

Zone Labs Integrity

Enterprise Endpoint
Security

// Trusted Zone //

Real World Security with Cooperative Enforcement

A White Paper Presented
by Zone Labs



A Check Point Company

Zone Labs

Integrity

Enterprise Endpoint
Security

White Paper

Page
2

// Trusted Zone //

Executive Summary

The distinction between theoretical and real information security has become increasingly clear over the past several years. Common security technologies that enterprises rely on to safeguard their data and networks – as well as their business continuity and reputation – no longer deliver all their promised protections. Specifically:

- In the past, security administrators could count on properly configured perimeter firewalls to filter and block external attacks on corporate networks. Today, employee remote access, Instant Messaging (IM), port 80 traffic, and other forms of communication have made the perimeter so porous that the basic concept of a network perimeter is now questionable.
- A few years ago, anti-virus products were generally effective at protecting enterprises from virus outbreaks that typically took a number of days or weeks to reach mass distribution. IT departments often had enough time to 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 node on the Internet in minutes, compromise millions of systems, and take down corporate networks before anti-virus signature updates are even available, much less deployed to all of an enterprise's desktop and mobile computers.
- 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 internal and remote computers takes far 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 Systems (IDS) alerts and "false positive" alarms. Adding IDS logs from hundreds or thousands of network computers

The Cooperative Enforcement Advantage

Total Access Protection: An industry first, Total Access Protection extends endpoint security across all PC's that connect to the enterprise, including employees and guest PCs, remote and internal PCs, and wired and wireless PCs. By providing best-of-breed, policy-enforced security on each endpoint, Total Access Protection dramatically mitigates the risks of worms, spyware, and other threats to business continuity and network integrity.

Broad Gateway Integration: Through Cooperative Enforcement, Zone Labs provides comprehensive policy enforcement in conjunction with network access devices from Check Point Software Technologies, Cisco Systems, Nortel, and more than 20 other leading vendors. Cooperative Enforcement technology verifies endpoint security and policy compliance as a condition of network access through an enterprise's VPN. It also ensures that the endpoint is protected throughout the network session. Zone Labs is the first vendor to support the Extensible Authentication Protocol (EAP), part of the 802.1x industry standard, which enables Integrity to integrate with over 200 network access devices – including many switches and wireless access points.

Total Client Lockdown: If an endpoint security client can be disabled by an end user or a hacker, all policy enforcement benefits can be lost. To alleviate this potential problem, administrators can "lock down" all Integrity clients providing security that cannot be altered or disabled, even by end users with local administrative privileges on the endpoint.

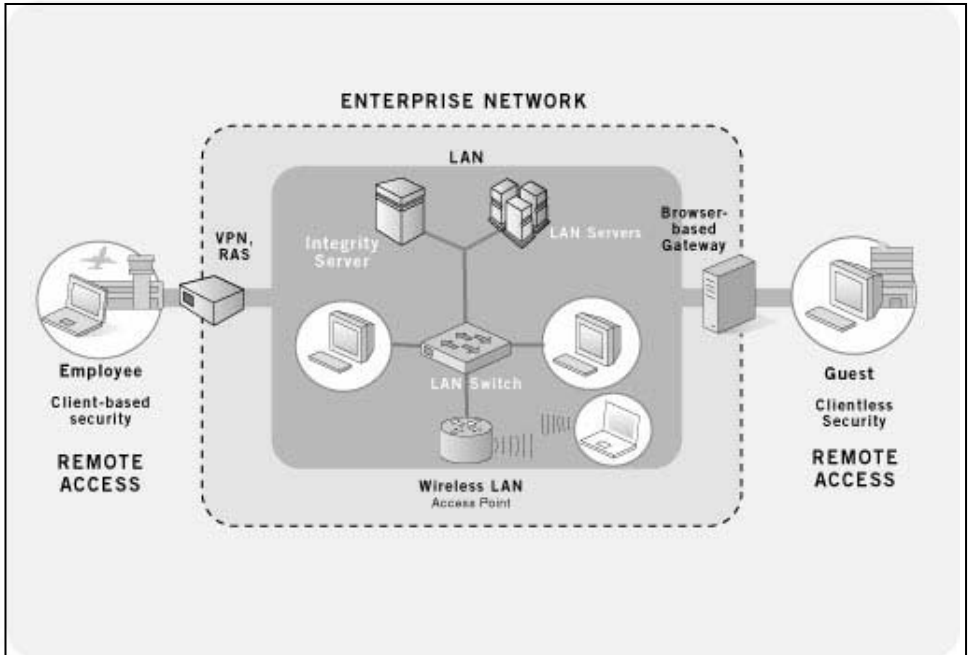
Common security technologies that enterprises rely on to safeguard their data and networks – as well as their business continuity and reputation – no longer deliver all their promised protections.

