Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Endpoint Policy Enforcement

Assuring Total Access Protection for the Enterprise

In This Document

INTERNAL WEB PERIMETER

Intelligent Security

Check Point SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Introduction

The distinction between theoretical and real information security has become increasingly clear over the past several years. Common security technologies that enterprises once relied on to safeguard their data and networks — as well as their business continuity and reputation — no longer deliver all their promised protections. A new approach is needed to address the factors that have caused this loss of effectiveness.

- In the past, security administrators could count on properly configured perimeter firewalls to filter external attacks on corporate networks. Today, employee and guest remote access, instant messaging, port 80 traffic, and other forms of communication have made effective perimeter security much more challenging to achieve.
- A few years ago, antivirus products were generally effective at protecting enterprises from virus outbreaks. There were fewer exploits, and they typically took a number of days or weeks to reach mass distribution. Because IT departments had enough lead time, they could usually deploy updated virus signatures before an attack could infect many of their PCs or degrade network performance. In contrast, the latest worms and viruses can propagate to every vulnerable host on the Internet in minutes. They can compromise millions of systems and take down corporate networks before antivirus signature updates are deployed to every desktop and mobile computer in an enterprise.

Common security technologies that enterprises once relied on to safeguard their data and networks — as well as their business continuity and reputation — no longer deliver all their promised protections.

- The weekly discovery of new application and operating system vulnerabilities has made patching impractical as a proactive security practice. Administrators have found that choosing the right subset of patches to apply, testing them for stability and compatibility in their environments and deploying them to both internal and remote computers takes longer than it takes hackers to exploit newly discovered vulnerabilities.
- Many enterprises lack the skilled staff needed to analyze the overwhelming volume of network Intrusion Detection System (IDS) alerts and “false positive” alarms. Adding IDS logs from hundreds or thousands of network computers or “endpoints” only amplifies the problem. Most importantly, the inherent reactive nature of IDS technology renders it powerless to prevent the damage caused by today’s lightning fast attacks.

INTERNAL WEB PERIMETER

Intelligent Security

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

- Endpoint firewalls and antivirus products have become targets of today's sophisticated exploits. These essential protections can be rendered ineffective if they can be disabled by hackers. End users can also evade enterprise security policy restrictions if they can figure out how to disable desktop security technologies.
- Network guests – including contractors, business partners, customers, and even employees using home PCs – are routinely given remote access to enterprises' Web-based applications and portals. IT and security administrators have little, if any, control over the security posture of these guest endpoints. As a result, it's become common for administrators to identify a compromised guest PC as the source of a network infection or information leak.

A Realistic Solution

Restoring the effectiveness of the security infrastructure requires a solution that addresses the new realities of enterprise risk. To minimize so-called "Day Zero" exploitation of new vulnerabilities, the solution must protect networked computers proactively rather than reactively. It must contain or stop threats and exploits immediately — preferably by default or with minimal configuration — rather than wait for signature or heuristic updates to be effective. It must also reduce the exposure of the enterprise network to attack via any inadequately protected entry point. To do this, it must ensure that every computer that connects to the network is in a secure state, as defined by IT security policy. This policy could require that every endpoint be running a host-based firewall and an antivirus product with up-to-date signatures before it is granted a connection to the LAN. It might also require that a critical Windows patch and an updated VPN client be installed prior to network access. The solution must be hardened to the extent that it cannot be tampered with or disabled by either hackers or end users. Last but not least, the solution should secure network access across the entire heterogeneous enterprise network, regardless of the brands of networking products or operating systems in place. A solution that met all these criteria could have saved countless organizations from the very costly damage caused by MS-Blaster, Welchia/Nachi, SoBig.F, MyDoom, Sasser, Netsky, Witty, and many other recent exploits.

