Technical White Paper
SYSTEMS AND RESOURCE MANAGEMENT

www.novell.com

Novell® ZENworks® Endpoint Security Management: Total Control from a Single Console

Novell®

Table of Contents:

The Answer to Endpoint Threats

> **“Without a sound endpoint data protection solution in place, organizations are at risk of millions of dollars in losses from misplaced intellectual property and unapproved use of valuable, sensitive data.”**
>
> **Aberdeen Group**
> *“Endpoint Security Strategies Part II: The Endpoint Data Protection Benchmark”*
> December 2006

Many different motives can drive a hacker to attack networked systems. It may be nothing more than the same gratification that drives vandals to destroy property. It may be a professional criminal’s scheme to undermine a competing business, steal identities or even extort money. It may be a cyber-terrorist’s plot to disrupt communications and cause social and economic harm to a perceived enemy. It may be simply “because I can” or any of countless other reasons.

But no matter what the motive, all these attacks share one thing in common: they take advantage of technical vulnerabilities in your network endpoints and/or procedural vulnerabilities in the design or enforcement of your security policies. If there are no vulnerabilities, there can be no successful exploits.

Of course, there’s no way to completely eliminate all vulnerabilities for all time, and the hackers count on being able to stay one step ahead of their prey. The goal, then, should be to identify and remediate vulnerabilities as soon as they’re known, and to meticulously protect the runtime environment, communication ports, removable media and other system components against code and connections that are not authorized and known to be benign. And the real challenge is to provide comprehensive endpoint protection—from core to periphery—without draining the budget or overburdening the IT staff.

Before we discuss the solution, it’s important to put IT staff time and budgets into perspective. According to the key findings of the Ponemon Institute’s 2006 annual study, “Cost of a Data Breach,”[1]

- *Among the 31 companies studied, each security breach cost an average of US$4.8 million in direct costs, lost productivity and missed customer opportunities.*
- *For each customer record that was lost in the security breach, companies incurred an average cost of US$182, a 30 percent increase over the 2005 results.*

From January 2005 until July 2007, nearly 160 million compromised records containing sensitive information were reported lost in the U.S. alone, according to the Privacy Rights Clearinghouse. And, as the Clearinghouse report notes, “In reality, the number … should be much larger. For many of the breaches listed, the number of records is unknown.”[2] U.S. businesses are losing tens of billions of dollars annually due to data security breaches, even by the most conservative estimate.

And things are only getting worse. The number of vulnerabilities is increasing exponentially each year, according to the National Vulnerability Database maintained by the National Institute of Standards and Technology.[3] At the same time, hackers are becoming more sophisticated, exploiting vulnerabilities faster than ever—in many cases before a vulnerability is even known to the general public.[4] As of July 2007, 40 zero-day vulnerabilities had already been disclosed to the public, with four zero-day vulnerabilities still unpatched over periods ranging from two to 20 months.[5]

And if all this talk of hackers isn’t frightening enough, consider this: your biggest security threat is your own end users. They can be sophisticated and malicious insiders trying to steal information or disrupt operations, or well-intentioned employees who don’t understand security risks and how to manage them effectively.

[1] *Ponemon Institute, “2006 Annual Study: Cost of a Data Breach—Understanding Financial Impact, Customer Turnover, and Preventative Solutions,” 2006.*

[2] *Privacy Rights Clearinghouse, “A Chronology of Data Breaches—Posted April 20, 2005, Updated July 10, 2007.”*

[3] *National vulnerability information and statistics can be found at http://nvd.nist.gov/nvd.cfm.*

[4] *See, for example, David Sancho, “The Future of Bot Worms,” Trend Micro, 2005.*

[5] *eEye Research, “Zero-Day Tracker,” http://research.eeye.com/html/alerts/zeroday/.*

To appreciate the security problems associated with authorized users, consider two simple facts. 70 percent of all computer attacks, security breaches and data thefts originate inside the firewall.[6] 53 percent of organizations surveyed say they would never be able to determine what information was at risk if a USB thumb drive or other removable storage device were lost or stolen.[7]

Two New Paradigms: Removing User Control and Redefining the Network Perimeter

But enough scary stuff for now. If you follow the IT press, you have a sense of the threatscape, and if you work in IT you know all too well the potential consequences of a security breach. The question is how do you protect network endpoints to prevent loss, corruption or theft of your knowledge assets—without disrupting the productivity of the users who create those assets in the first place? And how do you ward off security threats when you may not know the potential entry point, or even that a vulnerability exists?

