Shield Your Enterprise from Hackers

ZONE LABS integrity™

Targeted hacker attacks are the most damaging and costly security breaches to an enterprise. According to the 2003 CSI/FBI Computer Crime and Security Survey, at $70 million, stolen data remains the largest financial loss to enterprises. But, the ultimate cost to an organization is nothing short of its reputation, customer relationships and brand.

To gain access to the network, profit-driven hackers target the weakest link: the endpoint PC. Hackers have learned that typical security measures, such as antivirus, intrusion detection systems and perimeter firewalls, are no match for customized Trojan horses, spyware and other malicious code. And, with the proliferation of remote, mobile and wireless computing, there are more easily available, highly vulnerable PC targets than ever.

Zone Labs Integrity™ 4.5 is a best-in-class, centrally-managed endpoint security solution that locks down network PCs—local and remote—while working with the existing infrastructure to protect valuable enterprise data.

Proven endpoint security.

Zone Labs Integrity defeats hackers by concealing PCs, preventing unauthorized applications from trafficking confidential data, and blocking attempts to hijack trusted applications. Zone Labs' patented technology automatically blocks new and unknown attacks with its unique "guilty until proven innocent" approach to network security.

Proven in over 800 enterprises, our best-in-class solution allows for centralized management of PC security and security policy across the enterprise. It integrates with network access devices—VPNs, wired and wireless LANS—to ensure only PCs with the most current security can access the network.

Protect Your Data with Impenetrable Security

Zone Labs Integrity safeguards enterprise data by securing the network's most vulnerable access point—the endpoint PC. Our multi-layered endpoint security automatically blocks known & unknown threats to transparently protect endpoint PCs and the larger enterprise network from costly hacker attacks—including, Trojan horses, spyware and other malicious code.

- **Hides Targets.** Integrity hides PCs from hackers and blocks all unauthorized inbound communications.
- **Blocks outbound threats.** Integrity blocks Trojan horses and spyware from sending proprietary data to hackers.
- **Prevents application hijacking.** Integrity protects enterprise data by keeping trusted applications from being hijacked.
- **Restricts resource access.** Integrity allows administrators to segment network traffic and restrict resource access on the LAN while maintaining high security for Internet connections.
- **Thwarts tampering.** Integrity prevents hackers and users from circumventing or disabling security—even if users have local admin rights.
- **Closes gaps in existing security measures.** Only Zone Labs' Cooperative Enforcement™ technology integrates with the existing IT infrastructure—antivirus solutions, leading VPNs and 802.1X/EAP-enabled network access devices—to further harden network security.

Maximum Network Protection

No matter where employees work, Integrity protects their PCs and the enterprise data they access. Only Integrity integrates with network access devices to guarantee remote and local PCs are equipped and running the most current security BEFORE accessing the enterprise network. Out-of-compliant PCs are conveniently directed to Web-based resources, where updates may be obtained. Zone Labs' exclusive Cooperative Enforcement™ technology, integrates with select VPNs and 802.1X/EAP-enabled switches, routers and wireless access points to prevent network access until PCs are in compliance.

Integrity's Advanced Cooperative Enforcement (ACE) technology optimizes network security by allowing administrators to customize network "trust" criteria based on their organization's specific needs. ACE allows administrators to audit, inventory and enforce critical network access criteria on employee PCs. ACE enforcement rules include: patches, antivirus present & running, application presence or absence, application component, registry keys, and files.

Targeted Hacker Attacks Are Real

Date: 2000 - 2001 **Attackers:** Vasiliy Gorshkov & Alexey Ivanov

Victims: Five banks and online services companies located in Texas and California

Attacks: The attackers gained unauthorized control over numerous computers and then used them to commit massive fraud involving PayPal and eBay. The FBI found more than 56,000 credit card numbers and stolen bank account information on the attackers' computers.

Damages: Not quantified.

