Zone Labs
Integrity

Enterprise Endpoint
Security

// Trusted Zone //

New Threats, New Solutions: Enterprise Endpoint Security

A White Paper Presented
by Zone Labs

ZONE LABS™
A Check Point Company

“Only the paranoid survive.”

-Andy Grove, Intel Corporation

Executive Summary

In the rapidly evolving world of network security, there’s a thin line between paranoia and prudent protection. Hackers are growing in both number and sophistication, and the stakes are rising every day. New technologies have triggered a shift in the network security paradigm, expanding vulnerability exponentially. Distributed personal firewalls are needed to protect corporate networks from Internet-enabled espionage, sabotage, and vandalism. Each individual PC-local and remote-must employ security technology to prevent known and unknown attacks. Real-world security needs to be flexible and make intelligent use of Policy Lifecycle Management℠ to balance protection with productivity.

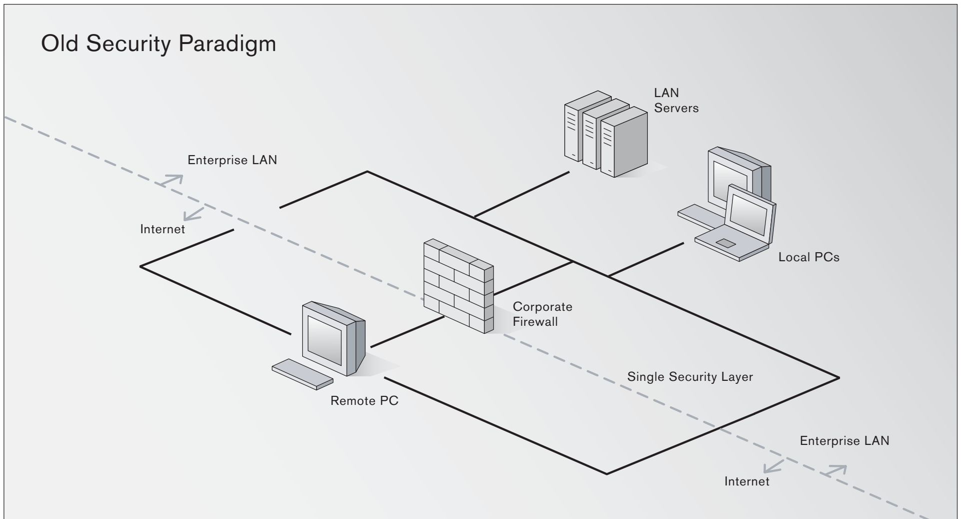
Zone Labs Integrity™ is a distributed endpoint security solution that enables central management of PC security and enforces security policy across the enterprise, protecting corporate data, productivity, and reputation. Integrity offers enterprise-class scalability, proven multi-layered security, and centralized security management. Unique Policy Lifecycle Management tools facilitate security that is continuously optimized for the needs of the organization. Integrity leverages existing IT investments for shorter implementation cycles and better lifetime return on investment.

Real-world security needs to be flexible and make intelligent use of Policy Lifecycle Management to balance protection with productivity.

Enterprise Networks at Risk

As networks become larger, more complex, and more distributed, corporations face a growing vulnerability to hacker attacks and industrial espionage. Security consciousness and security spending are both on the increase, but not at a sufficient pace to stay ahead of the growing threat. The DefCon Internet Security site estimates that “By 2002, approximately 19 million people will have the skills to mount a cyber attack.” According to the latest CSI/FBI survey, a new generation of profit-motivated hackers is raising the stakes for corporate security managers. They are using Trojan horses like Back Orifice, Sub7, and other custom spyware to control remote machines, steal passwords, and compromise corporate networks. Hackers randomly scan for vulnerabilities and deploy viruses to harvest IP addresses and information.

Once inside, hackers can conduct espionage or sabotage, steal financial information, disrupt business, and cause public embarrassment. Even networks with VPN tunnels are at risk. The VPN will secure the data in transit, but leaves the endpoints vulnerable. Data delivered safely can be harvested by Trojans at the exposed endpoints. Whether a hackers goal is vandalism or illicit profit, the costs can be enormous. Computer



With a single security layer of remote access and limited corporate traffic, perimeter defenses provided adequate corporate security.