To secure today's diversified and distributed IT environment, two old paradigms need to be radically revised.

First, while you still need to provide end users with all the tools and resources they need to be productive, you must remove the tools and responsibility for managing their own security environments. In simpler times, it may have been sufficient for companies to instruct users to update their own virus definition files and download their own patches. Now, however, the security landscape has become so complex and hazardous that users no longer have the time or expertise to thoroughly secure their own devices. Even if they're fully committed to complying with your security policies, users aren't qualified to understand all the implications of clicking OK in a security application. Moreover, it's unreasonable to expect them to. Security is not their job, and requiring users to deal with it robs their productivity.

Second, you need to move beyond the old-fashioned idea of perimeter security. Information security measures have traditionally concentrated on firewalls, network intrusion detection and other perimeter defenses. While these are still as important as ever, the size, fluidity and complexity of the modern enterprise network demand a far more multifaceted approach.

The whole concept of perimeter security relies on there being a well-defined and controllable perimeter to your organization—for example, a border router where all incoming traffic could be conveniently analyzed for threats. But today, the "perimeter" also includes every device that:

- *Can physically move data from behind your "official" perimeter, such as notebooks, USB drives and MP3 players*
- *Can accept data from (or pass data to) a thumb drive, CD or other removable storage medium*
- *Has a wireless radio built into it or can accept an aftermarket wireless card, including both notebooks and desktops*
- *Has a built-in modem or can accept an aftermarket modem*
- *Is capable of ad-hoc wireless networking*
- *Serves as a wireless access point to your network, whether authorized or rogue*

In other words, except for devices such as back-end servers and shared storage, almost all devices on the network can be considered perimeter devices in this new paradigm. And almost the entire network perimeter is in the hands of end users who don't have the appropriate tools or expertise to keep the perimeter secure against malicious code or data theft. So the question becomes how do you provide policy-based security from a central point of control—and protect the entire network perimeter—

The Hazards of Mobile Computing: Fast Facts according to leading analyst:

- **Two-thirds of critical business data reside on employee workstations or notebooks, not on servers.**
- **Approximately 90 percent of mobile devices lack the necessary security to prevent hackers from gaining access.**
- **"Everyone has been focusing on the [wireless] access point as the intrusion point. But no one is looking at the client."**
- **Each year, more than one million mobile computers were lost or stolen—and according to the FBI, less than 2 percent of them are ever recovered.**
- **A laptop theft results in an average loss of US$89,000**

[6] *Yankee Group, "2005 Security Leaders and Laggards Survey," 2006.*

[7] *Ponemon Institute, "2006 US Survey: Confidential Data at Risk," 2006.*

Novell ZENworks Endpoint Security Management allows you to create detailed policies that can be tailored for each of your organization's user groups, downloaded automatically, and stored in encrypted format on all endpoint desktops, notebooks and tablet PCs.

With Novell ZENworks Endpoint Security Management, you have centralized, single-console control over every aspect of endpoint security

while freeing end users to concentrate on their work?

The Need for Role- and Location-aware Security Policies

Given today's increasingly mobile workforce, the best way to reduce risk is through centralized, enterprisewide endpoint security management and enforcement. The idea behind this approach is simple: protect network and mobile data by enforcing client security policies that address both known and unknown security risks, whether they are within or beyond the office walls.

This requires a policy-based solution that provides fine-grained control over mobile devices, including the ability to automatically change security configurations to account for user roles and locations. For example, consider an employee who is issued a new notebook PC to replace an aging desktop PC:

- *When in the office, connected to the network via a wired connection on a desktop docking station, the security policy should allow unrestricted use of the notebook's hard drive, as well as access to appropriate IT resources based on the user's rights.*
- *In the evening and on weekends, to allow the employee to work from home via a cable modem or DSL connection, the same security policy might disable the notebook's wireless communications capability but keep the Ethernet cable port active.*
- *On the road, when the employee depends on access via a public wireless hotspot, the security policy could enable the notebook's wireless radio while also enforcing VPN usage, allowing access to the local hard drive only, and preventing any copying of files to and from thumb drives and other removable storage media.*

These measures might appear to be draconian—or entirely unenforceable if the end users were responsible for implementing them. But Novell® ZENworks® Endpoint Security Management provides a way to implement tightly controlled, highly adaptive security policies such as these without placing any configuration or enforcement burden at all upon the end user.

