



The Need for Endpoint Security

— Zone Labs, Inc.

► Hurwitz Report



The Need for Endpoint Security

— Zone Labs, Inc.

iii Executive Summary

This paper discusses a set of best practices that can assist in limiting the impact of problems associated with laptops and PCs. It also describes how the Zone Labs solution provides assurance that the endpoint of the trusted network — the PC — is protected.

1 Overview

A number of factors come into play when attempting to protect the complex networks of today.

2 Issues in Endpoint Security

The factors creating the need for endpoint security are clear, but problems remain, including client proliferation, moving among different types of networks, and the varied threats in today's computing environments.

3 Best Practices in Endpoint Security

A number of possible ways exist to protect an endpoint PC from threats and from the constant onslaught of new attacks.

4 The Zone Labs Integrity Solution

The Zone Labs Integrity (ZLI) solution for endpoint security combines a stealth firewall, application control, and email security.

6 Conclusion

The Zone Labs Integrity solution sets the bar for other products to meet in the centrally-managed endpoint security space.

A Hurwitz Group white paper written for:

Zone Labs, Inc.
1060 Howard Street
San Francisco, CA 94103
Tel: 415 341 8200
Fax: 415 341 8299
www.zonelabs.com

Published by:
Hurwitz Group, Inc.
111 Speen Street, Framingham, MA 01701 ► Telephone: 508 872 3344 ► Fax: 508 872 3355
Email: info@hurwitz.com ► Web: www.hurwitz.com

February 2002

© Copyright 2002, Hurwitz Group, Inc.
All rights reserved. No part of this report may be reproduced or stored in a retrieval system
or transmitted in any form or by any means, without prior written permission.

EXECUTIVE SUMMARY

With today's complex distributed systems, only one constant remains — the client PC at the source of a request. "Anytime, anywhere" access and a mobile workforce ensure that the paths to information resources are dynamic, with changes based on type of user or current location. First, we take it home, then the client PC is hauled around the world, connecting from hotels, remote offices, and partner locations. The client PC operates as the endpoint to the trusted network, providing direct access to critical enterprise information assets.

A number of challenges are associated with managing client PCs and laptops. The logistical challenges are obvious — their sheer numbers create a management nightmare. In addition, security risks abound, with proliferating attacks by new viruses and worms, as well as the plethora of new hacking scripts and exploit code. Since PCs act as the endpoint of trusted networks, a compromise is a considerable threat to enterprise information assets.

This paper describes the risks and problems associated with laptops and PCs. It discusses a set of best practices that can assist in limiting the impact of these issues. Finally, it describes how the Zone Labs solution provides assurance that the endpoint of the trusted network — the PC — is protected.

Overview

It is quite clear that technology has permeated all facets of our work lives. Today's computer systems are highly distributed and complex, with network devices everywhere and multiple paths to a particular destination. Often applications and systems are being built component by component — web servers, app servers, load balancers, database servers, and other components are combined both to tune performance and to provide the end-user experience people expect. A number of factors come into play when attempting to protect the complex networks of today. The most prominent are described below.

The Mobile Workforce

Laptops are getting smaller, travel is expected, and people work from home or at remote offices. Isn't it great that we can all take our work with us? Well, we do, and it's better than letting it pile up at the office. The flexibility and access demands of a mobile workforce creates an "anytime, anywhere" expectation on the part of the users. This often translates into multiple paths into a network that reflect the relative location of the user population.

.....

The onset of wireless devices and PDAs in conjunction with the ever-increasing communications demands in today's business world increase the number of devices and attack points against a trusted network.

.....

The Ubiquinet

Part and parcel with mobility comes an expectation of "always on." So maybe you don't want to connect your washing machine to the Internet just yet, but there is no denying the "Ubiquinet" is coming quickly. The onset of wireless devices and PDAs in conjunction with the ever-increasing communications demands in today's business world increase the number of devices and attack points against a trusted network.

The Disappearing Perimeter

Employees work while traveling or at home; contractors and temps have direct access to even the most sensitive information assets within an enterprise network. The blending of "insiders" (employees) with access from the outside (Internet) and "outsiders" (contractors/temps) with access from the inside (corporate offices) has further blurred the idea of a perimeter. Sure, there is a gateway, but each side has some territorial claim over the other. And the user population typically has the same access to sensitive resources, even though users constantly move from trusted to untrusted networks.

