

# Minimizing Security-Related Total Cost of Ownership

An Industry-Leading Approach for Optimal Security



## Introduction

Any security professional worth his or her salt understands that the job at hand isn't just a matter of protecting the technology ecosystem, it is a question of doing so without racking up costs that will raise the CFO's eyebrows. In today's economy, though, the antes have been raised. Nowadays security gurus aren't just expected to keep security-related problems at bay as cheaply as possible. They are also counted on to find ways to reduce the total cost of ownership (TCO) of *all* IT assets by minimizing risks, reducing network complexity and optimizing resources.

## TCO Overview

In the last decade, experts have dashed off dozens of equations and analyzed countless line items trying to calculate the long-winded value of IT asset TCO. What it really all boils down to, though, are two types of costs: direct costs and indirect costs.

Time after time, experts have shown that the readily evident direct costs (such as buying software and hardware) are often overwhelmed by equally expensive indirect costs (such as running and troubleshooting said software and hardware).

**“For an average enterprise, indirect cost elements may contribute 50% or more of the overall TCO.”**

according to Gartner, Inc.

To calculate the TCO in today's security environment, one must not only factor in the cost of technology and staff, but risks and potential lost values from not putting them in place. Hidden indirect costs could include lost productivity of end users and the time sunk by IT staffers responding to malware.

Read closely how security implementations in four major areas can reduce IT TCO dramatically, effectively paying for direct costs of these technologies by reducing the overall bottom line. They are:

### 1. Endpoint Protection

Centrally defining and controlling a trusted application environment protects against unauthorized and malicious software and reduces TCO by minimizing the amount of time staff spends reimaging machines and reacting to infections.

### 2. Data Protection

Offering effective data security by centrally defining trusted users and removable devices, while controlling, encrypting and auditing the inbound and outbound flow of information, mitigates the risk of data loss and brand equity, thus lowering your TCO.

### 3. Vulnerability Management

By detecting risks and deploying remediation automatically using a market-leading vulnerability management solution, organizations with complex environments can increase efficiency and cut TCO.

### 4. Reporting and Compliance

Automated reporting and compliance features embedded within vulnerability, endpoint and patch management tools reduce the cost of proving to the auditors that an organization's practices are up to snuff.

### Endpoint Protection

In January 2005, one of the largest healthcare providers in the U.S., a publicly traded company listed on the NASDAQ stock exchange that employs more than 16,000 people, **spent \$150,000 cleaning up a virus that crippled the company's entire network from a single infected machine.**

After nearly a week of working around the clock, the IT staff concluded that a malicious website exploited a flaw in Internet Explorer and flooded the network with Internet traffic from one poorly protected endpoint. This eye-opening incident vividly illustrates how ineffective endpoint security practices can dramatically impact operational TCO.

Traditional security technologies such as blacklist anti-virus technologies do not provide businesses with adequate protection against malware or other threats. Organizations that rely solely on this approach for protection require considerable system resources to continuously update their defensive engines while receiving little-to-no protection against unknown and targeted attacks. They have to consistently throw money at security incidents, reacting to problems rather than preventing them.

That same healthcare leader, for example, not only spent tens of thousands of dollars on that singular event—it also continuously drained its coffers before that every time a machine became infected.

The company's policy dictated that when a machine has a malware-related issue, the employee ships the infected machine to the IT staff and is given a new computer—a process referred to as “hot-swapping.” Prior to changing its security methodology, **on average, the company hot-swapped 30 machines per month at a cost of \$400 per machine. Over the course of a year, it burned through \$144,000 on this process alone.**

Things changed when the company deployed a centralized endpoint solution from Lumension Security that employs application whitelisting technology. The deployment **saves the company \$12,000 per month on hot-swapping costs alone because malware is not authorized to execute on protected PCs or laptops.**

Unlike blacklisting, a whitelisting approach is a more proactive way to protect against threats and reduce TCO. With a whitelist approach, end users are no longer allowed to install un-trusted software on endpoints, such as media applications, file sharing applications, etc. These installations eat up significant processing power and memory and are potential malware conduits.

Cutting off such resource drains at the pass eliminates the need to reimage machines after infection and keeps machines running efficiently—bottom line, whitelisting improves uptime and computers run faster. Both factors inevitably slash IT TCO.

#### Success Story

Another healthcare company, John C. Lincoln Health Network, observed these TCO reductions firsthand when it implemented Lumension Security Endpoint Protection Solution. Before they put the technology into place, IT staffers were drowning in work related to managing endpoints.