Novell ZENworks Endpoint Security Management: Single-console Control over the Entire Security Environment

Novell ZENworks Endpoint Security Management allows you to create detailed policies that can be tailored for each of your organization's user groups, downloaded automatically, and stored in encrypted format on all endpoint desktops, notebooks and tablet PCs.

The solution resides in the operating system kernel at the Network Driver Interface Specification (NDIS) layer for each network interface card (NIC), providing much higher security than first-generation firewall technology. The solution includes self-defense technology that makes it impossible for unauthorized users to change or defeat security policies or their enforcement. And it automatically tracks all enforcement actions as well as attempted attacks and other unauthorized activities, generating reports to ensure compliance with corporate policy as well as regulatory requirements.

With Novell ZENworks Endpoint Security Management, you have centralized, single-console control over every aspect of endpoint security—including solutions that can be deployed individually to meet specific needs, or as a fully integrated suite for perimeter-to-core endpoint protection.

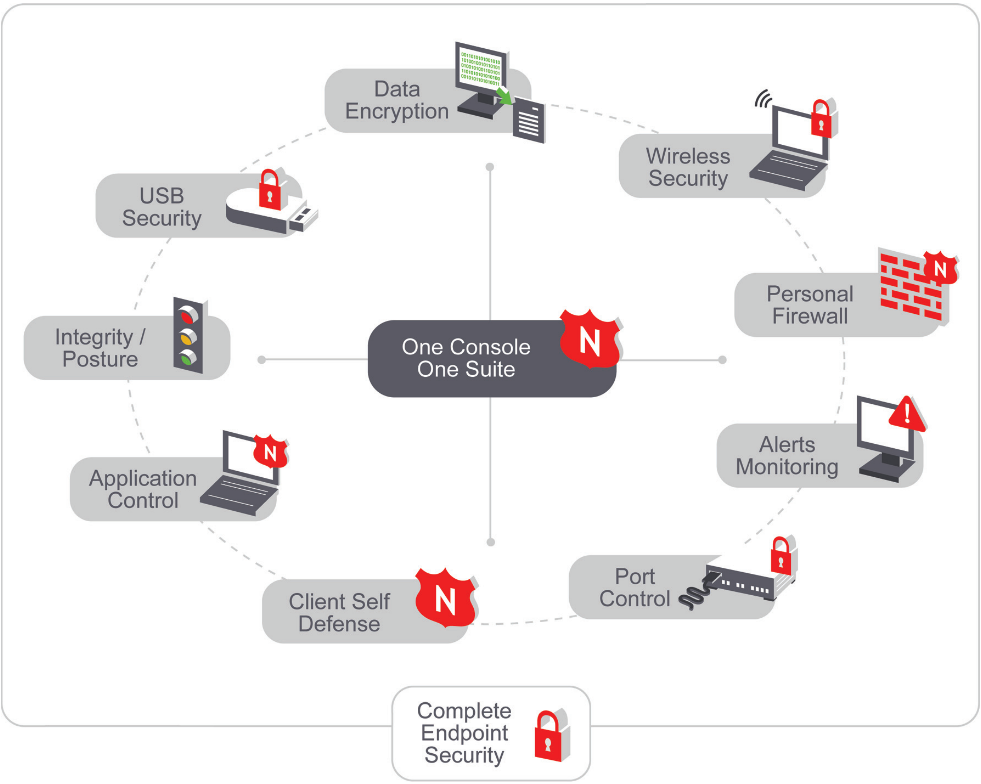

Figure 1. *From a single console, Novell ZENworks Endpoint Security Management secures every network endpoint.*

Personal Firewall

Novell offers the world's strongest firewall to protect against hackers, malware, protocol attacks and more—while keeping security invisible to the end user. Novell ZENworks Endpoint Security Management is superior to typical personal firewall technologies, which operate only in the application layer or as a firewall-hook driver. Because ZENworks Endpoint Security Management is integrated into the NDIS driver for each NIC, security protection is assured from the moment t raffic enters the PC.

Security decisions and system performance are optimized when security implementations operate at the lowest appropriate layer of the protocol stack. With Novell ZENworks Endpoint Security Management, unsolicited traffic is dropped at the lowest levels of the NDIS driver stack by means of our Adaptive Port Blocking (stateful packet inspection) technology. This approach protects against protocol-based attacks including unauthorized port scans, SYN Flood, NetBIOS and DDOS attacks.

