

## WHITE PAPER

---

# Novell's Secure Desktop Solution: A Modern-Day Marriage of Business Benefit and Risk Reduction

Sponsored by: Novell

---

Randy Perry  
Eric Hatcher  
May 2008

Christian A. Christiansen

## EXECUTIVE SUMMARY

The increasing mobility of the modern workforce and the competitive requirement to optimize that workforce with mobile communications and information have greatly increased the complexity of the IT department's mission. In addition, the more demanding governmental requirements for information control and reporting have exacerbated the need for information control and security best practices. Business assets on the road deliver added value, but they are also more vulnerable to attack and loss. Companies are seeking to deal with the increased vulnerability, and many companies are turning to integrated security solutions such as the Novell Secure Desktop Solution. ZENworks tools — Configuration Management, Endpoint Security Management, Asset Management, and Patch Management — in combination with good security practices not only provide a more secure and controlled IT environment but also deliver real business value. In this paper, both types of benefits are discussed. For this study, IDC quantified security benefits and conducted a cost-benefit analysis to calculate the real return on investment (ROI) companies are realizing from deploying ZENworks solutions.

The Novell Secure Desktop Solution is a combination of three products:

- Novell ZENworks Endpoint Security Management
- Novell ZENworks Patch Management
- Novell ZENworks Asset Management

## INTRODUCTION

---

### **Increasing Complexity of the Corporate Security Program**

Traditional security is no longer good enough because complexity is increasing significantly. Traditional IT security was formerly provided by firewalls, antivirus solutions, and other security products. Such measures worked fine when security was defined around known threats and well-defined perimeter defenses.

Now, a comprehensive security strategy must deal with the increased vulnerability of mobile assets and a threat environment that is smarter and more aggressive, organized, focused, and profit oriented.

### ***Laptops Outsell Desktops***

In the consumer market, as well as in Europe and Japan, laptop unit sales already outpace desktop sales. In 2008, IDC expects North American businesses to buy more laptops than desktops. This exacerbates data protection issues when laptops and other mobile devices are lost or stolen, are used to download unauthorized content/applications, and are attached to corporate applications through numerous public and private networks that are secured lightly or not at all.

### ***Locally Stored Data Exceeds Server-Stored Data***

A primary requirement for enabling user mobility is providing remote access to data. This is most often achieved by storing data on laptops or portable devices. As content creation, messaging, and personal storage increase because more storage capacity is available for less money, locally stored data will sharply exceed server-stored data. In many cases, this local data contains sensitive information that is subject to corporate and/or regulatory compliance, including customer data and intellectual property. However, the user of the mobile device may be unaware of the sensitive nature of this data and uncaring or ignorant about corporate policies.

### ***Wireless Networks Are Outpacing Wired Networks***

Increasingly, endpoint devices contain multiple network connections (e.g., Wi-Fi®, cellular, Ethernet, Bluetooth®). In most cases, neither the devices nor the users exercise any control over the networks they use. For the most part, they blithely ignore any security warning about insecure "free" Wi-Fi® networks, public hotspots, and insecure transmission of sensitive data. Many users are not aware of the risk associated with insecure wireless networks, or they ignore the warning for the sake of convenience.

### ***Smartphones***

Smartphones are getting more wireless connections (e.g., cellular, Wi-Fi®, and Bluetooth®), application processing capabilities, more memory, and substantial storage capacity (for music, video, and other applications). Moreover, these devices increasingly contain larger lists of business contacts, more application data, and greater levels of access to sensitive corporate data. Even though device management can remotely disable access, wipe the device's data, and kill the device, users often fail to notify IT in a timely manner when they lose the device. While some managers scoff at data exposure associated with smartphones, anybody who loses a device does not want a stranger looking at the device's data or using it in his or her name. This risk is even higher when devices are not owned and controlled by organizations but are still used by employees to access and store sensitive data. When these personal devices are lost or stolen, organizations may not have any record of the data stored on the devices or even be aware of the theft or loss of the devices.

**Bottom Line**

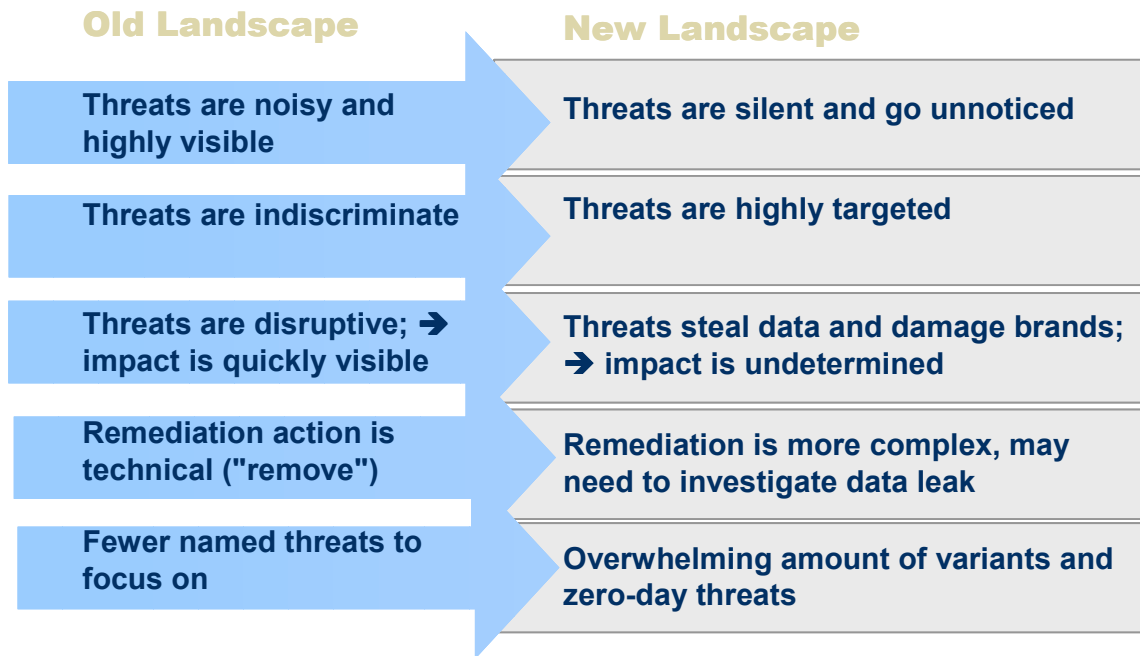
Perimeter security and antivirus solutions are necessary, but insufficient to address some of today's threats. Today, attacks are coming from multiple sources that must be addressed directly on the endpoint. Mobility jeopardizes corporate data because users are connected to insecure wireless networks, and data is not protected while it is "at rest" in the devices or "in motion" when it is transmitted. Despite all this, IT increasingly has to acquiesce to users' mobility demands, turning IT into a blind target.

**Threats and Security Issues**

Figure 1 illustrates the external threat landscape, which focuses on targeted attacks.

**FIGURE 1**

External Threat Landscape Focuses on Targeted Attacks



Source: IDC, 2008

In the past, security for data protection that focused on servers and antivirus solutions was adequate to dismiss desktop problems. This was a workable solution when most attacks were "pray and spray" or indiscriminate experiments largely tied to the vanity of the exploit writers. Many attacks were badly written and often created chaos because the code's execution was unpredictable.