Each year, **15%** of their computers would require service; **30%** required reimaging and **70%** needed the installation of more memory.

For John C. Lincoln Health Network, direct costs associated with reimaging each PC were **\$250**.<sup>1</sup> The indirect costs associated with reimaging a PC were estimated at **\$150**.

After John C. Lincoln Health Network implemented Lumension Security Endpoint Protection Solution, they were able to ‘reduce the FTE headcount dedicated to these tasks from 4.0 to 1.5. Additionally, the organization was able to avoid future headcount growth.’<sup>2</sup>

## Data Protection

Every week the media sounds the alarms on new incidents involving the loss of customer records, confidential information and intellectual property, most of them accidental, involving some type of removable device, whether an unencrypted USB stick, cell phone, external hard drive or the like. These high-profile bungles have the potential to dramatically contort IT TCO in very short order, not only in costs associated with notifying consumers and settling legal fees, but also in loss of brand equity and customer confidence.

In 2008, Countrywide Financial experienced a data breach from an employee who was downloading files onto his thumb drive – a total of 20,000 customer records. International headlines quickly uncovered Countrywide's lack of control over removable devices and an absence in oversight on security policy settings across their organization. As a 'high profile' breach in a highly regulated industry, experts estimated it will cost Countrywide a whopping \$6,100,000.<sup>3</sup>

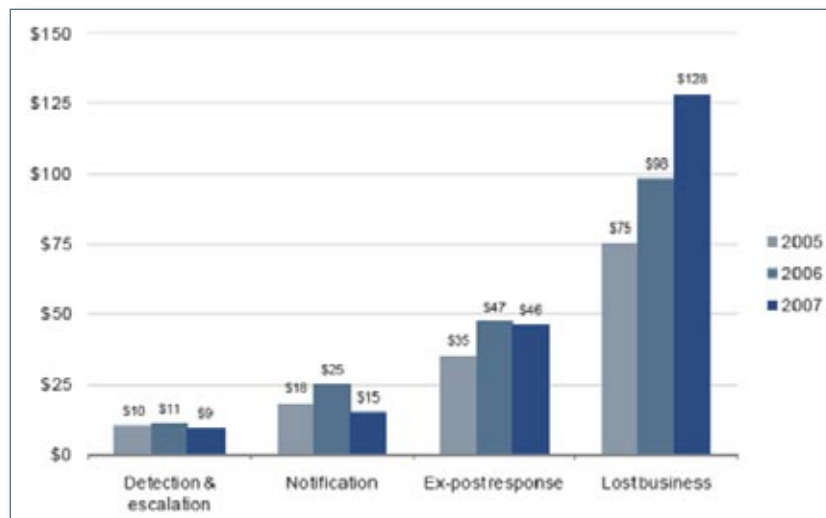
In April 2007, a Forrester Research study published metrics to calculate the potential cost of a security breach for any given company.<sup>4</sup>

- ▣ For a 'low-profile' breach in a non-regulated industry, the cost per record is \$90.
- ▣ In a 'low-profile' breach in a regulated industry, the cost per record is \$155.
- ▣ In a 'high-profile' breach in a highly regulated industry, the cost per record is \$305.

These numbers aren't the end of it, either—there is an even more important dynamic that organizations tend to overlook. Consumers prefer not to conduct business with a company who has ever experienced a data breach as more than 40% said that they might discontinue their relationship.<sup>5</sup> 19% of respondents have already discontinued their relationship with the company as a result of the data breach.<sup>6</sup>

If an organization has \$10,000,000 in revenue, they will stand to lose \$1,900,000 in revenue alone. This does not include the loss of trajectory in future business initiatives. The damage to a company's reputation is far greater than the cost of the fines themselves. They will have a commensurate loss of revenue amounting to 8%, or \$800,000.<sup>7</sup> Therefore, this organization has increased their TCO by \$2,700,000.

Compromised companies must increase spending, not only to pay legal fines, but also to rebuild a positive corporate brand image. These costs impose a heavy burden on organizations, increasing direct and indirect costs, thus increasing TCO. Check out the overall breakdown calculated by the Ponemon Institute in 2007 in the chart below:



Data breach costs by center per record compromised, 2005-2007

## Minimizing Security-Related Total Cost of Ownership

Preventing data loss through control and auditing of data transfer and encryption of data-in-motion and at-rest is critical to controlling these incidents within any organization.

The only way to manage all of the removable devices that attach and detach from a network is to identify them. Device scanning tools give an organization insight into all of the removable devices that are currently connected, or have ever been connected, to the endpoints.