Zone Labs Integrity



or “endpoints” only amplifies the problem. Most importantly, the inherent reactive nature of IDS technology renders it powerless to prevent the damage from today’s lightning fast attacks.

- ▶ Even the best desktop firewalls and anti-virus are the target of attackers, which mitigate many shortcomings of other security technologies, can be rendered ineffective if they can be disabled by end users or hackers.
- ▶ Network guests – including contractors, business partners, customers, and even employees using home PC’s – 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.



Unprotected endpoints are exposed to worms, spyware, and other threats to the enterprise network.

Restoring the effectiveness of security infrastructures requires a solution that addresses today’s sources of enterprise risk:

$$\text{Risk} = \text{Vulnerabilities} \times \text{Exposure}$$

To minimize so-called “Day Zero” exploitation of new vulnerabilities, the solution must protect networked computers proactively. It must contain or stop attacks and exploits immediately – preferably by default or with minimal configuration – rather than wait for signature updates to be effective. In addition, the solution must reduce the exposure of the enterprise network to attack via any inadequately protected entry points. To do this, it

Zone Labs offers a solution that proactively secures network endpoints and enforces policy as a condition of network access: Zone Labs Integrity with Cooperative Enforcement technology.

must ensure that IT security policy is enforced on every computer that connects to the network. The policy enforced by the solution, for example, could require that the endpoint be running a host-based firewall and an anti-virus product with up-to-

Zone Labs Integrity

Enterprise Endpoint
Security

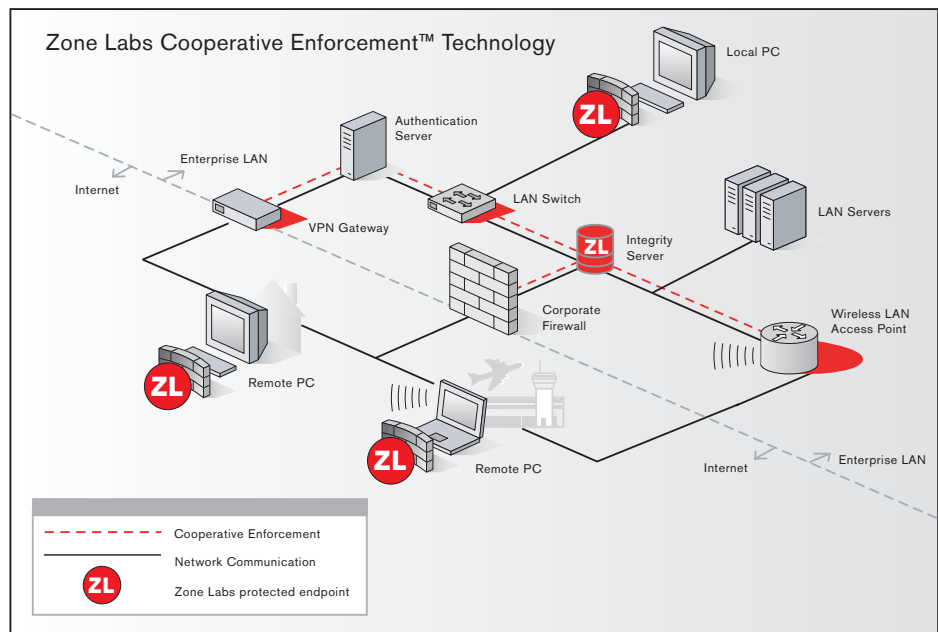
White Paper

Page
4

// Trusted Zone //

date signatures before it is granted a connection to the LAN. It might also enforce the installation of a critical Windows patch and an updated VPN client as conditions of network access. Last but certainly not least, the solution must also be hardened so that it cannot be tampered with or disabled by either hackers or end users. The solution's ability to enforce pro-active security policies would have saved countless organizations from the very costly damage caused by exploits such as MS-Blaster, Welchia/Nachi, SoBig.F, and MyDoom.

Zone Labs® Integrity™ is such a solution. It secures networked PCs with the most trusted protection available today. By ensuring policy compliance on the full spectrum of PCs that access the network – employee and guests, 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 – to ensure that non-compliant PCs are quarantined and brought back into compliance before they're allowed access to network resources. Integrity also features Total Client Lockdown, which prevents even users or hackers with local administrative privileges on a PC from disabling endpoint security and policy enforcement. The combination of comprehensive and assured security and policy enforcement provides real world reduction of the risks that other security products fail to mitigate.



Integrity checks each endpoint for compliance with all policy elements including anti-virus updates, patches, and registry keys. Out of compliant endpoints are quarantined until remediation takes place.

Cooperative Enforcement of Remote Access Security

Safe remote access was the initial goal of Cooperative Enforcement. Zone Labs worked with leading VPN and remote connectivity vendors – including Check Point, Cisco, Nortel, Avenail, Neoteris, NetScaler, and iPass – to integrate their IPSec and SSL products and services with Integrity in order to enforce remote access security policy. 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. Zone Labs and its partners used proprietary APIs to integrate their respective products, and each vendor certified the joint solution.

