totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Comprehensive Endpoint Security

New endpoint vulnerabilities such as Web-based malware are increasing information security risk in the enterprise

Contents

Executive Summary

In recent years, malicious activity on the Internet has advanced from worms and viruses attacking random computers in the wild, to the highly sophisticated and targeted attacks - such as the TJ Maxx and Heartland data breaches - that plague enterprises today. Individual hackers have been replaced by well-organized and globally dispersed criminal enterprises, motivated by easy and difficult-to-trace illicit financial gains. Valuable data, e.g. personal identity and consumer credit card information, is stolen from target organizations such as retailers, data processing facilities and government entities, and quickly sold to the highest bidder through global online clearing houses. As these criminal organizations improve their skills and increase their profits, costs to enterprises also increase; resulting in major business disruptions, loss of credibility with customers, and financial penalties arising from the violation of state and federal privacy laws and regulations.

When conducting security audits to address these new threats, legitimate organizations are quickly discovering that endpoints – sometimes numbering in the thousands of network-connected PCs and devices – are the new 'Achilles' heel' of information security. In a stop-gap attempt to protect endpoints and keep pace with new compliance rules, enterprises have been rapidly deploying multiple endpoint security agents and technologies from multiple vendors. Unfortunately, as each new endpoint security component may require a separate management server, configuration profile, security policy, update schedule and pre-deployment compatibility testing, this 'ad-hoc' strategy severely compounds administrative overhead and management complexities.

In order to simplify endpoint security and reduce costs, forward thinking companies are requesting the unification of endpoint security components into a single agent with centralized control. To be successful, enterprises pursuing this strategy must ensure that any new solution includes controls to protect against all types of endpoint attacks, is transparent to end users, and can be managed and enforced efficiently from a central location. This white paper will identify key endpoint vulnerabilities and introduce practical and efficient new solutions for endpoint security.

Developments in Enterprise Security

From an IT manager's perspective, technology infrastructure and data were far easier to protect before networked PCs and the Internet began to permeate organizations. During this transition to modern IP-based infrastructures, the network perimeter was the primary focus of security efforts. Hackers, however, quickly found ways through these rudimentary defenses, creating demand for ever more powerful and redundant network security solutions.

Today, conventional wisdom instructs businesses to implement network security using a comprehensive, multi-layered approach covering all potential vulnerabilities. This redundant approach works well in a controlled environment with powerful servers and appliances to run security software. Endpoints however, have limited processing power, are used frequently outside of the protected network environment, and most often contain sensitive work-related information. These new realities are prompting security experts to focus their attention towards the next frontier of enterprise security—the endpoint.

Endpoint Security Challenges and Vulnerabilities

In the modern business environment, endpoints of primary concern are the laptop and desktop PCs used by workers to access corporate networks and information. Recently, several overarching trends have conspired to raise the profile of vulnerabilities at the endpoint:

- In order to bypass established perimeter security measures, criminals are focusing more intelligent and coordinated attacks on endpoint computers. For example; users are being redirected to malicious Web sites that, without user interaction, install malicious software such as keyloggers used to harvest information, and trojans used to take control of computers for use in botnets or to access corporate networks.
- Large numbers of endpoints are now mobile - dramatically increasing data and device exposure outside of protected network environments. For example, notebooks now represent more than half of overall PC shipments worldwide[1], and that number continues to grow.
- Endpoints present a complex logistical challenge to IT staff, who must manage multiple security policies for multiple endpoint agents which have been installed on hundreds or even thousands of PCs. Deploying security software, installing updates and signature files, and maintaining consistent policies and configurations are time-consuming tasks which are difficult to do on a manual basis.
- Vulnerabilities in common networking protocols allow access to open or uncontrolled ports - make endpoints susceptible to a variety of new attack vectors. Some exploits focus on programming errors related to the sizing of software data buffers, whose overflow can corrupt the stack or heap areas of memory, allowing insertion and execution of malicious code.
- Thousands of corporate laptops are now lost and stolen around the globe every week. Many of these PCs contain critical data and information with no protection such as authentication or data encryption.

A New Strategy: Unifying Endpoint and Network Security

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

[1] Source: 451 Group

Enterprises have typically deployed single-function point solutions for endpoint security - such as a personal firewall or antivirus software. However, each time a software update is available for endpoint agents, engineering must complete a rigorous test cycle to qualify the release for compatibility with all other endpoint agents. Since it is not uncommon for organizations to have hundreds or thousands of endpoint PCs under management and deploy three or more security agents to each PC, this approach can quickly overwhelm IT departments.