Once this baseline is understood, best practices recommend setting a global policy across an entire organization. Implementing exceptions to the policy is most manageable and appropriate to protect a business. With enforcement of data and device policies across entire groups of users and devices, organizations can effectively protect their data from unauthorized and insecure transfer.

Data protection solutions effectively assess each device, the data on each device, from what machine, which user and when the user downloaded or uploaded information, mitigating the risks of a debilitating data breach.

This is the tact taken by Lancashire Care NHS Foundation Trust, which uses Lumension Security Data Protection Solution to control employee use of USB memory sticks. The solution provides the IT organization with the flexibility to set up a policy that states that a particular type of USB memory stick can be used, but only if it is theirs and only if it's encrypted. It also gives the trust the opportunity to shadow and log all usage of USB memory sticks for auditing and compliance purposes. Additional security measures put in place, included turning off the write function for DVDs and CDs by setting up a rule that only allows data to be read, not written, from these media.

**“I now don't have to worry about loss of reputation through someone losing a memory stick, which may contain person identifiable data or corporate sensitive information.”**

Lancashire Care NHS Foundation Trust

### Vulnerability Management

The number of vulnerabilities continues to increase across operating systems and applications as cyber criminals refine their methods day by day. These crooks are exploiting vulnerabilities at a faster rate than ever with automated tools at their fingertips.

In order to beat the bad guys, keep business running without interruption and reduce the costs of mitigating vulnerability risk, IT departments must deploy a centralized approach that pulls everything together in an automated fashion. This includes automated discovery and baseline of all IT assets, vulnerability assessment, security patch and remediation, and security configuration management.

#### Network Discovery

Network discovery solutions shed light into the risk areas that are often not visible within the network environment. With newfound visibility into the organization's environment, IT can discover all assets within the network and uncover undetected or unknown vulnerabilities. Oftentimes, discovered assets are silent or hidden systems within a network, providing access to potential threats. By performing comprehensive discovery, organizations receive a flexible approach to understanding and assessing what IT assets are connected to the network as well as discovering all rogue machines, including; IP address range, Active Directory, OUs, network enumeration, host name, and file port import.

Doing so not only solidifies security, it also has the potential to streamline operational TCO. Not only can these assets be a source of vulnerabilities, but they are also potentially underutilized resources. By adopting automated discovery, organizations can gain a complete view of all IT assets residing on the network.

#### Vulnerability Assessments

Effectively identifying and remediating vulnerabilities before they attack a network environment is a great way to reduce IT TCO.

“Increased investments in automating and simplifying the elements of the VM lifecycle represent a significant opportunity for all companies to increase operational efficiencies and reduce the total costs for this essential function,” wrote Derek Brink, vice president and research fellow for IT security at AberdeenGroup in a Sept. 9 Enterprise Systems article.

Brink and Aberdeen Group reported in Sept. 2008 (*Vulnerability Management: Assess, Prioritize, Remediate, Repeat*) that vulnerability management makes up about 14 percent of the average IT security budget. Those deemed Best-in-Class by Aberdeen reported a marginal return of over 90 percent on those investments. In other words, for every \$1.00 a “Best in Class” organization spends on the VM-related investments, it is able to avoid \$1.91 in VM-related costs. On average, organizations are able to reap the advantages of their Vulnerability Management solutions with a payback period of 15.4 months.

A combination of agent-based and network-based scanners is a best practice scenario for assessments. Agent-based scanning provides better insight into individual computer nodes connected to a network. Agent-based scanning is also better from a scalability perspective. With mobile devices becoming common in the workplace, agent-based scanning is the best way to optimize and look into these devices, even though they are further away from the network. Network-based scanning gives insight into all visible network components and systems. Therefore, by combining both scanning techniques, an organization can be assured they are identifying all of the vulnerabilities within their network.

