Responsive, Flexible, Centralized Security: Novell® ZENworks®
Endpoint Security Management
## Table of Contents:

2 . . . . Your Solution to Endpoint Threats

3 . . . . Two New Paradigms: Centralizing Control and Redefining the Network Perimeter

4 . . . . The Need for Role- and Location-aware Security Policies

4 . . . . Novell ZENworks Endpoint Security Management: Responsive, Flexible, Centralized Control over Your Entire Security Environment

5 . . . . Personal Firewall

6 . . . . Data Encryption

6 . . . . USB and Storage Device Security

7 . . . . Wireless Security

7 . . . . Port Control

7 . . . . Application Control

8 . . . . Client Self Defense

8 . . . . Alerts Monitoring

8 . . . . Making the Business Case

9 . . . . A Solution to Match the Threatscape
Our business depends on sensitive data, and we’re pretty sure yours does too. In many cases, this data is the very substance of your company—your business case and your means of survival. Source code, customer lists, renderings and drawings, legal opinions, medical records, financial data and so on: it all exists in digital form, stored on a multitude of devices and passed along through a variety of networks.

This data is constantly under threat. Users lose devices. Networking connections broadcast data in the clear. Malicious attackers use ingenious methods to hijack, intercept, corrupt, redirect or view sensitive data.

Sadly, eliminating vulnerabilities is an impossible goal. The threatscape is constantly changing, and the requirements of your computing network change as well. But in general, good security practice is to:

1. Identify and fix vulnerabilities as soon as they’re known.
2. Meticulously protect the runtime environment, communication ports, removable media and other system components against unsafe code and connections.
3. Secure (encrypt) data so that if it is lost, it can’t be read and used.

These requirements put a heavy burden on any security team. But in addition, you need to do this at a sensible cost, in an efficient way, and without disrupting your workers’ productivity.

It’s important not to underestimate the potential cost of data loss. According to the key findings of the Ponemon Institute’s 2009 annual study, “Cost of a Data Breach—Understanding Financial Impact, Customer Turnover, and Preventative Solutions.”

Among the 45 companies studied, each security breach cost an average of US$6.75 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$204.

These average costs have risen continually in recent years and should be expected to continue going up.

From January 2005 to July 2007, nearly 160 million compromised records containing sensitive information were reported lost in the U.S. alone, according to the Privacy Rights Clearinghouse. The 2009 Ponemon study confirms that these losses have continued to increase, even though the media are not reporting data breaches as often. 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.” Even by the most conservative estimates, U.S. businesses are losing tens of billions of dollars annually due to data security breaches.

Things are only getting worse. As mobile devices (laptops, smartphones, PDAs) become more prevalent, the number of vulnerabilities increases exponentially each year, even as active hacking causes a much larger share of data breaches than it did even a few years ago.

And if all this talk of hackers isn’t frightening enough, consider this: your own workers are your biggest security threat. Many security breaches happen from inside your own company—whether through authorized users bringing in malicious code (accidentally or intentionally), or through exposing sensitive
data (again, accidentally or intentionally). Secondly, sensitive data is very often passed around freely and located on devices that are easy to lose or steal. Think of it this way: do you know exactly what is on every USB drive floating around your company’s offices?

If you’re involved in security, it’s your job to think about such things and manage the risks. But your workers don’t specialize in security and can’t spend all their time managing settings—they just need the appropriate hardware and data access to do their jobs. This is a state of affairs that calls for a responsive, flexible, centralized security solution.

Two New Paradigms: Centralizing Control and Redefining the Network Perimeter

If you work in IT, the above information is probably no surprise to you. The question is, how can you protect your network, your endpoints, and your company’s sensitive data without placing too many restrictions on your workers? And how do you ward off security threats when you may not know the potential entry point or even that a vulnerability exists?

At Novell, we believe that most security vulnerabilities arise because many corporations still think of security in terms of user responsibility and perimeter defense. In other words, they think of their company as a team, under siege from security threats but dealing with those threats by educating their workers, practicing vigilance, and securing their network and associated devices from outside attack. We believe this approach is no longer appropriate to modern business reality for two main reasons.

1. Security issues have become so complex that workers can’t be expected to deal with them responsibly. Security is no longer an issue of common sense (though that helps), and the level of complexity in dealing with security protocols is a productivity drain on your workers.

2. The concept of a company perimeter really doesn’t apply anymore. Your servers and network aren’t your biggest security liability. Most of your company’s sensitive data resides on—or can be accessed by—mobile devices, each of which is open to attack, theft and loss.

As a result, almost any device can pose a threat to your entire organization by opening a back door for introducing malicious code or extracting sensitive data. This threat is true of any device that:

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

There are many such endpoint devices, almost all of which are in the hands of end users who don’t have the appropriate tools or expertise to keep them secure against malicious code or data theft.

So for modern IT security professionals, the question is no longer “How can I secure my network?” but rather “How can I manage the security actions of every device in my network?” The requirements demand a flexible solution with centralized control that can actively monitor and secure a wide range of mobile devices while requiring minimal input from the end user.