Economics, an independent research firm, estimated global financial damage from malicious code in 2000 at $17.1 billion. mi2g, a London-based e-commerce research and development company, put the mark even higher, at $20 billion.

New technologies have triggered a paradigm shift in network security. In the old network model, almost all PCs connected to the Internet via a central gateway. Guarding the gateway effectively created a defensive perimeter. This model is no longer adequate.

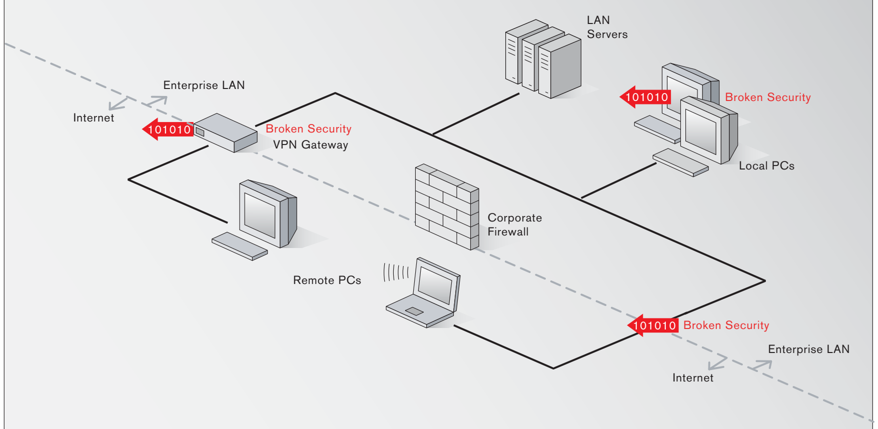
First, while corporate networks shored up their security with centralized firewalls, antivirus and intrusion detection, hackers exposed other vulnerabilities. Second, the explosion of remote and mobile users with always-on, broadband Internet connections to the network means most networks now have hundreds, or even thousands, of vulnerable "back doors."

The Gartner Group notes, "Broadband connections are rife with threats to remote devices. Viruses, Trojan horses, zombies, keystroke monitoring, file shares and denial-of-service attacks all threaten the remote machine and, by extension, put the enterprise's IT resources at risk." Microsoft and others were hacked in this way. Incursions of this sort can quickly turn into high-profile PR disasters, or worse, go undetected for months before being exposed.

Vulnerability has expanded exponentially. As companies go from single gateways to thousands of Internet connected endpoints, the number of vulnerabilities for networks has exploded. IDC reported the number of remote users in the year 2000 at 39 million and growing 9 percent annually. Telechoice estimates there are 5.7 million broadband subscribers, rising to 14.5 million in 2003.

As Companies go from single gateways to thousands of Internet connected endpoints, the number of vulnerabilities for networks has exploded.

New Security Reality



With the introduction of new technologies, hacker tools and ever-multiplying modes of corporate access, perimeter defenses alone are no longer adequate. These new security threats expose the corporate network and putcorporate assets at risk.

This accelerating trend is creating even more back doors. In addition, laptop users physically bypass the firewall every day, and wireless networks have no definable boundaries. Effectively, the network perimeter has disappeared. Hackers have taken notice, and so have government regulators: recent legislation requiring tighter security in the healthcare and financial services industries is a telling sign of the times, and a reminder of how much we all have to lose.

> **"The personal firewall may well become more significant in the long run than the corporate firewall."**
>
> **—Peter Lindstrom, Hurwitz Group**

Centrally-Managed Endpoint Security

Prolific threats require a pervasive solution. To reclaim peace of mind and control of the network perimeter, each endpoint must be secured. Distributed endpoint security, centrally managed personal firewalls, and application control technology offer the best defense against attacks that threaten corporate productivity, data, and reputation. IDC notes, ". . .as 'always-on' Internet access grows (with digital subscriber line [DSL] and cable modems) and as more companies allow telecommuting, the need for distributed and personal firewalls will grow." Consequently, Peter Lindstrom of the Hurwitz Group stated, "The personal firewall may well become more significant in the long run than the corporate firewall." Personal firewalls and application control can also help secure endpoints behind the corporate firewall, by preventing internal hacking, unknown Trojans, and spyware from exposing sensitive data outside the corporation.