Integrity™ is such a solution. It secures networked PCs with the most trusted protection available today. By ensuring policy compliance on all PCs that access the network – employee and guest, remote and internal, wired and wireless – Integrity provides Total Access Protection for the enterprise. Cooperative Enforcement™ technology enables Integrity to integrate with hundreds of network gateway products — from VPNs to switches to wireless access points — in order to ensure that non-compliant PCs are quarantined and brought back into compliance before they're allowed access to network resources. The solution ensures policy compliance in any IP-based network environment, regardless of the vendors and products the enterprise has chosen for its network infrastructure. Integrity also features Total Client Lockdown, which prevents any user or attacker from disabling endpoint security or enforcement of network access policy. The ability to deliver comprehensive, assured security and policy compliance enterprise-wide enables Integrity to defeat the threats that evade other security and network access products.

Cooperative Enforcement of Remote Access Security

Safe remote access was the initial goal of Cooperative Enforcement. The Zone Labs division of Check Point worked with all the leading VPN and remote connectivity vendors to integrate their IPSec and SSL products and services with Integrity in order to enforce a secure state on every PC granted network access. These Cooperative Enforcement integrations require that an Integrity client be running on a remote PC, both before the PC is granted access to an enterprise network and throughout a remote access session. They also check the security posture of the PC and enforce compliance with a broad range of security policy elements prior to granting network

INTERNAL WEB PERIMETER
Intelligent Security

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

access. Integrity can require that an endpoint have running and up-to-date anti-virus protection from any desired vendor. It can require that a particular service pack or software patch be installed, it can ensure that any specified process is running or not running, and it can require that any specified registry keys are present or not present.

End users whose PCs are out of compliance with any aspect of the required policy are denied access to the enterprise network. Instead, they are automatically redirected to servers that provide self-service remediation resources. Once end users take the simple steps needed to comply with security policy, Integrity and the network gateway automatically restore the users' authorized access privileges. Integrating Integrity with network gateways assures a secure state on every PC that accesses the network, and it avoids the additional points of failure that plague non-integrated approaches to enforcing enterprise policy.

Enforcement of LAN Access Security

The next phase of Cooperative Enforcement had two objectives. The first was to advance beyond integrations with individual products to integration based on a widely adopted open standard. The second goal was to extend policy enforcement inside the perimeter to both wired and wireless LANs. With its groundbreaking support for the Extensible Authentication Protocol (EAP), which is

INTERNAL WEB PERIMETER
Intelligent Security

part of the IEEE 802.1X standard supported by hundreds of products, Check Point's Zone Labs division was able to achieve both goals. Integrity and products from Cisco, Nortel, Microsoft, and many other leading enterprise switch, router, and wireless access point vendors now support EAP-based integration. As a result, Integrity can deliver Cooperative Enforcement for wired and wireless LAN connections with little custom configuration required. By integrating with any product that supports non-proprietary 802.1X specifications, Check Point's Zone Labs division also ensures that Cooperative Enforcement will work with equipment from virtually any networking vendor an enterprise chooses.

Integrity cooperates with internal EAP-enabled gateways to enforce security policy similarly to the way it works with VPN gateways. Integrity checks the security posture of each endpoint to assess compliance with each policy element. It then communicates the result to the EAP-enabled switch, router, or wireless access point. The gateway grants endpoints access to the LAN if they're deemed policy-compliant by Integrity, or quarantines them if they're not. When Integrity confirms that an endpoint has returned to compliance it informs the gateway, which restores the endpoint's access to the LAN.

Direct integration with network gateways provides the best assurance that enterprise policy will always be enforced. If an enterprise network is not yet fully 802.1X enabled, however, Integrity can enforce comprehensive policy compliance on its own, without gateway integration. It does this by applying endpoint firewall rules that allow a user access only to a limited set of network resources when it detects a non-compliant state. As with Cooperative Enforcement, Integrity-only enforcement provides remediation resources that help users get back in compliance quickly and easily. Once the user's endpoint is policy compliant, Integrity automatically restores the user's normal network access privileges. In this standalone configuration there is no gateway ensuring that an Integrity client is running on the endpoint. The Total Client Lockdown capability in Integrity is what gives administrators confidence that every Integrity client they have installed is always running and enforcing both endpoint security and policy compliance.

