

Novell® ZENworks® Endpoint Security Management

Secure your most vulnerable IT assets with a location-aware, policy-based solution that protects the data on every PC, controls how endpoints communicate and access information, and monitors and maintains the health of endpoint devices—all from a single console.

Product Overview

Novell® ZENworks® Endpoint Security Management provides fine-grained, policy-based control over all your desktop and mobile PCs—including the ability to automatically change security configurations depending on a user's role and location. By creating and managing policies from a central location, Novell ZENworks makes it possible to implement and enforce tightly controlled, highly adaptive security policies without placing any configuration or enforcement burden on end users. Novell ZENworks Endpoint Security Management also features robust client self-defense capabilities that provide assurance that security policies are not circumvented, as well as a complete suite of monitoring, alert, reporting and auditing tools.

Key Benefits

Novell ZENworks Endpoint Security Management is ready to help your organization:

- *Bring comprehensive, centralized security to your most vulnerable IT assets—the mobile PCs at the edges of your organization.*
- *Boost productivity by relieving end users of the burden of configuring and maintaining security settings and solutions on their own devices.*

- *Efficiently manage every aspect of endpoint security for every PC in your organization from a single console.*
- *Automatically adjust endpoint security policies and restrictions based on who users are, where they're located and what device they're using.*
- *Manage endpoint lifecycle and security issues through a single pane of glass with configuration, patch, asset and endpoint security management—all integrated in one console (and deployable as a virtual appliance).*
- *Ensure peace of mind by putting your security experts—rather than inexperienced users—back in control of defining, enforcing and maintaining endpoint security.*

Key Features

Novell ZENworks Endpoint Security Management includes a comprehensive, integrated set of enterprise endpoint security management and enforcement features:

USB AND STORAGE DEVICE SECURITY

Novell ZENworks Endpoint Security Management provides robust capabilities designed to ensure acceptable use of removable storage devices. This includes:

System Requirements

For detailed product specifications and system requirements, visit: www.novell.com/products/zenworks/endpointsecuritymanagement/technical-information

- **Data theft protection** that allows you to enable, disable or set any removable file storage device to read-only—including USB, floppy, CD/DVD and zip drives; .mp3 players; and flash memory, SCSI and PCMCIA cards.
- **Granular white listing controls** that allow administrators to control the use of USB devices.
- **Unauditable transaction prevention** that locks out local storage devices capable of copying data without leaving an audit trail.
- **Optical writer (DVD/CD) and floppy drive controls** that can allow, deny or set drive access to read-only—depending on a user's location and security situation.
- **AutoPlay/AutoRun controls** that provide centralized AutoPlay and AutoRun control functionality for your whole organization.

DATA ENCRYPTION

With Novell ZENworks Endpoint Security Management, you can centrally create, distribute, enforce and audit encryption policies on all your endpoints and removable storage devices. This includes:

- **Policy-based safe harbor encryption** that encrypts all the data stored in administrator- or user-defined “safe harbor” folders on fixed disks.
- **Removable storage device encryption** that encrypts any data copied to a removable storage device, as well as the entire contents of that device, the moment it’s plugged into a PC.

ADVANCED FIREWALL PROTECTION

Unlike traditional application layer or hook driver firewalls, Novell ZENworks Endpoint Security Management resides at the Network Driver Interface Specification (NDIS) layer for each network interface card (NIC). This ensures complete security protection from the moment traffic enters a PC. Novell ZENworks Endpoint Security Management includes the following specific firewall features:

- **Stateful firewall protection** that only allows solicited traffic to be communicated back to a device.
- **TCP/UDP port rules and Access Control Lists (ACLs)** that strictly manage and control firewall behavior on specific devices.
- **Location-based firewall behavior control** that automatically applies different sets of port rules and ACLs depending on the relative security of a device’s location.
- **Centralized, policy-based control** over firewall settings that cannot be disabled or circumvented by end users or unauthorized administrators.
- **True quarantine capabilities** that protect your network when the security integrity of a PC fails.

WIRELESS SECURITY

Novell ZENworks Endpoint Security Management provides centralized control over where, when and how users can connect to wireless networks. This includes:

- **Wi-Fi management** that allows you to create white and black lists for wireless access points and implement policies that restrict, disable or block Wi-Fi communications in specific situations.
- **Wi-Fi security controls** that limit Wi-Fi communications to wireless access points that meet encryption standards.
- **Wi-Fi adapter blocking** that only allows endpoints to connect to wireless access points using corporate-approved Wi-Fi adapters.

PORT CONTROL

In addition to Wi-Fi security, Novell ZENworks Endpoint Security Management provides complete protection for every other type of wired and wireless port and communication device. This includes LAN, USB, 1394 (firewire), serial and parallel ports, as well as modems, Bluetooth and infrared (IrDA) connections.

APPLICATION CONTROL

The application control component of Novell ZENworks Endpoint Security Management gives you precise, policy-based control over the applications running on all your endpoints. This includes:

- **Application blacklisting** that blocks known malicious or undesirable applications.
- **Location-based application control** that can allow specific applications to run, deny them access to the network or prevent them from running altogether—all based on the security of a user’s location.
- **Antivirus and spyware integrity checking**, which verifies that all required security applications are running properly—and then quarantines and remediates non-compliant devices.
- **VPN enforcement** that ensures users can only connect using an authorized VPN, protects against “evil twin” attacks and prevents dangerous user behaviors such as “split tunneling.”

www.novell.com



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

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

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