Similar to a corporate network, each individual PC – local and remote – must employ multiple approaches to security technology. Only a policy-based, application-oriented distributed firewall, on each and every enterprise PC, can provide the protection needed to stop thousands of new and unknown hacking combinations and techniques.

For true endpoint security, a distributed firewall must incorporate the following functions:

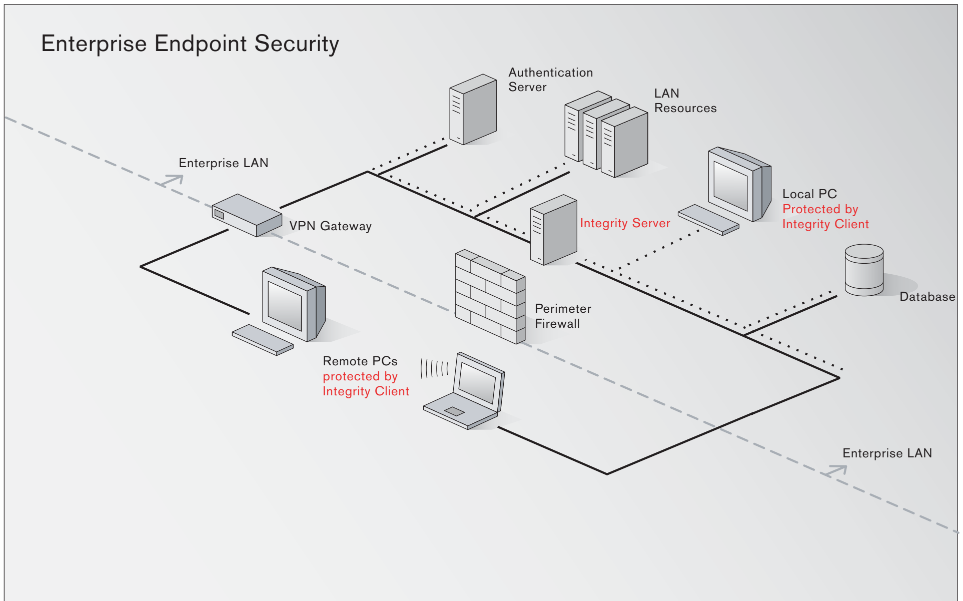
- Obscure PCs to prevent outside access from hackers
- Prevent applications from becoming hacker tools by allowing only authenticated and approved applications to access the Internet
- Secure email attachments to prevent email from being used as a transmission tool for viruses and malicious worms
- Block, alert and log intrusions
- Provide cooperative gateway protection to leverage the existing IS infrastructure and ensure that only endpoints with distributed firewalls and current security policy access the network

Real-world security has to be flexible. It is a fact of life that attackers will learn and adapt in an attempt to circumvent defenses.

Combined, these security functions and others protect each individual PC – local and remote. By distributing and enforcing PC security and security policy across all endpoints, the chances of a security breach are greatly reduced, thereby offering greater protection to the entire network.

Real-world security has to be flexible: threats, organizations, and corporate networks change. It is a fact of life that attackers will learn and adapt in an attempt to circumvent defenses. And, policy that once supported productivity may later thwart it. Real-world security solutions have to evolve to respond to new threats and changing organizational needs. Flexible security policy management is critical for maintaining maximum corporate security.

Policy Lifecycle Management is the key to maximizing corporate security and productivity. Centrally managed policy provides an enforcement mechanism



In order to protect today's dynamic corporate network frontier, an organization must extend corporate security and security policy to every PC–enterprise-wide.

to ensure all endpoints are compliant. Policy Lifecycle Management optimizes security by streamlining policy creation and providing feedback, enforcing and updating policy at all times.