Within each vulnerability assessment program, the most advantageous way to guarantee vulnerabilities are identified, is by defining the system configurations within the assessment. Since over 65% of vulnerabilities are due to mis-configurations, i.e. configuration errors and lapses by IT administration, these can be immediately identified and remediated.<sup>8</sup>

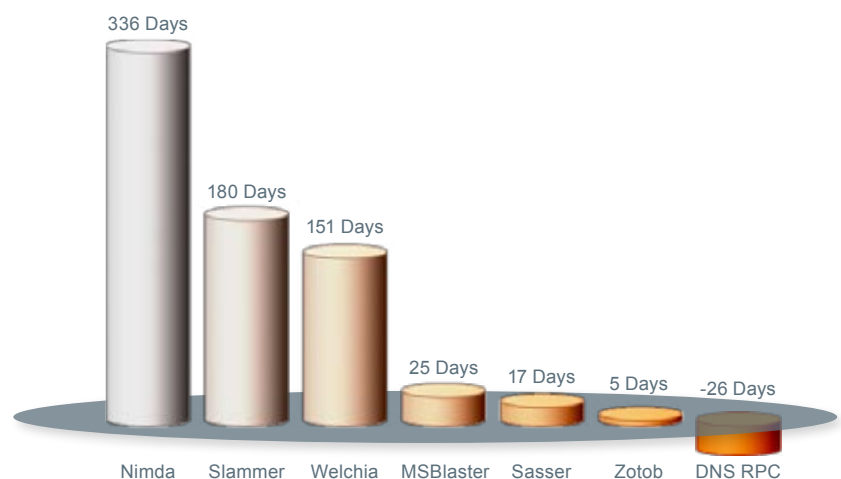
# Minimizing Security-Related Total Cost of Ownership

## Patch & Remediation

Due to the countless vulnerabilities threatening organizations each day, patching and remediation are skills every IT professional knows well. The deployment falls on the shoulders of the IT department to deploy and remediate each patch, from each vendor, for each application and operating system. When it isn't done right, it has the potential to eat up a lot of man-hours.

One of the largest cosmetic companies in the world, Shiseido was able to save over \$100,000 in IT salaries and benefits simply by streamlining its patch and remediation efforts through the use of Lumension Security products. Before Lumension, Shiseido lacked the tools to enforce policies and automate patching and reporting throughout its desktops and systems. PCs were often introduced by local IT administrators across 10 sites, and maintaining these PCs was time consuming. Additionally, IT staff was consumed during the morning hours with worm and virus issues, caused by missing patches on nodes. This problem was draining IT resources and reducing the organization's ability to stay compliant with their regulations. After deciding they needed an automated vulnerability management system, Shiseido was able to install and deploy the entire system within a single day. Not only did the automation process save tens of thousands of dollars in payroll, but now IT can react much faster to issues and minimize downtime throughout their network environment. This improvement in time is critical. As the chart below illustrates, criminals are getting better and better at exploiting vulnerabilities once they're found. Businesses must be quick about remediation in order to keep the exploits at bay.

Automated tools alleviate the pressures from the IT department and allow for proactive, best practice procedures to be followed programmatically. An abundance of security-related costs are eliminated within patch management and remediation solutions. Not only is there improved productivity within the IT department, but an organization receives increased opportunity costs.



The reaction period between remediation available and vulnerability exploit is gone. An organization must be proactive.

In a 2007 survey conducted by Lumension Security: <sup>9</sup>

- 39% of organizations spend at least 2 hours every day monitoring security and IT consoles, administrative agents, and updating security policies. If calculated, these organizations are spending at least \$230 per week, or \$11,040 per year, on manual patching.
- 66% of respondents stated it would take them greater than 1 week to deploy a patch throughout their organization.
- 56% of respondents did not have a global strategy. If they did, it was difficult to enforce. Therefore, these organizations are increasing their chances of vulnerabilities being managed.

### Reporting & Compliance

Security and compliance policy standards are implemented to protect organizations and their consumers. These policies force organizations to allocate time and resources for their adherence. In fact, over 67% of all enterprise businesses are subject to regulatory compliance.<sup>10</sup> Manual reporting is not efficient enough, as represented by the 90% of all businesses who still do not have sufficient policies in place to meet data governance regulations and adequately limit the risk of a breach.<sup>11</sup> Organizations must be able to quickly generate relevant reports to regulatory bodies and internal constituents that demonstrate compliance to internal and regulatory policies. Failing to do so costs organizations money.

An organization must be able to quickly and easily identify gaps in compliance, based on regulatory or corporate policies. By completing a proactive assessment, an organization will identify gaps in compliance, prior to external audits, ensuring a constant audit-ready posture and ensures no fines are incurred due to non-compliance.