The Cooperative Enforcement options available to enterprises are increasing as Check Point integrates Integrity with its full line of perimeter, internal, and Web security products. For example, Integrity will soon enforce network access policy in cooperation with InterSpect, Check Point's innovative internal security gateway. InterSpect blocks the spread of new worms and attacks across LANs, segmenting networks into security zones and quarantining compromised devices. Integration with Integrity will allow InterSpect to ensure that every internal PC is secure before it can communicate with the rest of the LAN.

Controlling Remote Access by Guest Endpoints

Until recently, endpoint policy enforcement always involved installing client software on PCs. Client-based security provides the most comprehensive protection for vulnerable endpoints, but in most cases an enterprise is unable to install client software on guest computers that access its network. Network guests such as business partners, customers, and even employees using home PCs are increasingly allowed to connect to an enterprise's web-based portals, applications, and data. If their PCs have been compromised by keystroke loggers or other types of spyware, however, they can cause the same types of security breaches as unprotected enterprise assets. Guest PCs can also cause infections and confidentiality breaches if their antivirus is not up to date, if they lack critical patches, or if they fail to meet the other criteria that define a secure endpoint state.

Integrity Clientless Security was developed to close this security hole. Because the product does not require IT to install client software, it lets enterprises extend network access protection to user

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

populations that were once beyond their control. When external users go to the log-in page for a protected web portal or application – such as enterprise webmail, an e-commerce system, or an SSL VPN gateway – an Integrity Clientless Security browser plug-in scans their PCs for keystroke loggers, spyware, and other undesirable programs. If it finds any spyware processes, Integrity Clientless Security immediately disables them. Administrators can also choose to prevent access to the web portal or application until other screened software is removed by the user. Disabling keystroke loggers before users type in their log-in IDs and passwords prevents an intruder from capturing credentials that would enable unauthorized access to sensitive data and critical network resources.

In addition to disabling spyware and facilitating its removal, Integrity Clientless Security offers enterprises the ability to enforce the same network access rules enforced by the client-based version of Integrity. The clientless solution can require up-to-date antivirus, patches, applications, registry keys, and other criteria before it gives the guest access to the log-in screen. Administrators can also configure the solution to provide remediation resources that make it easy for users to get their endpoints in compliance with security policy.

By adding the ability to enforce security policy on non-IT controlled as well as enterprise owned endpoints, Check Point has delivered the Total Access Protection that organizations need to defend themselves against today's real world threats.

The Cooperative Enforcement Advantage

Total Access Protection

An industry first, Total Access Protection extends endpoint security to all PCs – employee and guest, internal and remote, wired and wireless - that connect to the enterprise network. By providing market leading security and enforcing policy compliance on every endpoint, Total Access Protection dramatically mitigates the risks from worms, spyware, and other threats to business continuity and data confidentiality.