A new strategy is to unify endpoint security functionality into a single agent that can perform all endpoint security tasks. With a unified agent approach, IT only has to test one agent prior to deployment, and has the assurance that each function within that agent is compatible. Users benefit from greater transparency, as well as the ability to view security settings from a single client interface. This single agent can then be unified with network security technologies, enabling remote deployment and installation of agents, as well as centralized management of network and endpoint security policies from a central administration console.

Unification of endpoint and network security technology allows for simplified deployment and management which can lower overall cost of operations. In order to achieve complete endpoint security with minimal impact on workflow and IT departments, a business must carefully consider threat protections and management capabilities included with a particular solution. Only a complete set of security controls with centralized management can deliver comprehensive and efficient endpoint security.

Requirements for a Complete Endpoint Security Solution

At minimum, a unified endpoint security solution should include the following features and attributes:

1. Detect and block malware
2. Secure information stored on endpoints
3. Enforce policy compliance
4. Provide secure remote access to networks
5. Centralized management
6. Transparent end-user experience
7. Scalability and availability

1. Detect and block malware

Detection and blocking of malware on endpoints has traditionally been accomplished by deploying separate point products for firewall, antivirus, and antispyware. Each of these security applications provides vital and unique functionality.

A newer and often overlooked area of vulnerability is the Web browser. Phishing and Web-based malware attacks such as drive-by downloads, cross-site scripting attacks and malicious browser plug-ins and add-ons have been increasing steadily in frequency

and virulence. A comprehensive endpoint security solution should be able to protect endpoints against these Web-based exploits.
A firewall with program control is important because it provides core manipulation of inbound and outbound traffic. Only a firewall with program control can block unwanted malicious code, control which applications are allowed to access the network, and make endpoints appear invisible to hackers. As a matter of product heritage, some endpoint security suites are built around antivirus functionality, but the firewall is best suited as the first line of defense due to its ability to control traffic.

Antivirus applications 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 as well as detection and removal of spyware that was previously installed.

2. Secure information stored on endpoints
Securing information stored on endpoints is critical since endpoint devices, such as laptop PCs, are frequently lost or stolen. Also of concern are removable storage devices such as USB flash drives, CDs and DVDs which can also store large amounts of information. Once a device 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 with pre-boot authentication, removable 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 or password to decrypt the data and render it readable again. Support for multi-factor authentication options, such as smart cards and tokens, can provide an additional level of security. In the past, encryption has been cumbersome to execute on endpoints and has impacted system performance. Newer encryption solutions have solved these issues and have been deployed globally on millions of endpoints without incident.

Port/ device control allows enterprises to centrally manage the use of individual ports on an endpoint. One practical benefit is the ability to block unauthorized transfers of protected data from an endpoint to a removable storage device such as a USB flash drive. Additionally, some solutions allow enforced encryption of any data transferred to an authorized removable storage device.

3. Enforce policy compliance
Scanning an endpoint for viruses and security policy compliance prior to granting network access ensures that an endpoint won’t infect corporate networks and servers. At a basic level, this requires verification of up-to-date security policies and enforcement

rules. For example, compliance may require each endpoint to have the most current version of antivirus software, critical patches and latest applications; or assurance that the endpoint is not running prohibited programs. Failing a policy check can 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 non-compliant endpoints.

On-demand compliance can enforce security policy on unmanaged endpoints – i.e. no client software is required on the endpoint. On-demand compliance detects and disables spyware on endpoints and ensures session confidentiality. For 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 must be able to ensure that these machines are safe before allowing access to the corporate network. IT also must to ensure session confidentiality to ensure that nothing is left on the host computer after an employee terminates a remote access session.

More advanced solutions can scan removable storage media for viruses or malicious file types before granting access. Some solutions even have granular management controls that can be configured to block or allow removable storage devices according to brand, model, memory size, or device ID.

4. Provide secure remote access to networks

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 establishing a secure, encrypted communication tunnel that prevents 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 are ‘in the office’ when connecting remotely.

Advanced solutions provide roaming, location awareness and auto-connect features for an even more transparent end-user experience. In addition to username and password requirements, support for multi-factor authentication options - such as SecurID tokens, RADIUS, TACACS, and biometrics - can provide additional levels of security.

