

Novell ZENworks Endpoint Security Management and Full Disk Encryption

It's six o'clock on Friday morning. Do you know where your endpoints are? One of them is being hacked. It's a laptop. Your user is at the WifiCafe. He's cruising the web, thinking it's safe because the connection is labeled "WifiCafe." But next to him, someone else is running that web façade—and he's tunneling a direct line to your database.



Novell ZENworks Endpoint Security Management and Novell ZENworks Full Disk Encryption at a glance:

Lock down, don't lock out:

- Stop wasting time worrying about security—set policies and relax.
- Manage devices, even encrypted ones, from a distance.
- Keep bad guys from making a mess for IT to clean up, and move your people to better things.

Buy it individually or as a part of:

- Novell ZENworks Suite

Someone is hacking your system, and your user doesn't even know it. He didn't know it could happen; he thought he was safe.

This is a "man-in-the-middle" attack, and someone you don't know just took who-knows-what off one of your corporate laptops.

Endpoints Can Be Scary

Endpoint devices pose one of the greatest security risks to any organization. That's because as much as 70 percent of your most valuable data is carried around on endpoint devices.

We're talking about more than protecting against thieves who walk away with your machines (though we have to stop them too). We're talking about protecting against thieves walking away with your data while your own people are using those machines.

Man-in-the-middle attacks are just one of dozens of serious threats you need to protect against. There are others, like:

- **Drive bombing.** *Tempts users to plug "found" or "free" USB thumb drives into your machines—where Autorun releases malicious viruses without your even knowing it.*
- **Thumb sucking.** *Users bring their thumb drives to work and put data onto them, but that moves the data out of your control. Then your data is beyond the reach of your security policies.*
- **Pure theft.** *Someone steals a laptop. Even worse, employees bent on behaving badly can leverage unsecure endpoints and exploit vulnerabilities to their advantage—from the inside.*
- **Hacking.** *Someone inserts malicious code onto your devices from the outside, hoping your firewall won't catch it before it uploads and infects your whole system.*

You try to stop it. You set rules and policies. But you can't make people follow those policies, can you? You can try encryption, but that can be expensive, and what happens if the user loses his or her password? Then nobody can get to the data. There must be a solution.

You need a way to enforce the policies that protect your business. Because if you have that, you don't have to hope your people will stick to the rules. You know they will, because the policy makes it happen.

Power to the Policy

Truth is, you can't leave it up to people to stay out of trouble. Hackers are obvious, but insiders are just as big a risk. Most of them just don't know how to practice safe computing, and it only takes one employee with malicious intent to do harm.

You need a way to enforce the policies that protect your business. Because if you have that, you don't have to hope your people will stick to the rules. You know they will, because the policy makes it happen.

Every. Single. Time.

You can always change that policy, but your users can't. That's the point: It's not up to them. It's up to the policy.

Making Up for Their Mistakes

Users will make mistakes. Sometimes that mistake means leaving a laptop at the airport. Although it is always painful and expensive to lose a machine, with Novell® ZENworks® Full Disk Encryption, the far more valuable data it carries is indecipherable to whoever

becomes the laptop's next owner. And with Full Disk Encryption, you don't have to worry where on the hard drive the user saves data—everything on the drive is encrypted.

In a more mundane, but much more common incident, your user has lost a password. With other encryption software, this is no longer just another day at the helpdesk. Without that password you've got a hard drive as impenetrable as rock. With ZENworks, you can make this just another helpdesk procedure. Help the user reset his or her password or go in and manage the device yourself: either way, the encryption that protects the data doesn't lock you out.

It's eight o'clock on a Wednesday. Do you know what that employee in cubicle six is really downloading onto his thumb drive? Is your traveling CFO going to remember to grab his laptop bag when he gets on the plane?

Good Cop, Bad Cop

Novell ZENworks Endpoint Security Management is the ultimate policy enforcer for endpoint devices. It knows who your users are and what they should (and shouldn't) be doing. And unlike anything else, it also knows where your users are—and dynamically adjusts to meet the threat level.

When you combine the policy-enforcing power of Endpoint Security Management with the insurance of Full Disk Encryption, you can rest easy knowing that bad guys outside can't get in in, bad guys inside can't make a mess, and good guys who just want to do their jobs can't get into trouble. Your data is secure.

Practice Safe Productivity

Strike the perfect balance between productivity and protection. With Novell ZENworks Endpoint Security Management and Novell ZENworks Full Disk Encryption, you can:

- *Apply security that dynamically gauges threat levels based on who and where users are and responds accordingly, adjusting policies (such as Wi-Fi connections) on the fly.*

-
- *Encrypt data saved on portable devices.*
 - *Apply strict policies against misuse such as controlling what USB devices users can and cannot use.*
 - *Give users full control over what they need to do their work, but prevent them from circumventing security standards and policies.*

Untouchable Security

Novell ZENworks Endpoint Security Management is the ultimate policy enforcer. It can't be bought, it can't be bullied and it doesn't sleep.

It takes your policies and makes sure they're applied every time.

It's eight o'clock on a Wednesday. Do you know what that employee in cubicle six is really downloading onto his thumb drive? Is your traveling CFO going to remember to grab his laptop bag when he gets on the plane?

If you've got Novell ZENworks Endpoint Security Management and Novell ZENworks Full Disk Encryption, you don't have to worry about it.

“We needed to protect our network against viruses, hackers and a host of threats to our business. With Novell ZENworks Endpoint Security Management, we get the best of both worlds: traveling users have the freedom they need for remote access and we have peace of mind that our network isn't at risk.”

LAURA DAVIS

Technology Lead
Woolpert, Inc.

“The return on investment on Novell ZENworks Endpoint Security Management alone is astounding. If we stop just one data breach, we might have saved ourselves a \$3M lawsuit.”

ROBB PETTIGREW

*Manager, Technical Systems and Help Desk
Wyoming Medical Center*

www.novell.com



By engaging Novell Services for Premium Support, Consulting or Training, we can help you get the most of your product investment to suit your business needs. Please contact us today, or contact your local Novell Solutions Provider:

Premium Support and Consulting:
1 800 714 3400 U.S./Canada
1 801 861 4272 Worldwide
crc@novell.com

Training:
1 800 233 3382 U.S./Canada
1 801 861 3381 Worldwide
training@novell.com

Novell, Inc.
1800 South Novell Place
Provo, UT 84606 USA