Broad Gateway Integration

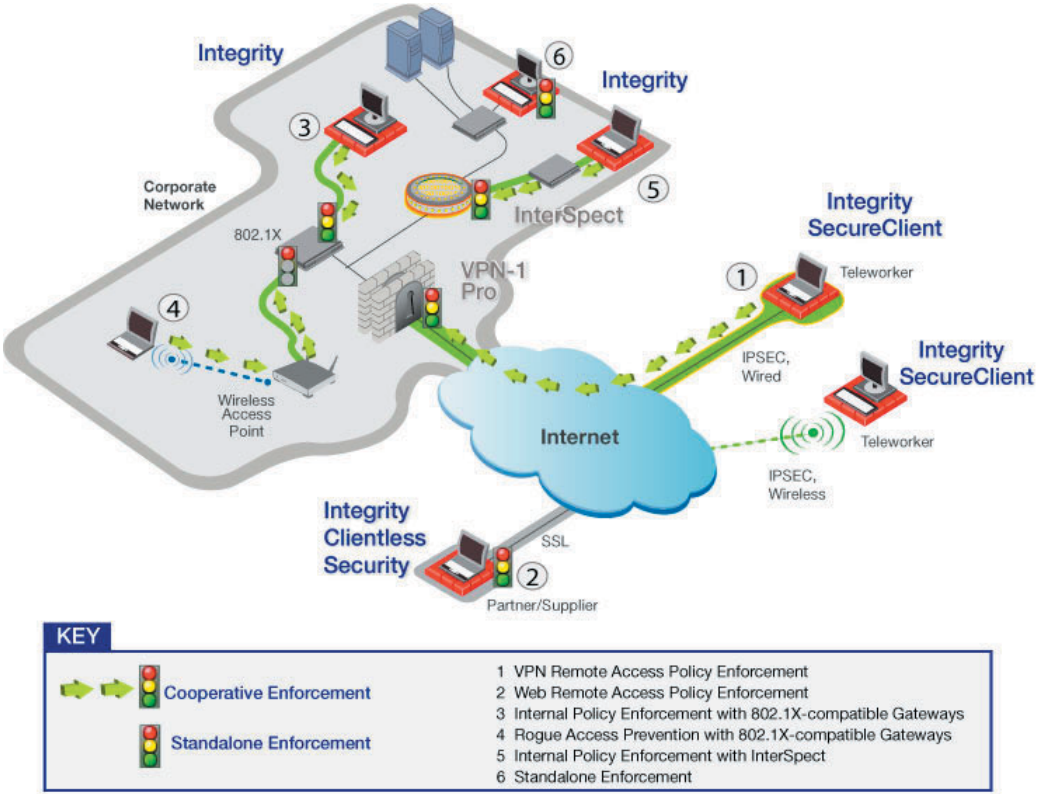
Integrity assures comprehensive endpoint policy compliance by cooperating with network gateways from more than 20 leading vendors. Cooperative Enforcement technology enables Integrity to verify the security posture of an endpoint and control network access via most leading VPNs and over 200 switches, routers, and wireless access points. Integrity was the first endpoint security product to support non-proprietary Extensible Authentication Protocol (EAP), a key component of the widely adopted 802.1x standard, in order to secure network access in the widest range of environments.

Total Client Lockdown

All network access control can be lost if security client software can be altered or disabled. In environments where older internal gateways aren't able to quarantine out-of-compliance endpoints, administrators must rely on the security client to enforce compliance on its own. The advanced self-protection mechanisms built into Integrity ensure that it cannot be tampered with or disabled by either attackers or end users. The result is a solution that can secure network access in virtually any environment, regardless of the gateways in use.

INTERNAL WEB PERIMETER
Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.



The Future of Network Access Policy Enforcement

The proliferation of enterprise communication channels and always-connected computing devices is multiplying both business opportunities and security risks. Check Point and its Zone Labs division have a long track record of delivering proactive security innovations that keep enterprises one step ahead of continually evolving threats. Looking forward, Check Point is committed to ensuring that any host connected to enterprise computing resources by any means will be secure and compliant with enterprise policy. This assurance extends across user populations, device types, platforms, and networking environments. Announced approaches to network access control that fail to provide this flexibility – such as those that support only a single vendor's networking equipment or operating system – serve the interests of the supplier rather than those of the customer. Proprietary implementations of industry standards such as 802.1X have the same ulterior motive. Most enterprises will want to avoid the vendor lock-in and higher TCO that such implementations will entail.

In addition to enabling open, comprehensive policy enforcement in any environment, Check Point is committed to minimizing the administrative effort needed to deploy and manage its endpoint security solutions. The combination of standards-based technology and ease of administration results in the lowest possible TCO, both for endpoint security and IT infrastructure in general. By delivering these security and financial benefits, Check Point will continue to assure the best endpoint protection for the enterprise at all times.

INTERNAL WEB PERIMETER
Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

About Check Point Software Technologies

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's Zone Labs (www.zonelabs.com) division is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of 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 over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,300 Check Point partners in 92 countries.

CHECK POINT OFFICES:

International Headquarters:
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: 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**

June XX, 2004 PN: 000000

INTERNAL WEB PERIMETER
Intelligent Security