This could save an organization thousands in fines and sanctions. For example:

- ▣ The cost of PCI non-compliance can range from \$5,000-\$25,000, monthly.<sup>12</sup>
- ▣ The U.S. Department of Health and Human Services (HHS) recently levied the first penalties against a healthcare agency for HIPAA security and privacy non-compliance - a six-figure settlement related to the loss of 386,000 patients' personal health information.<sup>13</sup>

Though auditors want to verify the integrity and security of data, they want to see, “policies that describe how an organization will provide security and integrity; proof that the policies have been operationalized; and evidence that the organization can discover and fix policy compliance lapses.”<sup>14</sup> Since organizations have budgets allocated for their compliance, they can also reduce the cost of compliance reporting by mapping their vulnerability management policies to control standards. All of these directly align with best practices and decrease TCO.

### Conclusion

Proactive security is no longer a luxury, but a necessity to compete in today's economic environment. Without implementing automated security solutions, IT will continue to spin its wheels to keep up with manual processes that react to threats penetrating networks every day. By investing in the necessary software and automation, IT resources can be freed up to work on strategic initiatives that drive profit to the bottom line.

The cost savings are profound. Today, the average organization must reimagine 85% of its laptops and desktops each year due to malware.<sup>15</sup> Earlier, we showed how a typical organization was spending \$250 per endpoint to do this, plus an extra \$150 each in indirect costs related to end-user inefficiencies. For a mid-size organization of 500, this equates to \$212,500 that could be shaved off from the TCO each year by instituting better endpoint management practices and technology.

Proactive security also reduces costs related to security-related downtime. The typical reactive organization experiences an average network downtime of 23 people annually. When the average daily cost of an employee is \$185, this calculates to \$1,021,200 of inefficiencies every year. In the event malware intrudes a network environment, the average time to achieve full recovery is an additional 31 person days, or \$1,376,400.<sup>16</sup> As stated earlier, indirect costs could create ramifications that would double these figures when calculating TCO.

These viable resolutions to decreasing direct and indirect costs are accomplished within Lumension Security's solutions. By adopting Endpoint Protection, Data Protection, Vulnerability Management and Reporting and Compliance, an organization can proactively secure the network environment and immediately begin reducing TCO. And, an organization can rest assured that your security is never neglected and your organization is always retaining an 'always on' security posture.

### Who is Lumension Security?

Lumension Security develops, integrates and markets security software solutions that help businesses protect their information, network and endpoint assets. Lumension focuses on establishing a low TCO, with minimal impact on production environments. Companies require effective security to meet the rising and evolving threats to their mission critical data and systems. Lumension integrates operational security management, with proactive endpoint threat protection, and control. By utilizing a proven whitelisting security model and employing both network and agent-based vulnerability management technologies, an organization is protected through an 'always on' security posture. Lumension's approach enables companies to meet the increasing requirements to protect their data without impacting the productivity of their employees.

#### SOURCES:

1. Hughes, Lauren, & Lipsitz, Jonathan. (2007, September 10). The Total Economic Impact of Lumension Security's Sanctuary Application And Device Control. Forrester Consulting, pp 18.
2. Hughes, Lauren, & Lipsitz, Jonathan. (2007, September 10). The Total Economic Impact of Lumension Security's Sanctuary Application And Device Control. Forrester Consulting, pp 14.
3. (2008, August 5). Gohring, Nancy. Security Oversight May Have Enabled Countrywide Breach. Washington Post.
4. Hughes, Lauren, & Lipsitz, Jonathan. (2007, September 10). The Total Economic Impact of Lumension Security's Sanctuary Application And Device Control. Forrester Consulting, pp 18.
5. (2005). 2005 National Survey on Data Security Breach Notification. Ponemon Institute.
6. (2005). 2005 National Survey on Data Security Breach Notification. Ponemon Institute.
7. (2007, February). Taking Action to Protect Sensitive Data, Benchmark Research Report. IT Policy Compliance Group.
8. Pescatore, John. Gartner Research Group.
9. 2007 PatchLink Customer Survey. 250 CIOs, CSOs, IT managers and network administrators across Europe, Asia Pacific and the U.S.
10. Yankee Research Group. <http://www.yankeegroup.com>
11. IT Policy Compliance Group. <http://www.itpolicycompliance.com/>
12. PCI Security Standards Council. <https://www.pcisecuritystandards.org/>
13. (2008, September 17). Nash, Randy. HIPAA privacy regulations get some teeth: Be prepared. <http://www.searchsecurity.com/>.
14. Kavanaugh, Kelly, & Nicolett, Mark. (2008, June 2-4). Managing Security Information and Emerging Vulnerabilities. Garnter IT Security Summit.
15. (2005). Yankee Group Security Leaders and Laggards Survey. Yankee Group.
16. (2005). Yankee Group Security Leaders and Laggards Survey. Yankee Group.