Additionally, Novell ZENworks Endpoint Security Management provides administrators the ability, based on location, to trust or not trust specific hosts by IP or MAC address. Similarly, networking structures that use

Novell ZENworks Endpoint Security Management gives you central control over where, when and how users can connect.

multicast or broadcast packets can be accommodated by allowing for certain broadcast types, such as IP multicast, ARP, ICMP, 802.1x and others.

Wireless Security

Wireless networking is here to stay, whether or not your organization plans for it. Mobile devices come with wireless radios as standard equipment, and there's no way you can secure all the access points a device might locate and use. Major threats include accidental associations, rogue and unsecured access points, "evil twin" access points, ad hoc networks, dual-homing and more. Since you can't possibly control every access point, the best response is to control the way your mobile devices connect.

Novell ZENworks Endpoint Security Management gives you central control over where, when and how users can connect. You can limit wireless connectivity to authorized access points, establish a minimum level of encryption strength or even disable wireless networking completely. You can also automatically enforce VPN policies, requiring VPN software to be running while devices connect to foreign networks such as those in hotels, hot spots and coffee shops. Rogue access point detection helps ensure wireless security in and around the office.

Port Control

In addition to delivering wireless security, Novell ZENworks Endpoint Security Management secures all your endpoint communication ports and adapters, including:

- *LAN*
- *USB*
- *Modem*
- *Bluetooth**
- *Infrared*
- *1394 (FireWire*)*
- *Serial and parallel ports*

In essence, you can create and automatically enforce policies governing every means by which unauthorized data can pass into or out of a network endpoint—and hence the network itself.

Data Encryption

According to the Ponemon Institute, more than half of the states in the U.S. require customers to be notified if personal data is lost, stolen or compromised—an expensive proposition, especially when you consider the potential for lost customers. However, these regulations include a "safe harbor" exception to these notification requirements if the data was encrypted when it was lost.[8]

In today's decentralized networks, irreplaceable knowledge assets can be anywhere: residing on personal workstations and notebooks, and traveling on removable media and over the public Internet. Novell ZENworks Endpoint Security Management allows you to centrally create, distribute, enforce and audit encryption policies on all endpoints and removable storage devices to ensure data is secure anywhere and everywhere. Rich, flexible policies allow you to control encryption by specifying directories to encrypt on the local hard drive and enforcing encryption of all files copied to removable storage, without requiring users to manage their own security settings and keys.

USB and Storage Device Security

If not properly managed, the new generation of removable storage devices can seriously compromise your security and compliance policies. Devices containing sensitive information can be easily lost or stolen. Malware can walk through your front door unhindered on a USB device to infect your entire network. And the uncontrolled transport of unencrypted data outside the organization can get your CxOs into trouble with HIPAA, SOX, GLBA and regulatory auditors.

[8] *Ponemon Institute, "2006 Annual Study: Cost of a Data Breach—Understanding Financial Impact, Customer Turnover, and Preventative Solutions," 2006.*

The hacker community has even developed autorun code that enables an MP3 player or USB thumb drive to download huge quantities of confidential data with no explicit user commands and no audit trail. Many IT departments are just beginning to understand the scope of this threat, and are responding with extreme tactics such as sealing USB ports with glue.

With Novell ZENworks Endpoint Security Management, you can preserve your hardware investments while allowing productive—yet secure—use of USB ports and removable storage media.

With Novell ZENworks Endpoint Security Management, you can preserve your hardware investments while allowing productive—yet secure—use of USB ports and removable storage media. Highly customizable storage device security policies can be automatically distributed and continuously enforced without user intervention. It's a solution that gives you powerful, granular control over all optical media and removable storage devices, including:

- *CDs*
- *DVDs*
- *USB drives*
- *Flash memory*
- *SCSI PCMCIA cards*
- *Floppies*
- *ZIP disks*
- *Music players, smart phones and other personal devices*

To support compliance with company policy and government regulations, you can permit, block or limit access to local storage devices that can copy data without leaving an audit trail. You set up permissions that can be flexibly enforced based on automated policies that can account for the user's location and even the device's serial number. For example, if you allow write access to a removable device, you can automatically generate detailed alerts and reports on any files that were transferred to the device.

Unlike other solutions, Novell provides control at the storage device and file system level. This allows you to keep devices that pose no security threat—such as a USB keyboard or mouse—enabled and productive. You can even manage multiple functions that share a single USB connection separately. For example, with a photo printer that uses the same USB connection for both the printing and memory, you can set the memory to read-only or disabled while still allowing the device to print.

