opentext™

Data Sheet

ZENworks Endpoint Security Antimalware

Reduce your organization's vulnerability to business disruption and data breaches by protecting your Windows endpoint devices against a growing number of new and evolving malware threats.

Product Highlights

OpenText™ ZENworks Endpoint Security Antimalware, a key component of OpenText ZENworks Endpoint Security Management, provides real-time malware protection for Windows workstations and servers. The advanced Antimalware scan engine protects against known and unknown malware threats, including viruses, Trojans, worms, spyware, adware, rootkits, and more. The default Antimalware policy enforces best practice threat detection and remediation behavior while allowing for easy customization through the central management console. The interactive Security Dashboard monitors the threat status of all protected endpoint devices and tracks all detected malware threats on those devices.

Key Benefits

ZENworks Endpoint Security Antimalware helps your organization:

- Protect your endpoints and their data against the latest malware threats whether they are in the office or remote working.
- Configure and maintain endpoint protection through the same central management console that is used by other ZENworks products.
- Know when malware threats have been detected on protected endpoints and how those threats have been remediated.

Key Features

Real-Time and On-Demand Protection

ZENworks Endpoint Security Antimalware checks files as they are accessed (real time) or when initiated by a schedule or a user:

- Real-time protection scans files as they are opened, copied, moved, or executed on an endpoint.
- On-demand protection lets you schedule scans to be performed at regular intervals or when external drives, such as USB thumb drives, are connected to the endpoint.
- Contextual scans let end-users scan worrisome folders and files.

Targeted Scans with Customizable Exclusions

Not everything on the endpoint should be scanned every time, and sometimes never at all. ZENworks Endpoint Security Antimalware lets you target the areas you want scanned.

- The Full Scan performs a thorough check of all areas of the endpoint.
- The Quick Scan focuses on the areas most susceptible to infection.
- Modify the Full and Quick scans as needed, or supplement them with Custom scans you create.
- The Network Scan lets you designate an endpoint device to periodically scan a network share.

Advanced Antimalware Engine Technologies

- Unique file format analyzers and parsers extract only relevant data needed for malware detection and handle damaged and altered file formats.
- Archive algorithms support both modern and outdated archivers, provide configurable depth scanning of embedded archives, and handle damaged archives.
- Executable unpackers ensure that runtime packers are not being used to obfuscate malware in program code.
- Emulation simulates execution of suspect files in a virtual environment to determine file behavior and provide more accurate threat prediction.
- Heuristic-based detection uses complex algorithms, emulation, and behavioral characteristics to detect new and emerging (zero-day) threats.
- Generic detection uses key characteristics of known malware threats to identify variants of the same malware family.
- Signature-based detection relies on code snippets extracted from malware samples to quickly detect known malware threats.

- Exclude specific files, file extensions, folders, and processes from any of the different scan types: On-Access (real-time), Full, Quick, Custom, Network, External Drive, or Contextual.
- Assign exclusions globally to all endpoints or target groups of endpoint devices.

Flexible Scan and Update Schedules

ZENworks Endpoint Security Antimalware performs on-demand scans and product updates on the schedule you want:

- Schedule Full, Quick, Custom, and Network scans monthly, weekly, daily, or on an interval.
- Keep the default update schedule for malware signatures (every 1 hour) and scan engine changes (every 4 hours) or customize the schedules to your needs.
- Assign a base schedule to all endpoints and override schedules as needed for individual endpoints or groups of endpoints.

Controllable User Interaction

ZENworks Endpoint Security Antimalware lets you determine how much interaction, if any, you want end-users to have with your malware protection:

- Disable alerts to suppress pop-up notification of malware events.
- Configure whether users can pause, postpone, or cancel administrator-scheduled or initiated scans.
- Hide the Endpoint Security Antimalware console completely to suppress event notifications and remove all user interaction.

Policy-Based Administration

ZENworks Endpoint Security Antimalware uses administrator-configured policies to control the behavior of the Antimalware scan engine.

- The required Antimalware Enforcement policy lets you enable the scan types to use (On-Access, Full, Quick, External Device, and Contextual) and the settings for each scan type. This includes target scan locations, file types to scan, scan exclusions, file quarantine options, and remediation actions to take on infected files.
- Optional policies let you create Custom and Network scans as well as define global scan exclusions to be used across all policies.
- Assign the same policies to all endpoints or assign different policies to customize the malware protection options needed by different endpoints.

Central Threat Monitoring

You want to know when threats are detected on your endpoints. ZENworks Endpoint Security Antimalware provides extensive threat monitoring capabilities in the central management console:

- The Security dashboard shows all detected threats, the current threat status of each endpoint, and the last time scans were performed on the endpoints.
- View a detected threat to see all infected endpoints and whether the threat is resolved or unresolved on each endpoint
- View an endpoint to see its detected threats and the actions taken on its infected files.
- Restore or delete false positive files (infected or suspect) that were quarantined.

System Requirements

Supported Operating Systems

- Workstations: Windows 10 and newer
- Servers: Windows Server 2012 and newer

Additional Requirements

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

Learn more at

www.microfocus.com/products/zenworks-endpoint-security-management/overview

www.opentext.com

Connect with Us

opentext™