Increased Threat Level

Act and react — it's all part of the game. Hackers attack, we react. Hackers then respond with newer tools and techniques. The threats are increasing in complexity, with polymorphic viruses and worms, the use of encryption to bypass network security, and custom attacks against a specific target. Meanwhile, the number of scripts and exploits continue to increase and information assets grow in value.

The Need for Endpoint Security

The fact that today a user may be accessing resources from within the trusted network environment and tomorrow be coming from a completely different, untrusted location is critical to understand. Since PCs and laptops perform their own processing, the remnants of activities occurring in both locations can remain on the device. Viruses, Trojan horses, inappropriate configurations, or rogue software all create risk, particularly when moving from untrusted to trusted networks. Constant vigilance is required to protect against this threat.

The idea of a mobile workforce on the Ubiquinet, and trusted PCs with no apparent bounds, leads directly to the need for endpoint security — control over client PCs regardless of location or connection status. Although traditional firewalls still maintain their place protecting the static network, there is no denying the need for a distributed firewall to travel with the client PCs and protect against all threats.

Issues in Endpoint Security

The factors creating the need for endpoint security are clear, but problems remain. It is no easy task to protect the endpoints from being compromised themselves, thus providing a foothold for compromising a trusted network. These issues include client proliferation, moving among different types of networks, and the varied threats in today's computing environments.

Client Proliferation

In many ways, personal computers have become commodity items — they are inexpensive enough to replace for the next, more powerful version. Then, the PC being replaced becomes the “backup” or “second PC” that performs some specific point function. Although PCs may be replaced every three years, they often aren't thrown out for seven or eight years. At home, this is even more likely the case, with PCs being used in many different ways, sometimes allowing corporate connectivity along with a teenager's chat sessions, music downloads, etc.

PDA's and wireless devices, even cell phones, now have links into the network to perform

certain functions. This all creates an abundance of clients with network access. All of these access points act as a connection to the critical business information in corporate data centers.

Net, Net, and Net (Internet, Extranet, Intranet)

First came the local area network, now redubbed the intranet, deployed to take advantage of the basic communication needs of an enterprise. Second was the Internet with its real-time, global broadcast capabilities. Finally comes the extranet, an intranet deployed externally to support employees as well as business partners and other related parties. These different types of networks have different security requirements, and yet they are often interchangeable to an end user who needs to use different ones.

Trusted Tunnels

Authorized clients can claim a trusted position on corporate networks. They are often given “express lane” access to corporate information assets, using trusted tunnels through the untrusted network. These tunnels bypass the traditional security measures used to thwart hackers and therefore must be protected.

Multiple Known and Unidentified Threats

Nowadays, threats come at you from all angles. They propagate via email and the Web, take advantage of open file shares and other misconfigurations to collect information, install a Trojan horse, and wreak general havoc across an enterprise. And just when all of the known threats are addressed, a new vulnerability is found and a new exploit is created, beginning the protection cycle once more.

Best Practices in Endpoint Security

A number of possible ways exist to protect an endpoint PC from threats and from the constant onslaught of new attacks. Enterprises must review these solutions from the perspective of best practices. The most important best practices are described below.

Quick Deployment

An insecure client PC is an imminent threat to your network. Time wasted is inherent risk. The logistics of dealing with thousands of clients cannot be overlooked. The ideal endpoint security solution would enable a simple and fast initial deployment that provides foundational security for the PC.

Group-Level Restrictions

As the enterprise gains insight into its security needs, it becomes apparent that different user populations require different security restrictions. The ability to group these users together to define those requirements provides a way to effectively manage the risks while still ensuring that users gain appropriate access where necessary.

Centralized Command and Control

Securing thousands of clients requires control over the applications that are intended to protect them. Central management ensures that configurations are maintained that are consistent with corporate policy and that updates are distributed accordingly. They also provide the ability to perform instant security policy upgrades for rapid response to evolving threats.

Protect Against Multiple Threats — Known and “Unknown”

Just when one security hole is plugged, another opens up. It is important to recognize that the threats to a PC come from multiple points. Each of these avenues of approach and types of attacks should be evaluated for impact and addressed by an endpoint security solution.

“Unknown” threats are only unknown to us — the hackers are constantly creating new and unidentified exploits that are known to them but will not be picked up by traditional signature-based protection systems. Blocking unknown threats is crucial because once hackers have gotten into a network, they are very difficult to get out, as they sniff for admin passwords, install backdoors, and plant more malicious code. Preventing these unknown threats is inherently more efficient and can yield tremendous cost savings.

