

# Zone Labs Integrity

---

Enterprise Endpoint  
Security

---

// Trusted Zone //

## Minimizing Endpoint Security TCO with Zone Labs Integrity

---

A White Paper Presented  
by Zone Labs



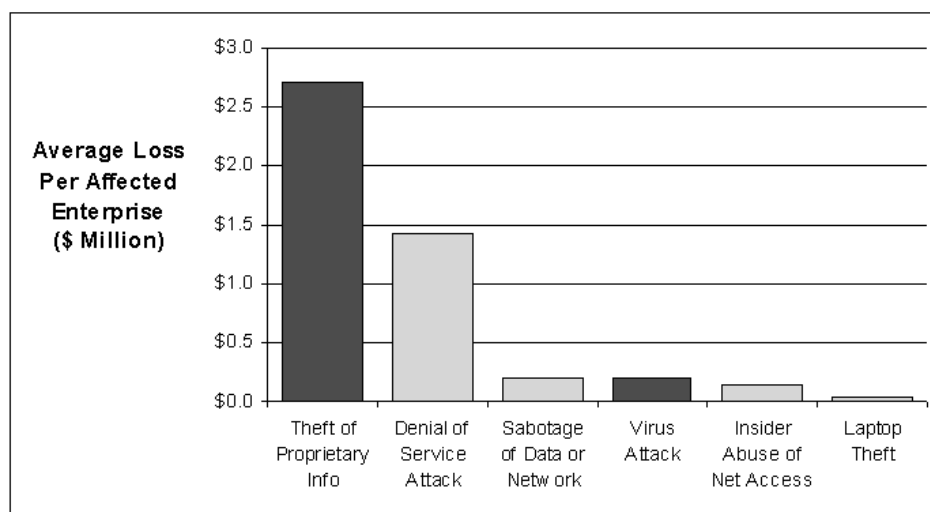
A Check Point Company

### Introduction

Investing in enterprise security solutions ultimately involves weighing value and cost. This paper focuses on the Total Cost of Ownership (TCO) of products that secure network “endpoints” – the PCs and other devices that connect to the enterprise network and the Internet. As such, the reader should first understand the value that these products can provide.

The 2003 CSI/FBI Computer Crime and Security Survey found that despite almost universal use of anti-virus products, viruses caused the most frequent enterprise security breaches. In 2003, the average annual cost of virus damage was \$200,000 per organization. However, the best PC firewall-based products could have limited or prevented propagation of worms and viruses across affected enterprise networks. By doing so, they would have substantially reduced the disruptions to business continuity caused by exploits such as SQL Slammer, MS Blaster, SoBig.F, and MyDoom.

The CSI/FBI survey also found theft of proprietary information occurred in only 20% of enterprises, but at an average loss of \$2.7 million it was the most costly type of security breach. Endpoint security could have protected the organizations that incurred these losses from the intrusions and hacker tools that cause them. In addition, the best endpoint products enforce security policy compliance on PCs before they're allowed to connect to the enterprise network. By delivering these benefits, endpoint security can greatly mitigate the risk of



Theft of proprietary information causes the greatest financial losses. Virus damage is less costly but affects more enterprises than any other threat. Both risks can be mitigated with endpoint security. Source: 2003 CSI/FBI Computer Crime and Security Survey

major financial damage. More detailed information on this topic is available from Zone Labs at [www.zonelabs.com](http://www.zonelabs.com).

Once the financial value of endpoint security is established, the next step is to evaluate its cost. The TCO of endpoint security is driven by factors beyond software licenses and maintenance fees. It is heavily influenced by the:

- Amount of hardware needed to administer security policies
- Up front cost to install, configure, and deploy the product
- Amount of IT staff time required for ongoing administration and maintenance
- Impact on end users, which affects both organizational productivity and IT support requirements.
- Potential for security losses if the product is ineffective or disabled

This paper examines these TCO factors and highlights the advantages of Zone Labs Integrity™, the leading endpoint security solution for enterprises. Integrity's superior scalability, ease of deployment and management, and minimal impact on end users minimize TCO while delivering the most trusted endpoint protection available.

## Elements of Endpoint Security TCO

### Security Software Licenses and Maintenance

Initial per-user license fees don't always reflect the full software cost of an endpoint security deployment. Other costs in this category may include charges for first year maintenance, recurring software subscription fees, and "optional" modules needed for management or policy enforcement. Zone Labs Integrity software licenses include standard first year maintenance, and all management and all enforcement functionality, all at no additional charge.