### ***Silent and Unnoticed***

Current attackers are no longer interested in vanity. Because these attackers are profit driven and want to continue exploiting compromised sites, the threats are silent and often go unnoticed. The situation is akin to robbing a bank of \$5 million and fleeing to another country versus embezzling or skimming \$1 million every year for 10–20 years. The payoff is longer, but the risk is considerably lower because these criminals may never get caught and the victimized company may never acknowledge the attack(s).

### ***Highly Targeted***

Past attacks were nonselective. Now, threats are carefully targeted. Attackers are well-funded criminal, industrial espionage, and government agencies. These organizations intensively research their targets and develop a comprehensive list of the targets' vulnerabilities and incident response strategies. They will survey all the remote sites and partner networks that have authorized access. To test systems, they will run mock attacks in cooperation with other criminal partners. They will also use social attacks to gain access to privileged account names and passwords. When necessary, they will co-opt employees with bribery and/or blackmail. In other words, attackers consider this a for-profit business, but they are not bound by legal or ethical concerns.

### ***Steal Data and Damage Brands***

Past attacks focused on credit and debit card numbers to purchase high-value products (e.g., gas plasma TVs, laptops, servers) or rapidly withdraw money from automated teller machines. This is still a popular activity, but recent attacks are focused on information that can be resold many times to identity fraudsters, phishers, spammers, industrial espionage, and even certain government agencies.

### ***More Complex Remediation***

Because these criminal organizations are so secretive and their methods are so sophisticated, the attacks may go undetected for months or years. This makes damage assessment a very difficult project. Because the extent is unknown, the attacked company must notify customers even when there is only a slight chance they were affected. The notification and remediation process ranges from \$100 to \$200 per customer record. This can result in costs of tens or hundreds of millions of dollars, not counting the internal forensics and corrections. Although governance varies by state and regulatory bodies, these notifications can be avoided if the data is protected with at least 128-bit encryption or the breach is avoided. Considering the need for notifications, this alone can save an organization millions of dollars.

### ***Variants and Zero-Day Threats***

Using automated scanners, botnets, and partner networks, criminals continually create new variants of attacks. In many cases, they are probing and cataloging vulnerabilities for more targeted attacks at a later time. Within the threat environment, some groups focus on just this data collection activity. They sell the information to other entities who may exploit it directly and refine it even further for very tightly targeted attacks on a specific company or even down to a named individual.

When the target is very valuable (e.g., high net worth in accessible accounts or intellectual property such as new product designs, source code, etc.), zero-day exploits are built or bought. Because the vulnerabilities associated with zero-day exploits are not public, no signatures are available for defense. In an average security environment, this means that antivirus is not likely to be an effective defense. Since signatures may not exist to address these types of exploits, enforcement has to be broad enough to protect the data accessed by or stored on the device; control network access, including preventing incoming traffic that is not solicited, even when the device is out of the office; and control the settings and states on the system.

Overall, these new attacks can evade "average" security systems. In fact, many security problems now show up first as help desk questions concerning poor desktop performance, not security. This indicates a need for a synergistic approach that combines desktop security and management in a coordinated reporting and management system.

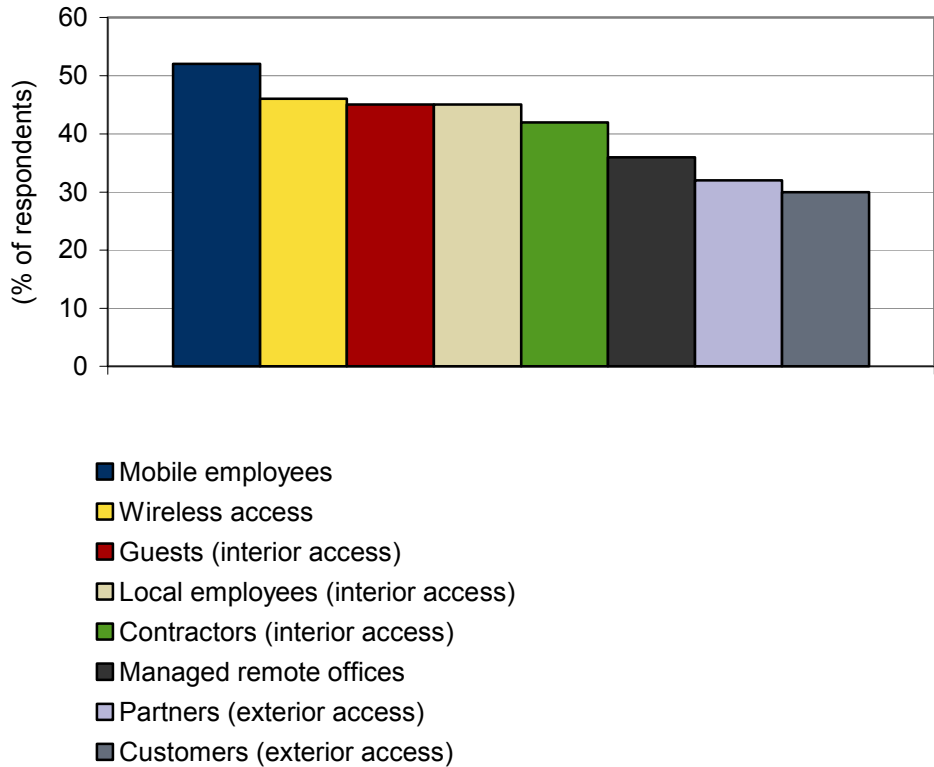
---

### **Top User Security Concerns**

As Figure 2 indicates, mobile employee security is a top concern of 52% of surveyed respondents. IT departments worry about stored information that can violate privacy compliance laws and unauthorized access to corporate networks and applications. The latter reason also factors into 46% of respondents fearing uncontrolled wireless access, including the interception of data in motion as it moves from the laptop (or smartphone) through nonsecured/public networks. Interior access by guests and local employees causes fear among 45% of respondents.

**FIGURE 2**

**Top User Security Concerns: Mobilization and Extended Perimeter**



Source: IDC, 2008

***Extended Perimeters and Managing the Unmanageable***

Fear of extended perimeters is shared by roughly one-third of the respondents. These perimeters go beyond corporate boundaries and firewalls to extend privileged access to consultants, contractors, customers, and partners. In some cases, these individuals may have more access to sensitive corporate data and applications than the actual employees. Managing the security of extended perimeters is difficult because corporate IT departments may have only loose control over the client operating system and applications, network connections, and user behavior. This leads to a situation where IT has to manage the unmanageable.

