



Keep Your Desktops Secure and Your Users Productive

As an IT administrator, your job is to provide end users with the resources and services they need to be productive. But too many companies require end users to manage their own desktop security applications—a task that’s not in their job description and that they’re rarely qualified to perform. Not only does this practice reduce productivity, it’s also a recipe for disaster.

Empower Users Without Losing Control

Your end users do the hard work that keeps your business on track and profitable. As an IT administrator, your job is to give end users access to the IT resources and services they need to do their jobs. But what happens if a user installs an unlicensed application that’s discovered in a software audit? What happens if a user opens an infected e-mail that spreads to unpatched systems across the network or loads sensitive company data on a USB drive, which is promptly stolen? What do you do if an employee spills a soft drink onto a laptop, wiping out the only copy of the data that was on the hard drive?

You don’t want to take away resources that users depend on to stay productive. At the same time, you don’t want users managing the security, application environment and policy compliance of their own devices. For one thing, when end users are configuring

security applications, they’re not focusing on their primary tasks and workloads. More critically, they’re not qualified to make the security decisions that keep your computing environment safe. In an ideal world, only the company’s security administrator would have complete, centralized control over every aspect of workstation security, including patch, asset and endpoint security management.

Welcome to the Ideal World

Secure Desktop Solution from Novell provides leading ZENworks® technologies for patch management, asset management and endpoint security management. Secure Desktop Solution gives you a cross-platform solution for all your Windows* desktops and consolidates all desktop security functions to help you:

Simplify management. Secure Desktop Solution removes the burden of complex endpoint security management from users

■ Solutions:

Secure Desktop Solution

■ Products:

Novell ZENworks technologies that deliver:

- Patch management
- Asset management
- Endpoint security management

70 percent of all computer attacks, security breaches and data thefts originate inside the firewall.

Yankee Group

90 percent of exploits occur through patch-related vulnerabilities.

CERT 2005

53 percent of organizations say they would never be able to determine what data was on a lost USB device.

Ponemon Institute



With today's alarming growth in vulnerabilities and zero-day exploits, you need to deliver properly tested and accurately targeted patches as soon as they're available.

so they can focus on their work. Users get secure access to the applications and services they need—and only the ones they need—without wasting time dealing with configuration issues. Speed, agility, availability and compliance with internal policies and government regulations—users get it all automatically, wherever they log in, so they can stay productive.

Control access. Business owners and IT managers retain control over the processes and policies used to ensure secure delivery of services to users. Retaining centralized control not only simplifies things for users but it also helps minimize risks to the company because it supports a total IT environment that's more reliable, predictable, credible and auditable.

Maximize assets. No gluing ports shut. No guessing about software usage and license compliance. No worries about losing data on removable media or a laptop. Secure Desktop Solution helps you understand exactly what IT assets you have and lets you control how they're being used—without denying access to the resources you've purchased. Even more important, it helps maximize your number one asset—your people—by providing them with secure, reliable, high-performance access to the resources they need to do their jobs.

Secure Desktop Solution from Novell eliminates management silos, supports the best security practices and takes the burden of

security management completely out of the hands of end users. You get central control over the entire endpoint security cycle: measurement of assets and vulnerabilities, mitigation of risks, compliance and audit inventories, and proactive defense against future risks. Secure Desktop Solution is your most powerful tool to minimize risk, reduce costs, maximize the value of your IT assets and keep users satisfied and productive.

Patch Management

In Secure Desktop Solution, the patch management functionality protects network endpoints from malicious exploits while improving compliance with internal policies and regulatory mandates. It manages the entire patch process, including continuous vulnerability assessment, using patented Digital Patch Fingerprinting, policy-based remediation and highly accurate reporting. This powerful, automated solution helps you quickly apply the right patches to the right Windows machines across your enterprise.

Your subscription includes automated patch acquisition for a wide variety of platforms and applications, with patches pre-tested, packaged and delivered to you on a daily basis. Strong baselining and reporting capabilities provide confidence that each machine meets the required level of patching, while allowing you to document the state of your environment at any time. Patch management features include:

- *Automated patch acquisition*
- *Detailed patch metadata*
- *Secured patch storage and delivery*
- *Robust agent-based architecture*
- *Applicable target management and selection*
- *Scheduling options*
- *Strong reporting*
- *Role-based management*
- *Minimum required patch conformance*

Asset Management

The unnecessary costs and security risks associated with assets you don't actually use can be substantial. And when you face software audits from BSA, SIIA and others, the risks and costs associated with assets you do use, but don't own, can be even greater. Using the Novell® ZENworks Recognition technology—and other asset management tools—in Secure Desktop Solution, you can immediately detect unauthorized software, OS and Microsoft* Office service pack levels, antivirus/spyware definitions and other potential risk exposures. Through integrated asset inventory, software usage and license reconciliation, you gain a complete and accurate view of software installations and license compliance. Asset management features include:

- *Hardware inventory*
- *Software inventory*
- *Network discovery*
- *Software compliance*
- *Contract management*
- *Software usage*

Endpoint Security Management

Secure Desktop Solution from Novell provides a full suite of driver- and application-layer endpoint security tools, all under strict IT policy control. You get the most advanced security available for the entire device environment—including the operating system, software, hardware, communications and both wired and wireless connectivity—without depending on end-user training and compliance to keep security features working correctly.

The solution includes a driver-layer stateful firewall that completely hides endpoints from port scans and other intrusions, providing the world's strongest, easiest-to-use protection against malicious exploits. Blacklisting technology and enforcement features ensure

complete IT control over the runtime environment so that only approved applications run on corporate IT assets. Automatic, location-aware enforcement of antivirus, antispymware and VPN policies ensures that key security applications are up to date and running before an endpoint can connect to the corporate network.

USB control prevents intentional or inadvertent transmission of data to removable storage devices, allowing you to place storage devices in read-only mode or to disable them completely. You can even require an audit trail for all files copied to a device, and you can keep USB ports open for devices and individual functions that pose no security risk. For example, you can set a photo printer's memory to read-only while still allowing the device to print.

To prevent inadvertent or malicious tampering, the endpoint security management tools in Secure Desktop Solution include client self-defense technology. This essential software prevents security features from being altered, hacked or uninstalled. Security administrators can also define security integrity/posture standards to automatically monitor each endpoint for compliance in real time. For example, integrity checking can ensure that antivirus, backup, audit and other processes are running as required by policy. If an endpoint falls out of compliance, even while disconnected from any network, it can be remediated using a wide range of options, from quarantine and lockdown to advanced reporting and audit mechanisms. And advanced alerting, reporting and audit tools provide the detailed information you need to monitor and document compliance with internal policies and regulatory mandates.

Employees are more productive and secure with endpoint security management features that you control by policy, requiring no input

Keep Your Desktops Secure and Your Users Productive

www.novell.com

According to the 2006 CSI/FBI Computer Crime and Security Survey:

- Virus attacks, unauthorized access to networks, lost or stolen laptops and other mobile hardware, and theft of proprietary information or intellectual property account for more than 74 percent of financial losses
- Cleanup costs for a single exploit for a 1000-node network average \$280,000