---


At Novell, we believe that most security vulnerabilities arise because many corporations still think of security in terms of user responsibility and perimeter defense.
The Need for Role- and Location-aware Security Policies

Given this set of requirements, we believe that the best way to achieve security objectives is to use centralized, enterprise-wide endpoint security management and enforcement. This approach protects network and mobile data and devices by enforcing a set of security policies that address known and unknown security risks, and by choosing the set of policies based on the device’s actual needs at any given time.

This means you need a policy-based solution that provides fine-grained control over mobile devices, including the ability to automatically change security configurations based on user roles and network location. For example, consider a worker who is issued a new notebook PC to replace an aging desktop PC:

- When plugged in to an Ethernet cable at the office, 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, the Ethernet port should be active but the wireless card disabled, to allow the worker to work from home via a dedicated high speed internet connection.
- On the road, the security policy could enable the notebook’s wireless radio to connect to a public wireless hotspot while also enforcing VPN use, allowing access to the local hard drive only, and preventing any copying of files to and from USB drives and other removable storage media.

Novell® ZENworks® Endpoint Security Management gives you a way to implement these types of tightly controlled, highly adaptive security policies without requiring the end user to do anything at all.

Novell ZENworks Endpoint Security Management: Responsive, Flexible, Centralized Control over Your Entire Security Environment

With Novell ZENworks Endpoint Security Management, you can create detailed policies tailored for different network locations and for each of your organization’s user groups. These policies are then continually monitored and updated on all endpoints. ZENworks Endpoint Security Management offers the following powerful features for best-in-class performance:

Part of ZENworks 11, it shares a common console and common agent with the whole family of management tools, limiting your install, training and maintenance requirements. The solution resides in the operating system kernel at the Network Driver Interface Specification (NDIS) layer for each network interface card (NIC), resulting in much higher protection than first-generation firewall technology. Includes both active security measures (such as enforcing certain firewall or connectivity protocols) and preventive measures (such as encrypting certain folders or whole drives to keep data safe in the event of a lost device). Automatically tracks all enforcement actions as well as attempted attacks and other unauthorized activities, generating notifications and/or full reports to aid compliance with corporate policy as well as regulatory requirements. Includes self-defense technology that makes it impossible for unauthorized users to change or defeat security policies.

Novell ZENworks Endpoint Security Management gives you fully customizable, centralized security control over every endpoint in your network. This means that each one of your workers has a full-time security consultant monitoring their activity and adjusting settings and permissions to keep their devices and data safe.

Aberdeen Group

“Endpoint Security Strategies Part II: The Endpoint Data Protection Benchmark”

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.

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.
Responsive, Flexible, Centralized Security: Novell ZENworks Endpoint Security Management

Novell offers the world’s strongest personal 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 common personal firewall technologies, which operate only in the application layer or as a firewall-hook driver. Our solution is integrated into the NDIS driver for each NIC, so security protection is active from the moment traffic enters the PC.

Security protocols work best when they are implemented at the lowest possible layer of the protocol stack. Novell ZENworks Endpoint Security Management uses a proprietary Adaptive Port Blocking (stateful packet inspection) technology, which drops unsolicited traffic at the lowest levels of the NDIS driver stack. This approach gives the best possible protection against protocol-based attacks, including unauthorized port scans, SYN Flood, NetBIOS and DDOS attacks.

Additionally, Novell ZENworks Endpoint Security Management lets you designate specific hosts by IP or MAC address and then allow or block access to those hosts, and to modify those rules based on the device’s network location. In other words, some hosts could be trusted while in the office but blocked while mobile, or vice-versa. Similarly, networking structures that use multicast or broadcast packets can be accommodated by allowing for certain broadcast types, such as IP multicast, ARP, ICMP, 802.1x and others.

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

Personal Firewall

Novell offers the world’s strongest personal 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 common personal firewall technologies, which operate only in the application layer or as a firewall-hook driver. Our solution is integrated into the NDIS driver for each NIC, so security protection is active from the moment traffic enters the PC.
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.

Data Encryption
Irreplaceable knowledge assets can be anywhere: residing on personal workstations and notebooks, traveling on removable media and over the public Internet. Novell ZENworks Endpoint Security Management allows you to create, distribute, enforce and audit encryption policies on all endpoints and removable storage devices to ensure data is secure anywhere and everywhere. Rich, flexible, hierarchical policies allow you to control encryption by file type, device network location, device type and more—without requiring users to manage their own security settings and keys. And information can be seamlessly encrypted and decrypted by users in the same security group, making secure collaboration easier than ever.

The business case for encryption is clear: nearly every U.S. state requires 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, many of these regulations waive that requirement if the data was properly encrypted when it was lost.6

USB and Storage Device Security
Removable storage devices are incredibly useful, but they can seriously compromise your security and compliance policies. They hold huge amounts of sensitive information and are easily lost or stolen. Users can intentionally or accidentally introduce malware by walking into your offices and plugging into any networked device. And the uncontrolled transport of unencrypted data outside the organization can get your CXOs into trouble with HIPAA, SOX, GLBA and regulatory auditors.