### Security Hardware and Maintenance

The cost of hardware will generally depend on the number of servers a product requires. Hardware servers may be needed for management, failover, database, and policy enforcement functions. Key drivers of total hardware cost are the size of the deployment and the security product's architecture. The more PC connections a product's management server can handle, the lower the per-user hardware and IT maintenance costs. Integrity supports as many as 75,000 connected users per management server, depending on the configuration. Such high scalability minimizes the number of servers needed for both administration and failover (if desired). In many cases, a single Integrity Server can support an entire enterprise deployment. Other products with lower server capacities can cost many times what it costs to deploy Integrity.

### Database Licenses and Maintenance

Database hardware cost drivers also influence the cost of database licenses. Midsize and smaller enterprises can avoid database license and hardware costs entirely by opting to use Integrity's built-in database. This option supports up to 1,000 connected users per server. Larger enterprises will need an external SQL Server or Oracle database. However, the same factors that minimize the number of database hardware servers that Integrity requires also minimize the number of database licenses needed.

#### Cost Factors to Consider

Recurring license fees
Server and appliance hardware
Configuration complexity
Rule writing volume, complexity
Incident response hours
Automated administration
End user impact
Security effectiveness

### Deployment Labor Costs

The labor cost of deploying an endpoint security solution is directly related to the complexity of initial configuration and rule set definition. Some products demand that administrators spend many hours learning proprietary rule scripting techniques. They may also require administrators to write complex rule definitions for large numbers of PC applications in order to

# Zone Labs

## Integrity

Enterprise Endpoint  
Security

White Paper

Page  
4

// Trusted Zone //

achieve the marketed benefits of the products. Products that rely on IDS or IPS technologies also burden IT staff with countless hours spent analyzing and fine tuning IDS/IPS behaviors and signatures. Without investing a substantial amount of time in these activities, administrators face a potential avalanche of "false positive" alerts. Enterprises also risk accidental denials of service to end users that can plague those technologies.

The relative simplicity of an Integrity deployment contrasts sharply with the burden imposed by other products. An administrator can install Integrity and deploy an effective baseline security policy to networked PCs in under an hour. Moreover, Integrity does not ask administrators to script a large number of complex rules. Its proactive security model blocks attacks and contains exploits that are instantly based on default settings and simple configuration steps. Whatever rules an administrator chooses to create can be defined mostly by pointing and clicking.

Many enterprises need to assign endpoint security policies to users and groups defined in their existing user directories. These organizations benefit greatly from Integrity's ability to import and retain group structures. The product is unique in the breadth of its integration with authentication systems and support for directory standards. Integrity integrates directly with Active Directory, NT Domain, LDAP, RADIUS, RSA SecurID, and other directory types. Some security products are unable to import group structures from those directories, forcing administrators to spend a considerable amount of time recreating group definitions.

### Ongoing Administration Costs

The annual management cost drivers of an endpoint security product can include:

- Creating and maintaining policies and managing policy exceptions

- Continually tuning IDS/IPS alerts to reduce false positives and rule errors
- Responding reactively to intrusions identified from IDS/IPS data
- Maintaining group definitions
- Updating the minimum anti-virus requirements enforced by the product

These processes may be executed at least weekly, if not daily. They can therefore have the biggest impact on TCO of any cost component, including software licenses. For this reason, superior usability has been a key design goal for Integrity from the beginning. Examples of Integrity attributes that reduce ongoing administrative costs include:

- An intuitive management interface that minimizes the number of steps needed to accomplish common administrative tasks. For instance, Integrity supports modifying a rule for one group without affecting how the same, global rule applies to other groups. Other products can absorb far more administrative time when a simple exception is needed to a global rule.
- Re-usable policy elements, such as firewall rules that automatically update and redeploy all the policies that use them when an administrator makes an edit.
- Automated synchronization with user directories, as opposed to the frequent manual updates of duplicate group structures that other products require.
- Automated updates of the anti-virus requirements in security policies. Other products demand frequent manual collection and entering of new information each time the anti-virus vendor issues an update. Integrity's automated anti-virus enforcement updates also minimize the time end users are exposed to new worms and viruses.

# Zone Labs Integrity

Enterprise Endpoint  
Security

White Paper

Page  
5

// Trusted Zone //

- ▶ Automated discovery of all PC applications in an enterprise that attempt network access. Administrators can use the resulting program inventory to make fast and informed decisions about network access privileges. Other products can only collect application information for individual PCs. One endpoint firewall even requires that administrators manually inventory and enter program information one PC application at a time.
- ▶ No ongoing IDS/IPS tuning and troubleshooting, and little forensic analysis of log reports. With Integrity's pro-active approach to security, administrators rarely need to deconstruct successful attack patterns and devise plans of corrective action. Unlike IDS/IPS-based products, Integrity is designed to stop attacks before they can succeed.