Zone Labs

Integrity

Enterprise Endpoint
Security

White Paper

Page
5

// Trusted Zone //

In the second phase of development, Zone Labs extended the scope of its policy enforcement capabilities to include the ability to check for and enforce compliance with a broad range of security policy elements. Integrity can now require that an endpoint have running and up-to-date anti-virus protection from any desired vendor. The solution can require that a particular service pack or software patch be installed, it can ensure that any specified application 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 a server that provides self-service remediation resources. Once end users take the simple steps needed to comply with security policy, Integrity and the network gateway automatically restore their enterprise access. Integrating Integrity with network gateways delivers assured policy enforcement, and avoids additional points of failure that plague non-integrated approaches to enforcing enterprise policy.

Enforcement of Wired & Wireless LAN Security Policy

Zone Labs had two objectives for the next phase of policy enforcement. The first was to advance beyond custom integrations with individual partners 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. Zone Labs groundbreaking support of the Extensible Authentication Protocol (EAP), which is part of the IEEE 802.1x standard supported by hundreds of products, allows Zone Labs to achieve both goals. Integrity and products from Microsoft, Cisco, Nortel, and many other leading enterprise switch 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 integration effort. By integrating with any product that supports non-proprietary 802.1x specifications, Zone Labs also ensures that Cooperative Enforcement will work with equipment from virtually any networking vendor an enterprise chooses. Network access control based on a proprietary implementation of 802.1x may be in a vendor's best interest, but most enterprises will want to avoid the vendor lock-in that such an implementation entails.

Integrity cooperates with switches, wireless access points, and other EAP-enabled gateways to enforce security policy similarly to the way it integrates with VPN gateways. Integrity checks each endpoint for compliance with all policy elements and communicates the result to the EAP-enabled switch 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. Many enterprise networks are not yet fully 802.1x enabled, however. In these cases, 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-compliance 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 configuration no gateway ensures that an Integrity client is running on the endpoint. Integrity's Total Client Lockdown capability is what gives administrators confidence that both endpoint security and policy compliance are always enforced.

Controlling Remote Access by Guest Endpoints

Until recently, endpoint policy enforcement always involved installing Integrity 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, they can cause the same types of security breaches as unprotected enterprise assets.

Zone Labs developed Integrity Clientless Security 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 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 an extranet, an on-line financial system, or an SSL VPN gateway – they are asked to accept the Integrity Clientless Security browser plug-in. The plug-in then scans their PCs for keystroke loggers, spyware, and other undesirable programs. If it finds any software that violates enterprise policy, Integrity Clientless Security can prevent access to the Web portal or application until that software is removed. Integrity Clientless Security guides users through the removal process and lets them log in immediately once their endpoints are policy-compliant.

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

The Future of Policy Enforcement

As enterprise perimeters dissolve and always-connected computing devices proliferate, business opportunities and security risks will multiply. Zone Labs 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 will extend across user populations, device types, platforms, and networking environments. It will be delivered in a way that minimizes administrative effort and makes it as easy as possible to return endpoints to policy compliance. By achieving these objectives, Zone Labs will continue to assure the best endpoint protection for the enterprise at all times. Zone Labs history of innovation means proactive protection against vulnerabilities before exploits can even occur.

Zone Labs Integrity

Enterprise Endpoint
Security

White Paper

Page
7

// Trusted Zone //

Zone Labs Integrity

// Trusted Zone //

Enterprise Endpoint
Security

White Paper

Page
8

To learn more about assured enterprise-wide security compliance with Zone Labs Integrity and Cooperative Enforcement technology, please contact a Zone Labs representative at 1-877-876-4960 (option 1).

About Zone Labs, Inc.

Zone Labs, Inc. is a leading creator of endpoint security solutions that millions of customers trust to protect their PCs from the risk posed by hackers and data theft. Zone Labs' proven technology is deployed by global enterprises, service providers, small business and consumers.

US Headquarters

Zone Labs, Inc.
475 Brannan Street
Suite 300
San Francisco, CA 94107
tel 415.633.4500
fax 415.633.4501

European Headquarters

Zone Labs, GmbH
Frankfurter Str. 181 a
63263 Neu-Isenburg,
Germany
tel +49.6102.36689.0
fax +49.6102.36689.99

www.zonelabs.com

© 2004 Zone Labs. All rights reserved. IMsecure, TrueVector, ZoneAlarm and Zone Labs are registered trademarks of Zone Labs. The Zone Labs logo, Zone Labs Integrity and Cooperative Enforcement are trademarks of Zone Labs L.L.C. Zone Labs Integrity protected under U.S. Patent No. 5,987,611. Reg. U.S. Pat. & TM Off. Check Point is a trademark of Check Point Software Technologies Ltd. All other trademarks are the property of their respective owners. v.06.18.04



A Check Point Company