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. The security policies you design are automatically distributed and continually enforced without workers doing anything. They can include the ability to:

- Block removable storage devices or set them to read-only
- Block file transfers over a certain threshold size

The Hazards of Mobile Computing: Fast Facts According to Leading Analysts
- Increasingly, critical business data resides on workstations or notebooks, not on servers.7
- Mobile devices are usually susceptible to hacking—most users do not have sufficient security protocols in place.
- Despite all the attention paid to wireless security (for example, using protected networks, SSL protocols, and/or VPN agents), the end user is ultimately the biggest security risk. Most data breaches occur when users lose mobile devices or fail to implement proper security protocols.
- Mobile computers and smaller devices (phones, PDAs) get lost all the time. For example, recent statistics show that 12,000 laptop computers are lost every week, just in U.S. airports, and that number keeps going up.8
- Some estimates place the average cost of a data breach as high as US$6.6M.9

Modern security threats are forcing security professionals to look at their jobs in a new way.
Responsive, Flexible, Centralized Security: Novell ZENworks Endpoint Security Management

- Block unaudited file transfer and/or automatically generate a report
- Selectively allow harmless devices (e.g., USB mice) or any devices on a whitelist
- Selectively manage multiple functions on a single port (e.g., printing and file transfer on a single USB port)

The ZENworks Endpoint Security Management solution gives you powerful, granular control over all optical media and removable storage devices, including:

- USB drives
- CD/DVD drives
- Flash memory
- SCSI PCMCIA cards
- Floppies and zip disks
- Music players, smart phones and other personal devices

Wireless Security

Most mobile devices and many stationary devices come with wireless radios as standard equipment. There’s no way you can secure all the access points a device might locate and use, so the best response is to control the way your mobile devices connect. This can help you defend your endpoints against threats like:

- Accidental associations and data transfer
- Rogue and unsecured access points
- “Evil twin” access points
- Ad hoc networks
- Eavesdropping
- Dual-homing

Novell ZENworks Endpoint Security Management gives you central control over where, when and how your endpoints can connect to foreign networks such as those in hotels, hot spots and coffee shops.

Port Control

In addition to delivering wireless security, Novell ZENworks Endpoint Security Management can control the functionality of all your endpoint communication ports and adapters, including:

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

When taken together, the capabilities mentioned so far let you 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.

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. Any blocked incident is simultaneously logged and reported.
- Antivirus and anti-spyware integrity, verifying that security applications are up-to-date and active. You can quarantine
It’s worth noting how data breaches typically occur and how Novell ZENworks Endpoint Security Management offers solutions for each type of breach.


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 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 itself 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 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**

We understand that it is difficult to calculate the return on investment for a security solution like ZENworks Endpoint Security Management. If the solution performs perfectly, it is difficult to say how many data breaches, and what associated expenses, it has saved.” But ensuring that these expenses remain hypothetical is the whole point of the security investment. A few years ago, the Aberdeen Group summarized the return on investment (ROI) dilemma perfectly in a report on endpoint data protection and benchmarks. Their conclusion is just as true today:

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.10

While the ROI estimate for any given company involves some speculation about 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 offers solutions for each type of breach.
Over 40 percent of the breaches involved data shared with third parties. Novell ZENworks Endpoint Security Management can:

- Encrypt files written to removable storage and provide access to all users in a security user group via a shared password
- Audit and report on what is written to removable storage and shared with third parties
- Enforce VPN use so that data is not vulnerable during transmission

Negligence was the cause of 40 percent of the breaches. Novell ZENworks Endpoint Security Management can:

- Control user activities and access to ensure good security practices
- Audit and report on user activities

Over a third of the breaches involved lost or stolen equipment, such as laptops and USB drives. Novell ZENworks Endpoint Security Management can:

- Control and audit files written to USB drives, MP3 players and other removable storage devices
- Encrypt files that are written to removable storage
- Encrypt all files on the storage device
- Specify a “safe harbor” location on the hard drive to store sensitive data

Over a third of the breaches involved system glitches. Novell ZENworks Endpoint Security Management can:

- Automate your patching process so that your endpoints are always running the most up-to-date code

Almost a quarter of the breaches were the result of malicious or criminal attacks. Novell ZENworks Endpoint Security Management can:

- Provide a stateful firewall to allow only solicited traffic into any endpoint device (and thus into your network)
- Control wireless access to prevent associations to “evil twins” and other wireless networking vulnerabilities
- Require VPN connections when users are outside the office to prevent eavesdropping and man-in-the-middle attacks
- Disable removable storage and communications hardware when users are out of the office
- Ensure that security software is installed, running and up-to-date

A Solution to Match the Threatscape

Only you can estimate how valuable your data is to your organization’s mission and profitability. But as we’ve seen, data breaches typically result in costs that are unacceptable for almost any enterprise. And apart from direct economic cost, data security is good for your brand and critical for complying with regulations. 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.
Novell ZENworks Endpoint Security Management gives you fully customizable, centralized security control over every endpoint in your network. So each of your workers has a full-time security consultant monitoring their activity and adjusting settings and permissions to keep their data safe.