Source: US Department of Justice, October 2001

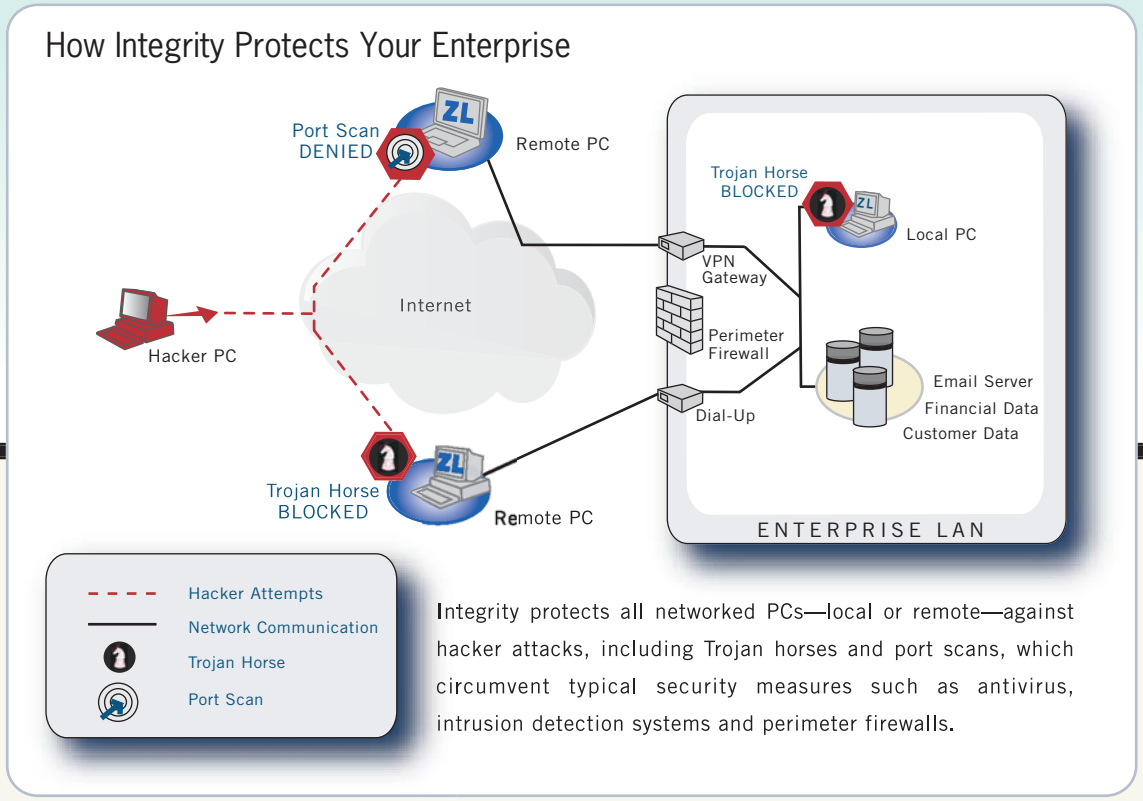
Date: October 2000 **Attackers:** Unknown **Victim:** Microsoft

Attack: Hackers penetrated Microsoft's corporate network and might have viewed or even altered the source code for Windows operating system and MS Office programs. Experts believe the attacker used a QAZ Trojan to compromise a remote access employee's PC and take control of the user's system.

Damages: Microsoft spent much more money and effort containing the public relations problem than fixing the security problem.

Source: Wall Street Journal, October 2000

Simple, centralized management.



Integrity protects all networked PCs—local or remote—against hacker attacks, including Trojan horses and port scans, which circumvent typical security measures such as antivirus, intrusion detection systems and perimeter firewalls.

Tools That Simplify Security Administration

Integrity delivers streamlined administration tools for efficient security policy creation, deployment and management. Integrity enables organizations to realize PC firewall security with minimal IT administration, and allows organizations to customize and strengthen their security policy using simplified management tools.

- **Delivers simple, rapid deployment.** Distribute and update client software with downloadable, pre-configured installation packages. And, easily update security policies in real time.
- **Enables immediate firewall protection.** Choose from a range of firewall management options, from powerful "out of the box" protection to defining a complete set of firewall rules for each application.
- **Provides quick and easy policy creation.** Manage and maintain security policy effectively using Integrity's intuitive Web-based interface, pre-defined policy templates and re-usable policy elements.
- **Facilitates informed and assured policy decisions.** Inventory user applications to quickly identify and secure vulnerable applications, creating policy that reduces risk while maximizing administrator and user productivity.
- **Enables flexible policy assignment.** Provision policies based upon users or groups; connection type (VPN, dial-in, wireless LAN); devices at particular locations; a simple default policy; or any combination of these methods.
- **Leverages existing infrastructure.** Opt to sync with a wide range of user management systems based on NT Domain, Active Directory, LDAP and RADIUS to save time and deliver role-based policy.
- **Allows flexible security management.** Maintain user productivity with minimal IT support. Administrators can choose a range of client management options; from transparent, IT-management to allowing end users to control their own security policies when disconnected from the corporate network.

To learn more about how Integrity protects your data by locking down your endpoint PCs with simple, central security administration, visit Zone Labs at www.zonelabs.com/integrity

Zone Labs Service and Support

Zone Labs, Inc. offers comprehensive service and support options for enterprise customers. Dedicated technical support is available via phone, secure Web site, or on-site systems engineers. Zone Labs is committed to providing our enterprise customers with the world-class service and support they need to maximize their technology investments.

> To learn more about Integrity, visit Zone Labs at www.zonelabs.com/integrity

ZONE LABS integrity™

System Requirements

▪ Integrity Clients

Operating Systems
- Microsoft® Windows® 95/98/NT/2000 and XP

Processor
- 233 MHz Pentium II (or greater)

Memory
- 32 MB RAM (128 MB or higher recommended)

Hard Disk Space
- 10 MB

▪ Integrity Server

Operating Systems
- Windows 2000 Server (SP4) and Advanced Server (SP4).
- Windows Server 2003

Processor
- Intel-based: 600 MHz Pentium III (or greater)

Web Browsers
- Internet Explorer 6 (or higher)
- Netscape Navigator 7 (or higher)

Database Management Systems
- Oracle 9iR2 with Oracle "thin" JDBC Driver 1.2
- Microsoft SQL Server 2000 SP3 with Microsoft SQL Server 2000

Gateways (Optional)
- Cisco VPN 3000 Concentrator Series
- Nortel Contivity VPNs
- Check Point VPN-1 with SecureClient
- EAP Supported Gateways

Directory and Authentication Applications
- RADIUS
- Windows NT Domain Services
- LDAP

ZONE LABS

Smarter Security™

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
Düsseldorfer Str. 40a
65760 Eschborn, Germany
tel +49 6196 773 670
fax +49 6196 773 6777