## End User Support

Organizations can deploy endpoint security software that requires little or no end user interaction. By doing so, they minimize the amount of user training they need to deliver. However, even invisible security can generate help desk requests. This can occur if a product initiates unexplained events that confuse, alarm, or disrupt employees' PC usage. An example of a potentially disruptive activity is an automated compliance remediation process. If implemented poorly, the process installs software updates or patches, and forces reboots of PCs, without the user's knowledge and/or consent. Zone Labs Integrity avoids this drawback by providing self-service remediation tools for end users. These resources explain to users why they're out of compliance with enterprise policy. They also tell users how to use the updates provided to get back in compliance quickly and easily. Administrators can customize all Integrity self-remediation tools and end user alert levels. Customization lets enterprises provide exactly the right information and resources needed to minimize support costs.

Under some circumstances, organizations let selected employees manage their own security settings. The support burden in these cases is directly related to how easy the security client's GUI is to understand and use. Integrity clients offer a clear TCO advantage in this area. Zone Labs has years of experience developing ZoneAlarm, the most widely used and praised personal firewall for consumers. ZoneAlarm has won numerous awards due to both its market leading endpoint security and the simplicity and intuitiveness of its interface. Millions of non-technical consumers use the ZoneAlarm family of products successfully every day with little or no technical support. Consequently, administrators can be confident that their

Cost Component	Zone Labs Integrity Advantages
Software	No extra cost for management or policy enforcement capabilities
Hardware	Fewer security servers needed, and lower maintenance costs, due to superior scalability
Database	Fewer database servers needed since database replication not required to scale
Deployment	Less IT time required due to default protection and configuration simplicity
Administration	Less IT time required to design and tune policies, synchronize with user directories, and update anti-virus requirements
End User Support	Fewer help desk calls caused by unexplained security events on PCs, or by hard to understand user interfaces
Productivity Impact	Less risk of business and IT disruption caused by a security breach, since Integrity can't be disabled or bypassed

# Zone Labs

## Integrity

---

Enterprise Endpoint  
Security

White Paper

Page  
6

// Trusted Zone //

Integrity users will also need little assistance. Other endpoint security products have been developed with much less consumer feedback. They are therefore more difficult for employees to learn and manage. The result is substantially higher TCO.

In summary, simplicity of use for both administrators and end users plays a major role in minimizing TCO. Conversely, complexity in management and endpoint user processes drives TCO up. But perhaps most importantly, an intrusion or exploit that is able to evade a second tier endpoint security product and damage business continuity can have a huge impact both on end user support costs and IT workloads. In this light, the security effectiveness of an endpoint solution is itself a major factor in the ultimate TCO of the product.

### Quantifying TCO and ROI

The focus of this paper has been qualitative because a given organization's costs and returns are heavily influenced by its unique circumstances. In addition to variations in hardware, database, and labor costs from company to company, differences in security infrastructures, risk profiles, security policies, and even corporate cultures can result in substantially different numbers. For these reasons, Zone Labs has developed a tool for modeling an organization's return on endpoint security investment and TCO using its particular cost inputs, industry benchmarks, and other characteristics. A Zone Labs account representative can help an enterprise use the tool to calculate its own ROI and TCO estimates, or provide a summary of results based on key inputs provided by the enterprise.

### Achieving Best of Breed Security with Minimal TCO

The number of sophisticated intrusion attempts targeted at the least protected network access points – remote and internal endpoints – is on the rise. The number of application and operating system vulnerabilities, and the worms and viruses that

exploit them, is also growing. Attackers use best of breed hacking tools to execute their most costly attacks. To counter them, enterprises must employ the best available security practices and technologies.

Zone Labs pioneered commercial personal firewalls and has always focused on providing the most advanced and effective endpoint security available. At the same time, Zone Labs fully understands that usability and cost effectiveness are critical to enterprise security administrators. The TCO advantages Integrity provides based on its superior scalability, ease of deployment and administration, and minimal impact on end users reflect this understanding. Enterprises can invest in Zone Labs Integrity with the confidence that they're getting the market's leading endpoint protection while minimizing their TCO.

# Zone Labs Integrity

---

Enterprise Endpoint  
Security

---

White Paper

---

Page  
7

// Trusted Zone //

## About Zone Labs, Inc.

Zone Labs, Inc., a Check Point Company, 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 businesses 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](http://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



We Secure the Internet.