opentext™

Data Sheet

ZENworks Endpoint Security Management

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

- 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
- 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

  CD/DVD, and zip drives; .mp3 players; and
- Granular white listing controls that allow

  and WPD devices.
- locks out local storage devices capable of copying data without leaving an audit trail.
- controls that can allow, deny, or set drive

  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 -

points. This includes:

- Encryption using native Microsoft technologies rather than additional encryption drivers; BitLocker is used for removable drive encryption and Encrypting
- Centralized key management to enable
- Removable drive authentication that enables encrypted removable drives to be unlocked on all devices or on ZENworks-managed devices only.
- 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
- 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

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.
- Location-based application control that

  them access to the network, or prevent

  on the security of a user's location.
- Antivirus and spyware integrity checking,

  and then quarantines and remediates non-compliant devices.

Advanced Firewall Protection