***Insider Threats***

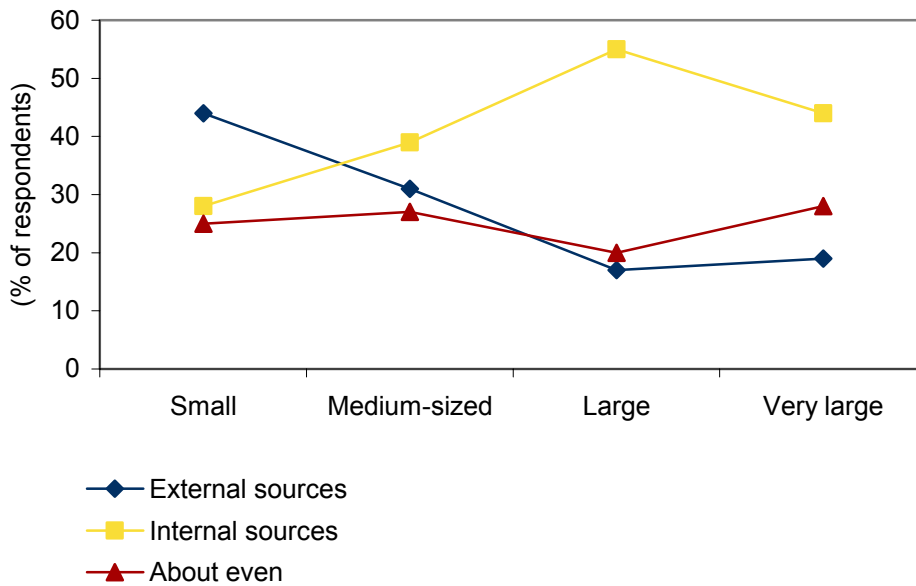
Insider threats are overshadowing external threats at many businesses. Over the past several years, IDC surveyed respondents about internal threats versus external threats. There has been a trend for increasingly smaller companies to take internal threats more seriously. As shown in Figure 3, this trend culminated in medium-sized companies (100 to 1,000 employees) now assigning equal threat ratings for internal

and external sources. Based on past trends, we expect medium-sized companies to assign greater risk to internal sources. The crossover point will move down to small companies (2 to 99 employees), which will place an even greater emphasis on securing employees against security risk, compliance violations, and leakage of sensitive data.

**FIGURE 3**

**Internal Threats Versus External Threats**

Q. *Do you believe that the most serious threats to your company's enterprise IT infrastructure originate from internal or external sources?*



Source: IDC, 2008

**Compliance**

Figure 4 illustrates just a few U.S. privacy and security laws. In addition, almost 40 states have consumer privacy laws that must be addressed if customer files are breached. This figure does not include international legislation, which should also be considered. As examples, most European countries have strict consumer privacy laws and Japan has enacted legislation for financial governance.

Multinational corporations face an overwhelming list of worldwide regulations. To begin solving this problem, they are examining the overlap in regulations. They map these overlapping requirements to products and services that can satisfy all or part of the regulations.

**FIGURE 4**

Privacy/Security Laws, Bills, Standards, and Guidelines

**Banking and Finance**



**Gramm-Leach-Bliley  
SEC 17A-4  
USA PATRIOT Act  
Check-21  
SANS Top 20**

**Healthcare and  
Pharmaceuticals**



**HIPAA  
21 CFR Part 11  
Sarbanes-Oxley**

**Services and Retail**



**Gramm-Leach-Bliley  
California SB-1386  
Credit Card PCI**

**Government**



**FISMA  
USA PATRIOT Act  
Paperwork Reduction  
Cybersecurity Enhancement**

**Telecommunications**



**CALEA  
USA PATRIOT Act  
e-Signature Act  
Sarbanes-Oxley**

**Utilities and Manufacturing**



**Sarbanes-Oxley  
HIPAA  
ISO 17799  
FERC/NERC**

Source: IDC, 2008

***Loss of Data***

News of security data breaches seems to be an almost daily occurrence. Successful attacks target university alumni lists, retailers, financial services organizations, and many other corporations. Figure 5 illustrates some of these incidents.

Less well known is the LGT Group breach. A former employee of this Liechtenstein private bank is alleged to have sold stolen customer data to tax authorities in Europe, the Americas, and Asia/Pacific. Formerly, criminals did business only with other criminals. The LGT breach, however, seems to create new and possibly legitimate markets for stolen data. This could set a dangerous precedent for corporations on a worldwide basis.

**FIGURE 5**

Major Data Security Breaches

**Security Breaches**

<b>LGT Group</b>	2002–2008	<b>stolen:</b> Liechtenstein private banking data sold to other government tax authorities
<b>TD Ameritrade</b>	Sep 2007	<b>stolen:</b> personal data for <b>6.3 million people</b>
<b>GAP Inc.</b>	Sep 2007	<b>stolen:</b> personal data for <b>800,000 people</b>
<b>Monster.com</b>	Aug 2007	<b>stolen:</b> personal data for <b>1.6 million people</b>
<b>Fox News</b>	July 2007	<b>stolen:</b> personal data for <b>1.5 million people</b>
<b>TJX</b>	Jan 2007	<b>stolen:</b> credit card details for <b>94 million people</b>
<b>CardSystems</b>	June 2005	<b>stolen:</b> credit card details for <b>40 million people</b>

**Data Lost in Transit**

<b>U.K. government</b>	Nov 2007	<b>lost:</b> personal data for <b>15 million U.K. citizens</b>
<b>ACS</b>	Mar 2007	<b>lost:</b> personal data for <b>2.9 million people</b>
<b>CitiGroup</b>	June 2005	<b>lost:</b> personal data for <b>3.9 million customers</b>
<b>Bank of America</b>	Feb 2005	<b>lost:</b> SS numbers for <b>1.2 million customers</b>

Source: Privacy Rights Clearinghouse and *The Wall Street Journal*, 2008

**Moving Beyond Viruses, Trojans, Worms, and Malware Attacks**

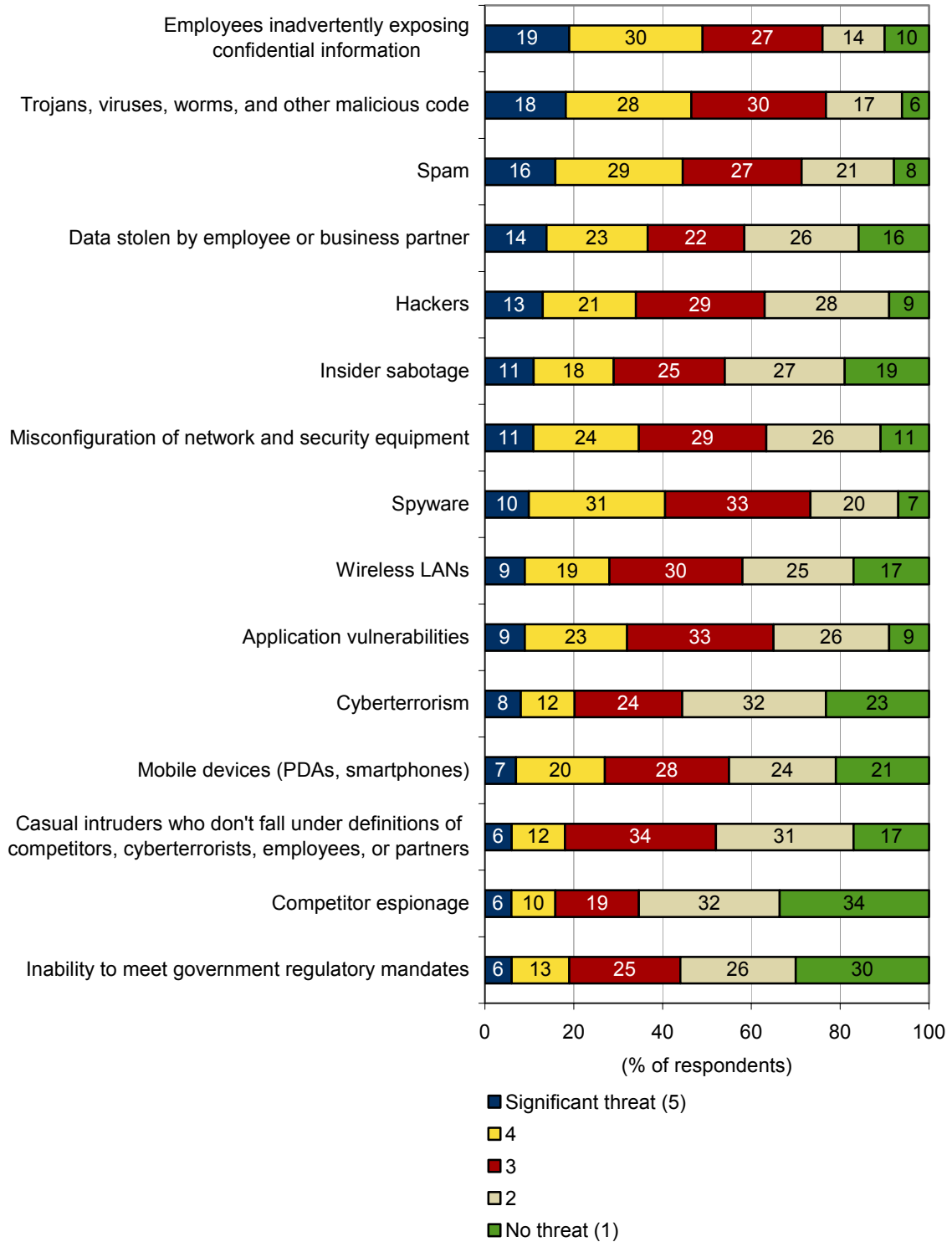
Figure 6 echoes customers' concerns about insider threats. For the first time in five years, malicious code protection (e.g., trojans, viruses, worms) was bumped to second place by "employees inadvertently exposing confidential information."

Moreover, other internal threats are also noted, such as "data stolen by employee or business partner" and "insider sabotage" from disgruntled individuals in the fourth and sixth spots.

At the bottom of Figure 6 is a data point that always raises customer questions. "Inability to meet government regulatory mandates" always causes people to ask, "Isn't this a number 1 priority?" When talking with CXOs and senior management, we find that compliance is their most important security issue. However, the IT respondents to this survey are focused on the root causes of compliance failure. In practically all cases, a compliance violation is caused by an insider.

**FIGURE 6**

Threats to Companies' Enterprise Network Security



Source: IDC, 2008

## Effect of Endangering Customer Confidence

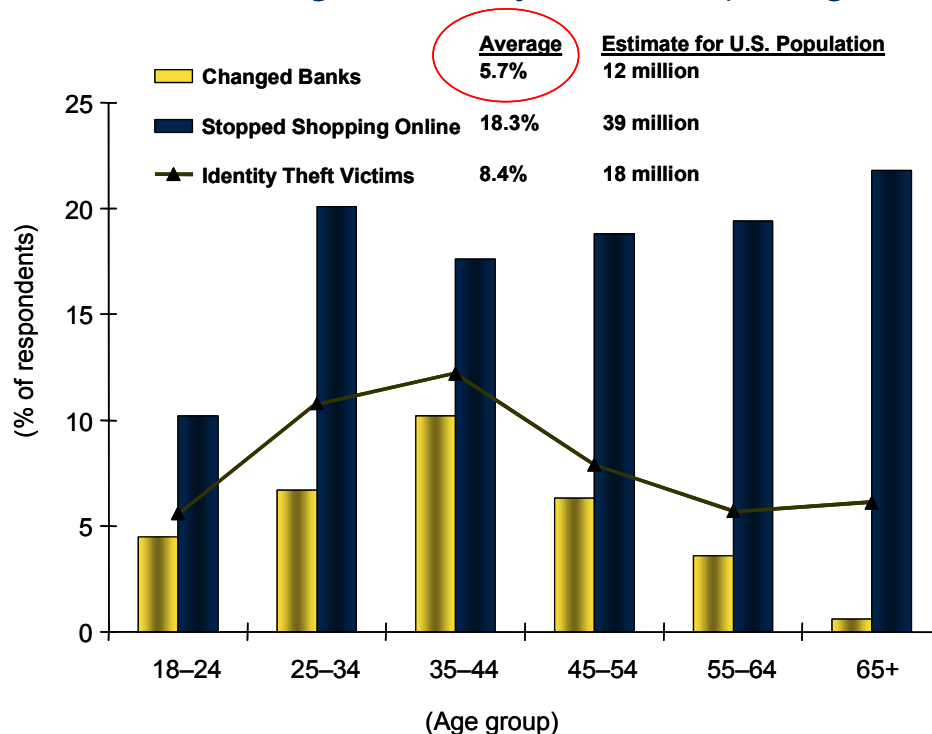
A few years ago, Financial Insights, an IDC company, conducted a survey that showed customer reactions to a data breach. Roughly 6% of financial services customers said they would change banks (see Figure 7). The greatest impact was in the 35- to 44-year-old age group. We believe that customers in this age group actively use online banking, hold considerable assets, and recognize security issues. For more mature customers (55+ years old), the low incidence is reflected by their limited use of online banking and their long-held loyalty to certain banks.

In the retail area, over 18% of respondents said they would stop shopping online. For retail, the distribution of the age group was roughly equal. We believe that customer loyalty to online retailers is just starting to rise. Customers still factor trust in known online retailers against lower prices from lesser known stores.

**FIGURE 7**

Banking and Retail: Reputation Risk Carries Big Consequences

**Customers don't care where or how the breach occurred; they take action to mitigate identity theft risk (change banks)**



n = 1,000

Source: Financial Insights Consumer Banking Survey

## 2008 Customer Priorities

Figure 6 highlighted customers' changing perceptions. Table 1 looks at future priorities. Not surprisingly, malware protection now falls into third place behind issues related to data leakage protection (DLP) — specifically, "unauthorized internal/external network access" (by endpoint devices; desktops, laptops, smartphones, and other network capable devices such as MP3 music players) and "data security and intellectual property protection."

**TABLE 1**

2008 Customer Priorities

Priority Items	% Responding
Unauthorized internal/external network access	81
Data security and intellectual property protection	74
Malware protection	68
Control unmanaged devices	58
Policy management and enforcement	57
Ensure endpoint compliance	53
Improved network health	52
Meet regulatory requirements	50

Source: IDC, 2008

Data security and intellectual property (IP) protection is also growing in importance. Over the past year, IDC analysts have heard more emphasis on IP protection. One company that manufactures wallboard (also known as sheetrock) worried about losing its business to foreign competitors if its proprietary manufacturing machine designs and the associated source code were leaked. Likewise, a midsize manufacturer of microwave antennas also worried about disclosure of new designs and engineering secrets.

These fears are also related to controlling unmanaged devices. As mentioned previously, IT worries about "managing the unmanageable." While these problems are mostly associated with people, they are also applicable to unmanaged devices such as factory-floor process controllers and supervisory control and data acquisition (SCADA) systems. These unmanaged devices often run very old operating systems and applications. Originally hardwired into control systems, SCADA systems have been quietly networked over the years. They cannot be patched or subjected to

network probes because they will fail. In these environments, failure is intolerable because critical processes will shut down (e.g., manufacturing lines, municipal water purification and waste treatment, refinery systems). Therefore, these systems need protection from internal and external attacks regardless of whether they are accidental or targeted.

---

## **Benefits of a Secure Environment**

**Optimizing IT operations.** For highly successful companies, optimizing IT operations is about getting multiple, synergistic benefits from all solutions. This means endpoint security works with desktop management and asset management systems. Multiple risks (e.g., security, patches, client configuration, external storage of data) are centrally managed. This provides IT with the agility to quickly make changes when a new exploit appears, boosts its productivity because it can manage large numbers of clients remotely, and provides consistency in policy enforcement.