Zone Labs Integrity

Zone Labs Integrity is a distributed endpoint security solution that enables central management of PC security and enforces security policy across the enterprise. Integrity's multi-layered defenses, including a distributed firewall with application control, block known and unknown hacker attacks by preventing unauthorized connections. Integrity's advanced Web management tools centrally deploy, maintain, and administer security policy enterprise-wide. Policy Lifecycle Management means that IT personnel can create, deploy, validate, and enforce policies quickly, for immediate security and productivity. Integrity integrates seamlessly with existing infrastructure management and security tools for an increased return on IT investments.

- Scalability: Integrity supports enterprise class hardware, network operating systems, databases, and protocols to deliver the scalability and reliability enterprises require. Client-side processing and platform independence accommodate organizations of any size.
- Proven Security: Integrity protects enterprise endpoints with the most widely used and recognized PC firewall and application control technology. More than 17 million users have proven the quality and stability of the Integrity Agent.
- Multi-layered Security: Integrity protects against the widest array of inbound and outbound, known and unknown threats providing powerful, optimized defense. Enterprise endpoint security is augmented with a layer of application control that prevents unauthorized applications from accessing the Internet. Controlling Internet access at the application level, rather than the network level, is highly effective at preventing rogue applications from sending data out to the Internet. In addition, Integrity's Mailsafe-email attachment protection stops transmission of email-borne malware.
- Balancing Security and Productivity: Integrity provides security policy deployment and management tools to deliver the best balance of security and productivity. Integrity's highly onfigurable client allows IT professionals to control security policy interaction-from silent to verbose. Customizable alerts can enhance communication of policy and user compliance while Zones facilitate trusted file and print sharing.
- Cooperative Enforcement: Integrity can leverage leading gateways to ensure that only endpoints with personal firewalls and current security policy access the network. Integrity seamlessly integrates with the Cisco VPN 3000 Concentrator Series to lock back doors and add security, convenience and cost savings for a complete endpoint security solution.
- Policy Lifecycle Management: Integrity gives IT professionals the tools they need to manage the entire security policy life cycle-from monitoring to creation and enforcement. Integrity allows IT professionals to create and implement flexible policies that address their organization's particular security challenges.
- Centrally-managed Security: Advanced Web management tools streamline all facets of enterprise policy management. Remote administration makes it simple for anywhere, anytime management. Distributed technicians or service providers can centrally manage thousands of endpoints.
- Leverage Existing IT Investments: Organizations relying on popular user and group management systems, network management systems, enterprise database management systems, reporting tools, Web and application servers will find superior interoperability and compatibility. Add or synchronize users and groups from existing directories (e.g. NT, RADIUS) for more efficient administration. Integrity leverages existing deployment technologies, including SMS and Tivoli for enterprise class rollouts to thousands of

distributed clients. Seamless integration with leading gateway devices (such as Cisco VPN 3000 Concentrator Series) ensures only secured PCs connect to the network. Integrity works well with existing infrastructure management and security tools to provide greater security and increased ROI on existing and future IT investments.

Conclusion

The costs of network incursions are increasing rapidly, as are the number of hackers and the sophistication of their methods. The potential damage to brand reputation, customer relationships, and capacity to do business, may dwarf conventional outage and repair issues. The traditional defensive perimeter has been shattered by legions of unsecured remote and mobile users logging in via Internet connections. The new paradigm for network security places a perimeter around each endpoint, via distributed firewalls.

Zone Labs Integrity leverages the most widely used personal firewall technology with centrally controlled Policy Lifecycle Management. Enterprises benefit from a scalable, flexible, multi-layered distributed firewall so that only authorized Internet contacts are permitted, blocking both inbound and outbound hacking. In this way, enterprises can proactively manage their security in an increasingly connected age, where failure to be sufficiently “paranoid” can result in significant, even catastrophic loss.

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

ZONE LABS™
A Check Point Company

Check Point™
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.