Application Control

When unapproved applications are run—knowingly or unknowingly—on corporate-owned machines, you face a variety of risks ranging from malware infection to steep fines for software licensing violations. To provide precise control over the applications running on corporate IT assets, the Application Control component of Novell ZENworks Endpoint Security Management solution offers:

- **Application blacklisting**, *enabling you to block known bad applications.*
- **Location-based application control**, *so you can allow an application to run, allow it to run only with no access to the network or prevent it from running. All blocked incidents are logged and reported to the server.*
- **Antivirus and antispyware integrity**, *verifying that security applications are up to date and running. You can quarantine and remediate out-of-compliance devices according to customizable policies—even if the device is attempting to connect away from the office.*
- **VPN enforcement**, *ensuring that users connect with an authorized VPN even when using public access points. In addition to enforcing a secure connection and encryption of data, VPN enforcement protects against "evil twin" attacks and*

If an endpoint data protection solution is successfully implemented, organizations will realize a positive impact on day-to-day operations while also improving their security posture. Seventy percent of respondents either reduced or maintained security staffing requirements, and 22 percent reported a decrease in the number of data loss incidents involving endpoints or end users in their organizations.

Aberdeen Group
"Endpoint Security Strategies Part II: The Endpoint Data Protection Benchmark"
December 2006

Novell ZENworks Endpoint Security Management is designed to prevent the endpoint security client from being altered, hacked or uninstalled.

The Alerts Monitoring component of Novell ZENworks Endpoint Security Management ensures that any attempts to compromise corporate security policies are reported to the management console so you can promptly remediate the risk.

prevents dangerous user behavior such as split tunneling.

- **Advanced scripting**, *allowing you to automatically check patches against the Microsoft* update site or an internal WSUS server, force remediation of missing patches, keep antivirus signature files and processes up to date and more—all without user intervention or IT assistance.*

Client Self-defense

Novell ZENworks Endpoint Security Management is designed to prevent the endpoint security client from being altered, hacked or uninstalled. Client self-defense features can be used to:

- *Require a password or an installation package pushed from an IT administrator in order to uninstall the client*
- *Require a password for service pause/stop, according to defined policy*
- *Disallow Windows* Task Manager requests to terminate security processes*
- *Monitor and protect critical files, keys and registry values against invalid changes*
- *Ensure that the NDIS filter driver is bound to the NIC*

Alerts Monitoring

The Alerts Monitoring component of Novell ZENworks Endpoint Security Management ensures that any attempts to compromise corporate security policies are reported to the management console so you can promptly remediate the risk. The Alerts dashboard is completely configurable, giving you precise control over when and how frequently alerts are triggered.

You also get a complete suite of reporting and audit tools to ensure that users are complying with internal security policies and to document compliance of your endpoint security controls with SOX, HIPAA and other regulatory mandates.

Making the Business Case

Evaluating the return on investment for a security solution is difficult. If the solution performs perfectly, any losses to the company's bottom line due to malicious exploits and data theft are merely hypothetical. But ensuring that these expenses remain hypothetical is the whole point of the security investment. The Aberdeen Group summarized the return on investment (ROI) dilemma perfectly in its recent report on endpoint data protection and benchmarks:

> *For many organizations, once the enormous cost of meeting or exceeding state and federal regulatory compliance regulations is added to the total cost of a loss event, what is left is a significant number which greatly exceeds the initial deployment and maintenance costs of a data protection solution implementation. So, although most agree that security ROI is difficult to prove, the ability to prevent a data loss event is at least compelling.*[9]

While the ROI estimation for any given company must rely to some degree on speculation as to the sources of risks and the associated costs of a security breach, it's worth noting how data breaches typically occur and how Novell ZENworks Endpoint Security Management deals with each type of breach.

[9] *Aberdeen Group, "Endpoint Security Strategies Part II: The Endpoint Data Protection Benchmark," December 2006.*

No company that's vulnerable to careless or malicious handling of data can afford to be caught without a complete, centrally controlled endpoint security solution. Novell ZENworks Endpoint Security Management is that solution.