**Delivering secure services.** Asset management is not thought of as a security tool, but a U.K. customer says that "[it] identifies potentially harmful or malicious software." Endpoint security ensures that clients attach only to the correct networks, as authorized by IT. However, a flexible policy enables laptops to connect to properly configured home networks. Patch management ensures that software is protected from vulnerabilities. All these client activities happen with little or no user interruption and minimal load on the client machine. This reduces help desk calls and possibly lengthens the PC amortization cycle.

**Meeting compliance demands.** Compliance often means satisfying local, state, federal, international, and industry regulations, but it also includes internal regulations. For example, IT organizations focus on software license management to avoid issues with auditors and violations of vendor contracts.

**Minimizing risks to the business.** Business risk is a swirling tornado. It includes security, compliance, business continuity, and many other issues. Targeted monitoring and enforcement can address specific issues without disrupting the user or the IT organization. This maximizes productivity for both IT and the end user. Security decisions are centrally defined, monitored, and enforced by IT experts for the entire organization. Monitoring cannot be circumvented, but policy enforcement can be adjusted by organizations and individuals to balance risk against convenience.

## **NOVELL'S APPROACH TO DESKTOP SECURITY**

Desktop security is often a contradiction in terms. Users complain to the help desk about poor application performance, long boot times, slow Web access, and strange activities, but they are more concerned about getting their PCs to "act normal" than discovering the actual cause of the problems. Their attitudes toward PCs are similar to most people's attitudes toward their cars — most people just want reliable functionality. They only want simple explanations when costly elements fail, and rather than understanding the complex nature of the issue, they simply want to be returned to normal operation.

When these types of issues occur, the help desk often realizes that security is only part of the problem. While infections with malicious code (malware) are a prevalent problem, sometimes the issues are related to misconfigurations, required patching, or other issues caused by the user. Any of these issues may become apparent only because they slow down performance or interfere with legitimate applications.

Legitimate downloads may also conflict with corporate system images (operating system and application configuration installed as a corporate standard desktop configuration). These untested and unauthorized applications (e.g., music players, digital photography, games, instant messaging) may also consume scarce CPU, memory, disk, and network resources, causing legitimate applications to run slowly.

Therefore, we believe that Novell's approach to desktop security is a holistic approach to managing these intertwined desktop problems. Before connection is permitted to a corporate LAN, endpoint security closely examines a client machine to see if it might infect internal networks and prevent infections that are targeted at the machine. This prevents the spread of malware to other corporate assets. Patch management automatically updates software to prevent vulnerability from being exploited by malware. It also fixes operating systems and application problems that may cause performance issues. Asset management monitors the corporate system image, potentially blocks unauthorized applications, and reports on possible conflicts.

The Novell Secure Desktop Solution is a combination of three products:

- Novell ZENworks Endpoint Security Management
- Novell ZENworks Patch Management
- Novell ZENworks Asset Management

---

## **Novell ZENworks Endpoint Security Management**

This product offers IT departments the ability to create, monitor, and enforce endpoint security policies. Its capabilities include:

- Data encryption.** Locks down desktop and laptop data, prevents privacy breaches, and often eliminates the need for privacy disclosures if the equipment is lost or stolen.
- Wireless security.** Policy-based enforcement for the proper usage of wireless network connections (e.g., Wi-Fi®, cellular, Bluetooth®) to prevent interception of data in motion across compromised networks, including the automation and enforcement of virtual private network (VPN) clients (traditional or SSL) when the device is remote.
- Personal firewall.** Protects the device against inbound attacks and prevents unauthorized application (e.g., worms, trojans, viruses, bots, and malicious code) from outbound communications of confidential data and propagation of threats.

- ☒ **Alerts monitoring.** Notifies administrators and users when users are violating policy. Gives IT the options to monitor, notify the user, block the user, and remediate. This flexible approach provides IT with a range of options for different types of users and behaviors.
- ☒ **Client self-defense.** This capability keeps users from hurting their clients and themselves. Even if users have administrative rights to their PCs, endpoint security will not allow users to disable or remove protection on files, registries, drivers, processes, services, and the application's uninstall.
- ☒ **Application control.** In conjunction with location awareness, automatically launches the VPN whenever the PC is remote from the office. Transmitted data (especially over insecure wired or wireless networks) is fully protected against interception. This automates a process that users often ignore and ensures data privacy. Both traditional and SSL VPN clients are supported. Additionally, endpoint security can block applications from execution. Using the capabilities of asset management to identify the applications that should be blocked, endpoint security can provide the enforcement to ensure that they are not usable.
- ☒ **Integrity/posture.** Independent of geographical location or connection status (e.g., connected to a secure corporate network, partially secure home network, insecure Wi-Fi® hotspot, or not connected at all), client security is continuously enforced. Routine tasks are always required, such as antivirus, firewall execution, and Windows patching. Failure of the machine to maintain a secure state can invoke quarantine with limited access until remediation occurs.
- ☒ **Port control and USB security.** PC ports and devices (e.g., USB, Ethernet, Wi-Fi®, cellular, printer, keyboard) are controlled by location-aware policies to ensure that Wi-Fi® and cellular are not used in the corporate office to prevent multihoming or backdoor access into the network. USB ports are controlled via software. Also, USB storage devices (e.g., thumb drives, iPods, external disk and optical drives) can be completely disabled or enforced as read-only. For customers that don't want to block access, data transfers to devices can require encryption and implement it automatically. Full monitoring is also available to track the usage of USB devices, including what is written to or accessed from these devices. This is very useful in monitoring and/or preventing accidental and deliberate data disclosures.

Given that security is always difficult, IDC found that the primary financial benefit was a 7% increase in mobile user productivity by automating policies for secure wireless usage for road warriors.

---

## **Novell ZENworks Patch Management**

Patching is critical to security. This product provides customers with an automated proactive system for fixing security vulnerabilities before those weaknesses can damage organizations. Because most enterprise PCs run custom system images composed of multiple vendors' software, a patch management solution needs to:

- ☒ Collect all patches from all vendors at all times (regardless of release cycle)
- ☒ Assess patches' applicability to a customer's specific PC environment

- ☒ Determine the criticality of a patch relative to the vulnerability's severity and customers' priorities
- ☒ Deploy the patches in phases to limit risk from patches that are incompatible with a customer's environment
- ☒ Monitor and enforce patch installation, especially for mobile users who infrequently update
- ☒ Report compliance with corporate and/or regulatory policies

Novell ZENworks Patch Management provides automated vulnerability patching for heterogeneous clients. Although patch management reduces administrative overhead and improves security, the major benefit was reducing user downtime by 25–50%.

---

## **Novell ZENworks Asset Management**

Knowing the numbers and status of IT assets is the backbone of establishing a secure environment. ZENworks Asset Management provides the customer with a full view of its IT resources from a single console. It contains two components:

- ☒ **Asset Inventory.** This feature set collects and organizes hardware system information, software products (packaged, proprietary, and legacy), and network discovery (uses network protocols such as SNMP/WMI to identify devices with or without agents) to help ensure the identification of all systems.
- ☒ **Asset Management.** This feature set performs usage tracking (e.g., local, network, thin client, Web), software license management (tracks license, reconciles license with usage, and monitors system image for potentially unwanted and/or malicious software), and contract management (software and hardware support/maintenance contracts, key dates and terms, and supporting documents).

