

ZENworks Endpoint Security Management

Secure your most vulnerable IT assets with a location-aware, policy-based solution that protects against malware threats, 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 Highlights

OpenText™ ZENworks Endpoint Security Management provides fine-grained, policy-based control over all your Windows 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 console, OpenText™ ZENworks makes it possible to implement and enforce tightly controlled, highly adaptive security policies without placing any configuration or enforcement burden on end users. ZENworks Endpoint Security Management also features robust client self-defense capabilities that provide assurance that security policies are not circumvented; in addition, it has a complete suite of monitoring, alert, reporting, and auditing tools.

Key Benefits

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.
- Ensure peace of mind by putting your security experts—rather than inexperienced users—back in control of defining, enforcing, and maintaining endpoint security.
- When used with the OpenText™ ZENworks suite, you can manage endpoint lifecycle and security issues through a single pane of glass with configuration, patch, asset, and endpoint security management—all integrated into one console (and deployable as a virtual appliance).

Key Features

Malware Threat Protection

ZENworks Endpoint Security Antimalware protects Windows desktops, servers, and mobile PCs against known and unknown (zero-day) malware threats. This includes:

- Antimalware engine technologies that provide multi-layer security through a variety of detection methods. Traditional signature-based detection protects against known threats; generic detection protects against known threat variants; and advanced heuristic analysis protects against unknown, zero-day threats.

System Requirements

For detailed product specification and system requirements, visit: www.microfocus.com/en-us/products/zenworks/specs

- Real-time malware detection as files are copied, moved, opened, or executed.
- Scanning of local and network drive locations at scheduled times or when manually initiated.
- Scanning of removable drives on insert.
- Disinfecting, quarantining, or deleting of infected and suspect files.
- Configuration of all endpoint malware protection behavior through the centralized management console.
- Monitoring of device malware status and detected threats via dashboards in the centralized management console.

USB and Storage Device Security

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

- Data theft protection that allows you to enable, disable, or set any removable file storage device to read-only—including USB, WPD (Windows Portable Device), 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 and WPD 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 ZENworks Endpoint Security Management, you can encrypt removable storage devices and fixed-disk folders on all your endpoints. This includes:

- Encryption using native Microsoft technologies rather than additional encryption drivers; BitLocker is used for removable drive encryption and Encrypting File System (EFS) for fixed-disk folders.
- Centralized key management to enable administrator recovery of encrypted files.

- Removable drive authentication that enables encrypted removable drives to be unlocked on all devices or on ZENworks-managed devices only.
- Optional fixed-disk folder authentication that requires a second password to be entered after Windows login before encrypted folders can be accessed.

Wireless Security

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, 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.

VPN Enforcement

To increase security when devices connect to open networks or require access to your internal network from an external location, ZENworks Endpoint Security Management provides 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.”

Application Control

The application control component of 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.

Connect with Us



- 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.

Advanced Firewall Protection

Unlike traditional application layer or hook driver firewalls, 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. 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