The “Decontamination” Chamber

PCs are being used in many different network environments, for different purposes and at different levels of trust. It is not practical to assume that security has been maintained throughout these many different sessions. The final check for security should be just prior to a request to enter the trusted network. This “sanity check” is activated upon login to the environment, and should perform a thorough, yet quick, review of the PC’s current security posture.

The Zone Labs Integrity Solution

The Zone Labs Integrity (ZLI) solution for endpoint security combines a stealth firewall to dynamically recognize incoming network events, application control to ensure appropriate behavior on a client, and email security to identify and quarantine suspicious attachments that

may affect this most likely attack point to the PC. These endpoints are controlled through a central management server that provides policy-based update and reporting capabilities. The core ZLI solution is proven, with field-tested technology on over 17 million devices worldwide (see Figure 1).

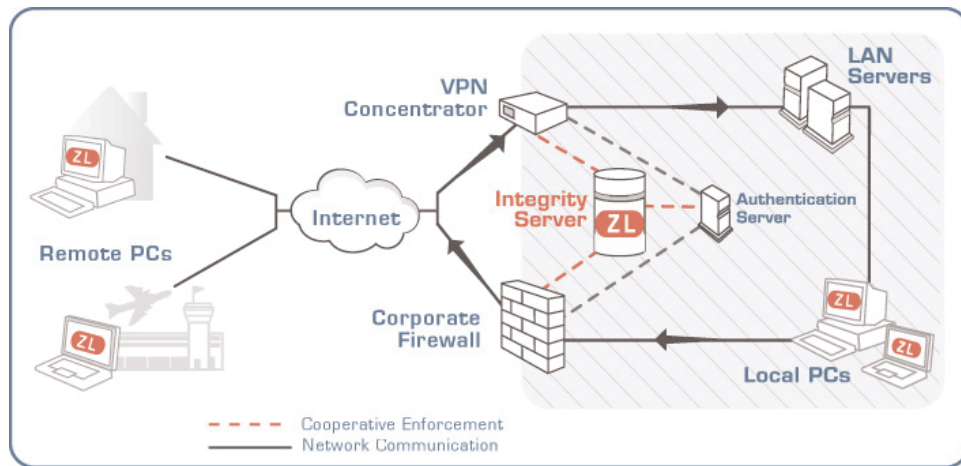


Figure 1. The Zone Labs Integrity diagram.

Flexible Configuration

ZLI clients can be configured to meet the needs of different types of enterprise users. High risk PCs and users can have both the security settings and the ability to modify those settings “locked down” to ensure they are always in place. Meanwhile, power users who are security savvy and need flexibility can be given some autonomy over the features and capabilities of the system.

Central Management

ZLI provides the mechanism to manage and control thousands of users. With its central console, client installations can be reviewed, policy updates can be distributed, and configuration settings can be modified.

Cooperative Enforcement

ZLI works with the Cisco VPN 3000 Concentrator Series during the initial setup of a secure tunnel, and while the user is connected to the enterprise network, to provide feedback regarding the security of the client. It ensures that systems that don’t conform to the policies set forth by corporate policy are denied network access in order to protect the network.

Policy Life-cycle Management

It is simple to set policy, but much more difficult to ensure that the policies get implemented and stay implemented. ZLI has the ability to automatically discover applications connecting to the Internet to ensure that no additional risks are introduced as well as to conduct policy analysis to ensure their successful implementation.

Conclusion

Endpoint security is a critical piece of the security architecture of enterprises today. If compromised, the client would provide that unfettered access to sensitive information resources that hackers desire. In the hands of end users, inappropriate risks are often taken solely to get the latest MP3 file or look at the latest animated file.

Zone Labs has been in the security business since 1997. Along with its client software, Zone Labs provides a management server component that serves a fundamental need in the enterprise. The Zone Labs Integrity solution sets the bar for other products to meet in the centrally-managed endpoint security space.



About Hurwitz Group

Hurwitz Group, an analyst, research, and consulting firm, is a recognized leader in identifying and articulating the business value of technology. Known for its real-world experience, consultative style, and pragmatic approach, Hurwitz Group provides strategic guidance to its clients by delivering analysis, market research, custom content, and consulting services. Clients include Global 2000, software, services, systems, and investment companies.