With an accurate accounting of the company's hardware and software licenses, IT can track the status of all equipment to ensure a standard level of security and compliance. There are no unaccounted PCs or servers or duplicated licenses. When a request for a new license or new machine is made, the IT department checks the request against what it has in stock. Thirty-five percent of financial benefits came from cost reduction.

As Table 2 indicates, the Novell Secure Desktop Solution covers a broad variety of generic compliance requirements. While full compliance with specific state, federal, and international regulations along with industry requirements (e.g., Payment Card Industry Data Security Standard [PCI DSS]) will need a careful review, the Novell Secure Desktop Solution can provide a series of infrastructure components that are applicable to a broad variety of regulatory situations.

**TABLE 2****Mapping the Novell Secure Desktop Solution to Compliance Requirements**

	ZENworks Endpoint Security Management	ZENworks Patch Management	ZENworks Asset Management
Protect IT assets (network, servers, clients, applications)	X (client only)	X	
Secure customer data (stored and transmitted)	X (client only)		
Run and maintain antimalware	X (client only with partners)	X	
Monitor, test, enforce, and audit security policies	X (client only)	X	X
Restrict, track, and monitor all access	X		

Source: IDC, 2008

To provide an even more robust regulatory infrastructure, the Novell Secure Desktop Solution could be complemented by Novell's Identity Management products. This would produce robust client- and server-side solutions that would be especially useful in managing network and application access. For more information on these products, see Novell's Web site: [www.novell.com/identityandsecurity](http://www.novell.com/identityandsecurity).

## **EVALUATION OF NOVELL'S POSITIONING, TECHNOLOGY, PRODUCTS, AND CUSTOMER BENEFITS**

Novell is well positioned to bridge the gap between desktop management and security. While desktop management and security administrators are often loath to interact, the centralization of many security issues around PCs, laptops, smartphones, and other client devices is forcing a reconciliation. When endpoint, patch, and asset management are combined in a single solution, consolidated administration becomes easier. It is also more efficient to deal with a variety of problems, regardless of whether they originate in the security or desktop management area. The shared threats of data leakage, compliance violations, and redundant problem resolution break down the IT barriers and turn these individual problems into common elements of a shared solution.

As for technology, Novell does a good job of incorporating acquired companies and products into its customer-driven strategies. Its customers rarely fault Novell's products or support. In our experience, Novell builds strategies based on close contact with customers. Its BrainShare users' conference is a highly collaborative forum where customers actively work with Novell to improve its products. We expect that BrainShare will ensure the continuous refinement of the Novell Secure Desktop Solution.

While the following sections detail customer benefits, this section briefly summarizes IDC's key findings. Controlling access to USB devices and insecure wireless networks significantly reduced data leakage of customer data and/or intellectual property. Securing wireless networks also provided benefits in reducing data leakage over insecure Wi-Fi® networks. Likewise, patch management reduced the time an endpoint would be at risk after a new vulnerability was announced.

The business benefit resulted from permitting users to access these capabilities, but to do so within the compliance framework of corporate policy. On the IT side, downtime from malware infections was lessened. Software incompatibility issues were reduced because corporate system images were easier to control. The number of help desk calls decreased because users did not contaminate their machines with unauthorized software.

## QUANTIFYING THE BUSINESS BENEFITS OF DEPLOYING NOVELL SECURE DESKTOP SOLUTION

### Determining ROI and Payback: Overview

IDC interviewed IT managers at seven medium-sized companies (the number of employees ranged from 200 to 7,000) in Europe and North America (see Table 3). These companies have had Novell solutions deployed for an average of 32 months. The companies represent the public sector, media, manufacturing, and technology industries, with stable user populations and an average number of 2,071 users growing at 3.5% annually and an average number of 37 IT staff. In addition to providing secure environments to client users, each company deploying ZENworks Asset Management was responsible for an average of 670 servers running on Windows and Linux platforms. Overall, these companies had a reasonable risk profile. All had centrally managed IT operations and a unified service desk. All companies tended to lock down their desktops and control the applications to which their users had access. On average, their environments were fairly distributed (78% of users per site on average) and fixed, with laptops making up only 30% of supported clients.

**TABLE 3**

#### Demographics

Number of users	2,071
Number of IT staff	37
Number of Novell-supported servers	670
Number of sites	51

Note: IDC interviewed IT managers at seven medium-sized companies in Europe and North America.

Source: IDC, 2008

## **Novell Secure Desktop Solution: Comprehensive Approach to Desktop Security, Asset, and Patch Management**

This study examined the business benefits of the Novell Secure Desktop Solution. IDC interviewed seven companies that deployed Novell Secure Desktop Solution elements:

- ☒ Novell ZENworks Endpoint Security Management
- ☒ Novell ZENworks Asset Management
- ☒ Novell ZENworks Patch Management

Each product group provided a specific set of capabilities to support a secure environment. Integrated by centralized management, the Novell Secure Desktop Solution capabilities provide in-depth defense, securing the endpoint, managing its configuration, and ensuring a heterogeneous client environment is safeguarded from vulnerabilities.

Based on customer feedback, IDC evaluated the impact on security. For each of the products, we quantified the benefits relative to reduced operation's costs and increased productivity (user and IT staff).

### ***Security Benefits and Risk Reduction***

In this study, key benefits realized were greater wireless and USB security, threat protection, and stronger resistance to virus infections.

The wireless safeguards restricted client connections to approved networks. Among the interviewed customers, several IT departments used ZENworks Endpoint Security Management to prevent laptop clients from connecting to insecure wireless networks that are prevalent during travel or required VPN usage when accessing the insecure wireless networks.

### **Controlling Wireless Access**

Setting the wireless antenna to turn off while the client is connected to a LAN is another example of this type of security. Customers used this measure because they reported that many of their users paid little to no attention to the wireless connection while connected to a LAN in the office or hotel room. That oversight left the machine and/or organization's network vulnerable to intrusion. One customer recalled how, in the past, his company did not allow any wireless connections. Removing all wireless connections negatively affects employee productivity, since employees would have lost their ability to use email or Internet when they were remote. As 60% of the customer's users were mobile, enabling secure wireless communications increased overall company productivity by 2%.

## **Managing USB Devices**

The USB security function allows the IT department to determine what, if anything, may be attached via the USB ports to the client. External hard drives and flash memory drives can pose a high risk for companies when sensitive data is present on their machines. These drives can store many gigabytes of information while still fitting in a shirt pocket.

This security feature allows the company to manage USB access, but it also keeps a log of activity. When a security breach occurs, instead of speaking with tens of hundreds of employees to gather information, managers turn to a log generated specifically to track USB activity. They have a detailed trail that identifies all company data and when it was moved via USB.

*"The reason that we chose Novell was that [our] reporting was broken. We couldn't get reports on anything. Say I wanted to find out how many users had correct policy. It would give me an erroneous number. Or if I wanted to say, 'Mr. Smith in Houston, we have noticed that you're copying financial info onto a USB stick, or if someone from finance is taking home records ... see what you can find about that.' Before we had no way of knowing about this. Prior to the deployment of this tool, we would have no way to know. We're increasing security because of this."*

Having insight into what is on the desktop and what users do with their desktops greatly minimizes risks. Companies can avoid compliance risks through controlling the kind of material that is stored on desktops. They might be using illegal software, so by controlling the desktop, companies avoided software licensing fines.