5. Centralized management

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

The ‘Holy Grail’ of endpoint security is to provide central management of all security functionality and endpoints - including configuration, deployment, client and policy updates, password recovery, reporting and deactivation - from a single central console. Some vendors have taken steps towards consolidating and streamlining management solutions, however, enterprises should strongly consider endpoint security solutions including:

- Centralized management with the ability to segregate and delegate authority
- Central monitoring and reporting on every endpoint security control
- Faster security incident discovery, monitoring, and forensics
- Support for directory services such as Active Directory to leverage existing user information and enable rapid configuration and policy deployment
- Comprehensive reporting and support for audits and compliance
- Fast and easy deployment of software agents without requiring on-site manual intervention from IT administrators or end-users
- Unification of endpoint and network security event management

6. Transparent end-user experience

An endpoint security solution should only interrupt end-user workflow when necessary, such as for security warnings, and remain transparent otherwise. Many endpoint security suites require loading three, four or even more agent software modules onto each PC. As a result, security applications begin to swamp memory capacity and consume too many CPU cycles - slowing performance of business-critical applications. Annoyance from end-users grows when they are expected to manually process updates to security software, patches, and other system maintenance. Very few endpoint security agents achieve the goals of easier management, better performance and less user intervention.

The ideal is to have all endpoint security functionality contained in a single, small-footprint agent. End-users benefit from greater transparency and fewer interruptions, while IT administrators and managers enjoy easier system maintenance and receive fewer support calls. Single logon capabilities, while not desirable in all scenarios, can provide additional transparency for end-users by safely storing logon credentials to enable one-time-logon to pre-boot authentication, operating system, remote access VPN and encrypted media.

7. Scalability and availability

An endpoint security solution should be able to grow with an organization, from infancy through to maturity. Manually uninstalling and reinstalling endpoint agents and management servers can disrupt normal business and result in unforeseen costs and demands on critical IT resources. The option to easily scale to hundreds, thousands, or even hundreds of thousands of seats can be a huge advantage for a business on a fast growth curve.

Support for multiple languages is another important consideration as it can allow an organization to expand or relocate internationally.

Check Point Endpoint Security

Check Point Endpoint Security offers enterprises a complete set of endpoint protections, deployed through a single, centrally managed agent. Endpoint security functions are combined and unified with network security, enabling easy centralized configuration and deployment with central policy enforcement.

Unified Functions of Check Point Endpoint Security

Function	Description
Desktop Firewall	Based on 16 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.
Browser Virtualization	Browser virtualization protects endpoints from drive-by downloads and zero-day Web-based threats. Check Point WebCheck utilizes a powerful yet lightweight browser virtualization engine that surrounds the Web browser in a ‘bubble of security’ while a user surfs the Web. Check Point WebCheck also contains advanced anti-phishing and data protection functionality to protect endpoints and critical information against online scams and targeted attacks.

Full Disk Encryption	Check Point Full Disk Encryption leverages market-leading Pointsec® technology, offering an easy-to-deploy combination of strong full disk encryption and multi-factor pre-boot authentication. All information on the hard drive is protected - including data, operating system and system files - while remaining transparent to end-users.
Media Encryption and Port Control	Check Point Media encryption provides strong and enforceable encryption for all policy-approved removable media used in an 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 including data security and remote access in a single unified agent. Our new Endpoint Connect VPN client provides auto-connect, location awareness, and roaming capabilities for seamless and secure connectivity with corporate networks while traveling or working remotely. Functionality is fully integrated, sharing the same user interface and system tray icon with other endpoint security functions.
Logon Control	Check Point OneCheck safely stores user logon credentials, allowing one-time-logon to Full Disk Encryption pre-boot authentication, Windows operating system, remote access VPN and removable media protected by Check Point Media Encryption.
Centralized Management	Centralized management provides administrators with powerful tools to customize endpoint security policies for users, groups, or specific needs within the organization. Administrators 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 operate 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, minimizing administration time, cost and complexity— while maximizing security.

Conclusions/ Learn More

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 organization. Check Point Endpoint Security unifies the highest-rated firewall, network access control (NAC), program control, antivirus, anti-spyware, data security, Web protections and remote access VPN into a single, centrally managed agent - eliminating the need to manage multiple endpoint security agents while dramatically reducing endpoint security administration overhead.

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

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

Corporate headquarters
1-800-429-4391