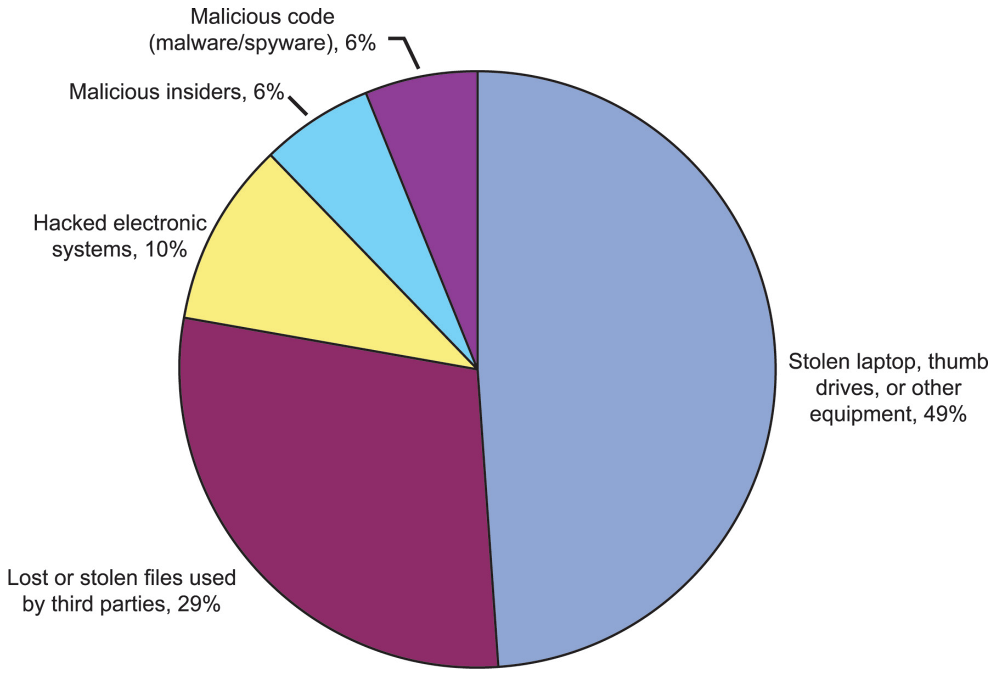

Figure 2. *In its 2006 study, the Ponemon Institute identified the sources of enterprise data breaches and their relative prevalence.*

- *Almost half of the data breaches involved lost or stolen equipment, such as laptops and thumb drives. Novell ZENworks Endpoint Security Management:*
  - Controls and audits files written to thumb drives, MP3 players and other removable storage devices
  - Encrypts what is written to removable storage
  - Specifies a "safe harbor" location on the hard drive to store sensitive data
- *Almost one third of the breaches involved data shared with third parties. Novell ZENworks Endpoint Security Management:*
  - Encrypts files written to removable storage, providing access through a shared password
  - Audits and reports what is written to removable storage and shared with third parties
- *Ten percent of the breaches were the result of hacked systems. Novell ZENworks Endpoint Security Management:*
  - Provides a stateful firewall to allow only solicited traffic into the network
  - Controls wireless access to prevent associations to "evil twins" and other wireless networking vulnerabilities
  - Requires VPN connections when users are outside the office to prevent eavesdropping and man-in-the-middle attacks
  - Locks down removable storage and communications hardware when users are out of the office
  - Ensures processes that protect the system are installed, running and up to date
- *Six percent of the breaches were due to malicious insiders. Novell ZENworks Endpoint Security Management:*
  - Controls user activities and access
  - Audits and reports on user activities

Novell ZENworks Endpoint Security Management lets you implement tightly controlled, highly adaptive security policies without placing any configuration or enforcement burden at all upon the end user.

www.novell.com

- *Six percent of breaches were due to malicious code, such as malware and viruses. Novell ZENworks Endpoint Security Management:*
  - Ensures that antivirus/antispyware is installed, up to date and running before permitting network access
  - Provides a stateful firewall to allow only solicited traffic and to prevent propagation
  - Enforces VPN for all communications outside of the office

A Solution to Match the Threatscape

Only you can estimate how valuable your data is to the organization's mission and profitability. But as we've seen, stolen or corrupted data typically results in costs that are unacceptable for almost any enterprise. That's why the business case is clear, even in the absence of a precise ROI calculation: no company that's vulnerable to careless or malicious handling of data can afford to be caught without a complete, centrally controlled endpoint security solution. Novell ZENworks Endpoint Security Management is that solution.

☎

Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400	U.S./Canada
1 801 861 1349	Worldwide
1 801 861 8473	Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA