes secure remote access a key requirement for endpoint security. Technologies include a remote access agent, flexible connectivity, and authentication options.

Virtual Private Network (VPN) technology is the most common means to enable secure remote access to an enterprise network gateway. The remote access link protects communications by providing a secure, encrypted tunnel for access, preventing eavesdropping and data tampering.

Flexible connectivity should include dynamic and fixed IP addressing for dialup, cable modem, or digital subscriber line connections. It should enable the addressing of potential routing issues between the agent and the remote access gateway by encapsulating IP packets with the original remote user IP address, thereby enabling users to appear as if they were "in the office" while connecting remotely.

Authentication options should include support for SecurID tokens, username and password, RADIUS, TACACS, and biometrics.

5. Streamline management

A big goal of unified endpoint security is to manage everything from a single console. It should provide central configuration, policy administration, reporting, and analysis of all endpoint security—including all the security controls described above that are deployed on every enterprise endpoint. Enterprises should expect streamlined management to include:

- Centralized and delegated management options
- Central monitoring and reporting on every endpoint security control
- Faster security incident discovery, monitoring, and forensics
- Comprehensive reporting and support for audits and compliance
- Easier, faster deployment of software on agents without requiring on-site manual intervention of IT or end users
- Unification of endpoint security with network security event management

6. Minimize end-user impact

It is important that unified endpoint security stay out of end users' ways as they do their work. The ideal is to have all security control functionality contained in a single, small-footprint agent on the endpoint. Most endpoint security suites actually require loading three, four, five, or even more agent software modules onto each PC. As a result, security applications begin to swamp memory utilization, consume CPU cycles, and trigger sluggish performance of business applications. Annoyance from end users grows when they are expected to manually process updates to security software, patches, and other system maintenance. Fewer agents result in easier management, better performance, less user intervention, and stronger endpoint security.

Performance benefits of unifying endpoint security

Unification of comprehensive unified endpoint security functions results in a low-impact, small-agent-footprint, and better-performing endpoint system. With fewer agent modules, such a system would be easier to deploy and manage.

Check Point Endpoint Security

Check Point Endpoint Security represents a new opportunity for existing customers and other organizations to unify endpoint security for total protection, control, and performance. This software unifies all the major security controls required for comprehensive protection of endpoints and does it in a low-impact, small-footprint agent that is centrally controlled and requires no user action.

Unified functionality of Check Point Endpoint Security

Function	Description
Firewall	Based on 15 years of firewall leadership and leveraging the widely deployed ZoneAlarm® personal firewall technology, Check Point Endpoint Security provides proactive inbound and outbound protection. It prevents malicious code from compromising endpoint PCs, blocks unwanted traffic, and uses a "stealth mode" to make endpoints invisible to hackers scanning for vulnerable systems.
Program control	Controls application behavior using traditional firewall rules. It automatically creates an inventory of all PC applications that attempt network access, enabling fast, efficient identification, and securing of potential network vulnerabilities. Also ensures that approved programs cannot be spoofed, tampered with, or hijacked.
Program Advisor	Provides administrators the ability to automate most application policy decisions based on real-time data collected from millions of PCs worldwide. Leverages the Check Point knowledge base of trustworthy applications and malware to immediately apply a best-practices policy that either blocks or allows program communication. It also automatically kills the execution of any malicious program identified.
Network access control (NAC)	Lets administrators control access to their networks and enforce endpoint policy for both VPN-based access and internal network access. NAC functions can interoperate with Check Point gateways as well as infrastructure devices from leading network equipment manufacturers. And support for industry-standard 802.1x authentication enables NAC in multivendor networking environments—with or without Check Point infrastructure.
Antivirus	Unified, high-performance antivirus technology detects and eliminates viruses and other related malware from endpoints. Virus detection is based on a combination of signatures, behavior blockers, and heuristic analysis that together enable your network environment to attain one of the industry's highest detection rates.
Anti-spyware	Protects enterprises from the financial damage caused when spyware steals or exposes sensitive data, congests internal networks, and increases helpdesk expenses by slowing PC performance. It features centrally configurable and enforceable signature updates to ensure that endpoints have the latest spyware protection at all times.
Data security*	Check Point Endpoint Security uses Pointsec® market-leading data security technology to provide confidential data protection through an efficient blend of preboot authentication with full-disk encryption, media encryption, and port management. Full-disk encryption provides a simple-to-deploy combination of strong encryption with access control that completely protects all hard-drive data while remaining transparent to end users. Media encryption provides strong and enforceable encryption for all policy-approved removable media in the organization, such as USB flash drives. Port protection includes comprehensive inbound and outbound content control through data inspection, centralized auditing, and port management working in concert to prevent data leakage.
Remote access	Check Point Endpoint Security is the only endpoint solution that unifies an advanced IPSec VPN agent, based on the award-winning VPN-1® SecureClient™, delivering secure remote access as an integral part of endpoint security. This IPSec VPN functionality is fully unified into the single endpoint security agent, sharing the same end-user interface and system tray icon as the other endpoint security functions.
Unified management	Gives administrators powerful tools to enhance and customize endpoint security policies to the specific needs of their organizations. They can define distinct policies that are automatically applied to endpoints as they move between networks, locations, and gateways. Check Point Endpoint Security minimizes the time and effort necessary to manage deployments and security policies so that business can continue smoothly, safely, and efficiently.
Integration with Check Point Unified Security Architecture	Based on the Check Point Unified Security Architecture, administrators can manage endpoint security and NAC with the same SmartCenter™ and Provider-1® management systems used to manage other Check Point products. Unification eliminates the need for separate management logins and servers, reducing IT time, costs, and complexity—while improving overall enterprise security.

*Single agent including data security available Q3 2008

Conclusion/learn more

Without unified endpoint security, endpoints are the new Achilles heel of network and information security. By using the industry's most comprehensive endpoint security solution—Check Point Endpoint Security—enterprises can ensure the application of unified security controls on every endpoint, while simplifying management of endpoint security across the enterprise. Check Point Endpoint Security unifies the highest-rated firewall, network access control (NAC), program control, antivirus, anti-spyware, data security and remote access in a single, centrally managed agent, eliminating the need to manage multiple endpoint security agents and dramatically reducing the time and effort for endpoint security administration.

Check Point, the global leader in network security, data security, and security management, invites you to contact us for more information about Check Point Endpoint Security.

Product information

http://www.checkpoint.com/products/endpoint_security

Corporate headquarters

1-800-429-4391

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

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
URL: **http://www.checkpoint.com**

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, 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, IPS-1, IQ Engine, MailSafe, 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, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, 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 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, 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, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.

July 22, 2008 P/N 503073