## **Patch Management**

ZENworks Patch Management proved to have considerable security benefits. Automated pretested patching ensured that the majority of systems (89% according to one customer) were protected when a patch alert was issued. Automated pretesting patch deployment prevents conflicts between the current environment and the patch and frees the IT staff from manual tests. Prior to deploying ZENworks Patch Management, one customer experienced an average of 1,000 virus infections per month. That number has been cut to just one infection per month since the deployment. The same customer noted that its firewall was breached approximately 24 times annually. Since the deployment, the customer has seen only one breach per year. Patching reduces downtime.

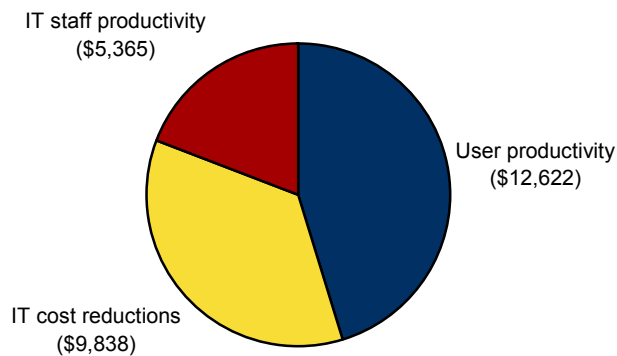
*"It's not a matter of how many we had before, as much as it is how many we're avoiding. It's quite difficult to quantify how many we're avoiding ... if you consider how many different virus updates and vulnerability alerts there are every week. There's probably a couple a week for applications. So by proactively applying those patches, we're preventing ourselves from being vulnerable to security breaches. If I were to guess, maybe we're avoiding a couple a month."*

### **Financial Benefits**

Companies in this study are recognizing average annual benefits of almost \$28,000 per 100 users, with the largest portion coming from increased user productivity (45%). Figure 8 shows the average annual benefits per 100 users.

**FIGURE 8**

Average Annual Benefits per 100 Users



Source: IDC, 2008

### **User Productivity**

The average user in the study was able to recognize 20.6 hours per year in additional productive time. The increased time came from the following annual savings:

- Downtime (PC turned in for rebuild) reduction — 7.3 hours
- Reduced time dealing with software compatibility issues — 4 hours
- Fewer problems dealing with security issues related to patching — 3.5 hours
- Fewer security-related calls with help desk — 2.5 hours
- Fewer firewall breaches — 1.8 hours
- Avoided setup time due to automated software — 1.3
- Fewer virus problems — .2

### **Lost Productivity and ZENworks Patch Management Solution**

ZENworks Patch Management is instrumental in combating the primary causes of lost productivity. Customers reported that their speed in responding to threats that required patching increased greatly. One customer required a full day to rebuild a system and recover all user data after each crash. ZENworks Patch Management enables the IT staff to deploy and repair a problem when users are logged off and unaware of what issue existed. Security intrusions, firewall breaches, and virus infections are common causes of downtime. These events cause machines to break down, which affects user productivity, and on the back end, the machine has to be repaired or restored. One customer in this study said that after installing ZENworks Patch Management, the number of firewall breaches it experienced decreased from 24 to 1 annually. These types of benefits translated into an average 30% user productivity gain due to the lack of downtime.

### **Lost Productivity and ZENworks Asset Management Solution**

ZENworks Asset Management also helps to reduce downtime by identifying dated hardware, server systems, and PCs. Old and outdated hardware is then removed, improving the performance of the total environment and reducing the total hours the company's computers are not functioning.

Asset management gives IT an overall better management platform, which in turn reduces IT staff manual time or physical time of having to chase down a lot of information. Because IT has more time, it can be more proactive, in general.

*"I've been able to get a better planning handle on what equipment we want to roll out; it's now allowed me to put more equipment out on the floor in the production areas. So in that sense, the proactivity has certainly helped alleviate the downtime [because the better planning helps retire the older unreliable machines faster]."*

### **Improved Productivity and ZENworks Endpoint Security Management Solution**

Endpoint security solutions, in combination with security best practices, support increased productive time in the mobile scenario. In an effort to reduce the risk of data theft, companies in the study had not offered mobile communications until the ZENworks Endpoint Security Management created a controlled wireless environment. Wireless connectivity is critical to mobile workers. Most airports and hotels offer only wireless connectivity now. Novell's granular solution offers a lot of configuration flexibility to enable mobile users to access wireless networks while still protecting their corporate network. One participant estimated that its mobile workers were 50% more productive with wireless access and attributed half of that productivity increase to ZENworks Endpoint Security Management. Of course, airports and hotels are a minor part of the story. The real sweet spot for mobile warriors is the ability to do presentations and mobile applications such as CRM while at a customer's premises.

Based on the study's aggregated data, over a three-year period, customers experienced less downtime and fewer performance issues, which led to a \$12,622 annual savings per 100 users.

## **IT Cost Reduction**

Participants in the study experienced an average IT operations cost reduction of \$9,838 annually per 100 users. This direct cost reduction came from the following sources:

1. Reduced/avoided hardware costs
2. Reduced/avoided software costs
3. Consolidation of management tools
4. Reduced IT travel costs
5. Avoided IT staff increase (patching network management, security, and troubleshooting and repair staff)

The ZENworks Asset Management solution is key when considering cost reductions. This solution provides the IT staff with greater control over software licensing and inventory. All of the customers in this study cited the ability to track software licenses as a sizable benefit. In the past, customers would have to choose between doing a lengthy manual check on the number of available software licenses or simply ordering a new license. This usually led to a customer overpurchasing licenses.

ZENworks Asset Management provides a real-time view of the license inventory. At the time of a request, the IT staff can examine the number of available licenses and evaluate the amount of usage for each. If there are licenses with very limited use, or licenses assigned that have not been used in a considerable time, they could be reallocated to users with a greater need for them. The result from these assessments is that IT can move licenses to where it needs them most and avoid a purchase when they are not needed. Companies with this deployment said they saved approximately 2–3% of their total licensing costs by reallocating.

Customers also mentioned a reduction in licensing fines. These companies are now able to see when each license will expire and renew before they receive a penalty.

Companies also reduce their hardware costs. When a request for a new client or server is made, the IT department can check the requesting department's inventory. The inventory report often shows that a department has unused machines that it is unaware of. IT also avoids new purchases by moving machines from a department with available units to the department requesting the hardware.

ZENworks Patch Management reduces costs by trimming the total number of repair visits made to satellite locations. There will always be repairs that require a technician to travel to the site. ZENworks Patch Management's speed and automation protect 89% of one customer's clients from vulnerabilities once they are reported. It was estimated that IT has avoided 30 trips from the home office since the deployment.

In this study, the average customer experienced reduced costs on hardware, software, licensing, and travel of \$9,838 annually per 100 users.

## **IT Staff Productivity**

Each of the companies with the Secure Desktop Solution have increased IT productivity since the deployment. Fewer staff hours are spent investigating the cause of the problems and then repairing the issues. One customer estimated the reduction in time spent rebuilding machines is equivalent to four full-time equivalents (FTEs) per year. Prior to the deployment of Novell solutions, the customer's IT staff spent considerable amounts of time tracking down the point of a security breach. This search would require a technician spending up to 10 hours, according to one interview, scanning many machines to locate the problem. Over time, IT departments viewed this as unreasonable. Now, with Novell's solution, the staff can monitor data downloads and search through the generated logs rather than tens or hundreds of machines and external drives.

The customers in this study witnessed their help desks saving time due to fewer and shorter calls. Fewer calls are made since the number of total incidents is down. One customer saw the number of help desk calls drop by 1,000 over one year and the average call length decline from 30 minutes to 10 minutes. Based on the interview data, customers on average reduced the number of calls to the help desk by 46% annually. ZENworks Asset Management saves the IT staff time because it does not have to search for data in multiple places. Because customers benefit from having a centralized location for their data and have a more orderly workflow, they are more efficient. Customers now have the time to be proactive in their departments.

One IT department increased its machine load by 25% since the deployment, while the number of IT staff remained unchanged.

ZENworks Asset Management helps to reduce the time it takes to conduct an audit. One customer estimated that his company saves approximately 40 hours per audit because the manual tasks are removed. Increased productivity has also improved the internal satisfaction rating of at least one of the customers interviewed in this study. That organization reported that over the five years since it deployed the ZENworks solutions, it has improved its internal customer satisfaction rank each year — and has moved from one of the lowest-rated departments in the company to one of the highest-rated departments.

These IT staff time savings, plus more efficient processes, provide an average of \$5,365 of benefits per 100 users annually.

## **ROI ANALYSIS**

IDC studies of Novell Secure Desktop Solution have always yielded quite high returns on investment. On average, companies invested \$8,381 per 100 users over a three-year period, with 74% of the total investment occurring in the initial year before any benefits are realized. Novell Secure Desktop Solution tends to be quick and easy to deploy, taking from two weeks to 12 months, depending on the number of solutions, deployment practices, and complexity of the environment. Some deployment best practices gleaned from the interviews appear in Table 4.

**TABLE 4**

## Deployment Best Practices from the Interviews

1	For asset management, plan on allotting 50% of the deployment time to collecting all of your company's hardware and software license information and 50% to installation and configuration.
2	Even though the products are easy to deploy, plan on using a Novell partner to support you.
3	Plan on training on the products and build training into the contract.
4	The full range of capabilities of the full-suite version makes it a better bargain than the "lite" version.
5	As a way of reducing initial costs, the Novell products can be run in a virtual environment using an in-house server.

Source: IDC, 2008

Despite the front-loaded investment, Novell Secure Desktop Solution yielded a more than 7 to 1 (726%) return over the three years with an average payback period of 7.5 months.

Table 5 shows the ROI analysis of cash flows discounted at 12% over three years. The ROI equals the net present value (NPV) discounted value of the benefits over the three years divided by the NPV discounted investments over the same time, including the initial deployment costs.

**TABLE 5**

## ROI Analysis per 100 Users

Three-year benefits (discounted)	\$65,795
Three-year investments (discounted)	\$7,965
Net present value	\$57,830
Return on investment	726%
Payback (months)	7.5
Discount rate	12%

Source: IDC, 2008

Payback is viewed from different eyes when evaluating a security solution such as Novell Secure Desktop Solution. For some of the participants in the study, it was all about reducing risk.

"I think it's paid for itself ... I would say yes. We have audit trails that we have to provide. Like I said earlier, we have users that may or may not be copying confidential information to a USB stick or a CD, and we can stop that."

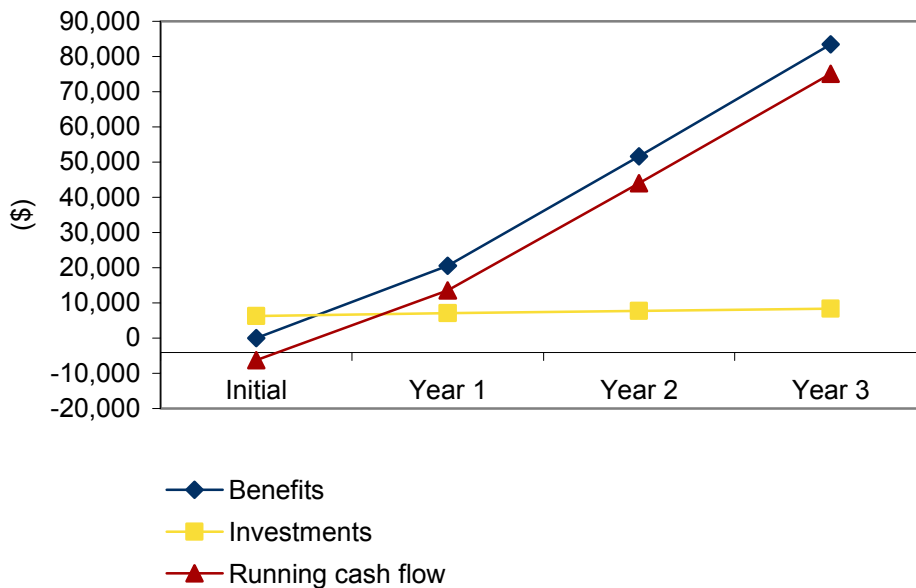
For others, it was about the broad range of benefits from three complete product suites.

"I know that they weren't the only company that we looked at, at the time. They weren't the least expensive company, but they had, for us, the most bang for the buck."

Figure 9 shows the annual cash flow over time. Annual benefits grow at \$27,825 per year, totaling \$83,474 after three years, while investment is less than \$10,000 per year.

**FIGURE 9**

Novell Secure Desktop Solution Cash Flow per 100 Users



Source: IDC, 2008

---

## Methodology

IDC used a three-step process to assess ROI.

First, IDC measured the impact of the solution on the organization. IDC looked at the realized benefits generated by the Novell Secure Desktop Solution by organizing them into the following categories:

1. **User productivity:** The increase in time users have to perform business operations
2. **IT cost reductions:** The savings on hardware and software purchased, savings on repairs due to security breaches, and benefits from hardware consolidation
3. **IT staff productivity:** The increase in time the staff has to conduct activities that support the business (For the Novell Secure Desktop Solution, the majority of these savings came from avoiding patching and repair to clients because of infections or security breaches.)

Second, to calculate the ROI of the Novell Secure Desktop Solution, IDC had to capture the total costs associated with the entire solution. These investments included initial planning and deployment as well as annual operational costs over a three-year period.

IDC ascertained the initial and annual costs of the following:

- Software — costs and licensing fees
- Servers — hardware costs
- IT labor costs — installation and annual maintenance
- Services — training and consulting

Third, IDC forecast investments and benefits over a three-year period and calculated the ROI and payback for the solution. IDC used the discounted cash flow method to calculate the NPV, ROI, and payback period over three years. As a standard, IDC uses a 12% discount rate. This provides a conservative estimate that does not overstate the benefit. IDC evaluated all the investment and benefit information and forecast that data over three years. Three years of forecast data was used, since that is the standard investment cycle for IT departments.

## CONCLUSION

The combination of ZENworks Endpoint Security Management, ZENworks Patch Management, and ZENworks Asset Management reduces administrative costs, improves security, and boosts user productivity. While some of the individual benefits seem small, the sum of the improvements is substantial. Moreover, IT security groups desperately need the standardized policy creation, monitoring, and enforcement that these solutions can provide. This provides a consistent and automated approach to

compliance with internal and external policies and regulations. Moreover, there is a highly beneficial management synergy with knowing what PCs a customer has, how the PCs are configured, when the configurations change, what patches are needed, when the patches are needed, what security policies are in place, and if and where those policies are enforced. Having the answers to all these questions provides a holistic client management infrastructure that is extensible to future mobile devices, networks, management best practices, and compliance regulations.

---

### **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.