ZENworks Patch Management

Organizations today experience a seemingly endless stream of software security threats accompanied by the patches required to fix them. Keeping up can strain even the best-staffed IT department. Simply maintaining patched endpoints can feel overwhelming. Quickly responding to critical security threats can feel impossible. ZENworks Patch Management helps you easily update your endpoint software on a regular schedule as well as quickly identify and remediate emerging security threats.

Product Highlights

OpenText™ ZENworks Patch Management helps you proactively manage threats by automating the collection, analysis, and delivery of patches to a diverse range of endpoints. Policy-based patching lets you maintain patch currency on devices through regularly scheduled updates. Security-focused patching lets you identify software security vulnerabilities that impact devices and apply, in one action, all patches required to remediate the devices. ZENworks Patch Management is available either as a standalone product or as a discounted subscription option in the OpenText™ ZENworks Suite.

Key Benefits

ZENworks Patch Management is ready to help you:

- Dramatically lower patch management costs and effort by enabling accurate, automated processes for patch assessment, monitoring, and remediation across your whole organization.
- Expand the reach of your patch management efforts with a cross-platform approach that provides pre-tested patches for more than 40 different Windows, SUSE, Red Hat, and Macintosh operating systems.
- Boost compliance with tools that allow you to monitor patch compliance on every device in your organization, quickly identify and assess vulnerabilities, and automatically apply updates and patches to bring devices up to predefined policies and standards.
- Identify critical software security vulnerabilities (WannaCry, NotPetya, SamSam, BlueKeep, and more) that impact your devices in order to respond quickly to emerging threats.
- 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.

Key Features

Monitoring and Reporting

With a powerful monitoring and reporting engine, ZENworks Patch Management provides deep insights into the patch status and overall security posture of your network. This includes:

- **Agent-based monitoring** that detects security vulnerabilities on individual endpoints, continually assesses security risks, and provides automatic notification of patch compliance issues and concerns.
- **Dynamic, dashboard-style graphical reports** that quickly provide a complete, high-level view of patch compliance across your organization—and make it easy to drill down to detailed patch data for individual endpoints.

System Requirements

For detailed product specification and system requirements, visit: **www.microfocus.com/products/zenworks/patchmanagement/specs**

Collection, Analysis and Pre-Testing

ZENworks Patch Management eliminates the extensive time and manual effort required to collect, analyze, and test the overwhelming number of patches available for different types of endpoint systems. This includes:

- **Vulnerability announcements** that inform organizations when a new patch is ready for deployment.
- **The world's largest dynamic repository of patches**, which provides more than 50,000 pre-tested patches for more than 100 major current and legacy applications and operating systems (including Linux and Mac).
- **Reliable and thoroughly pre-tested patch packages** that dramatically reduce the time and labor required to check, verify, and deploy patches.

Automated Deployment

In addition to providing an extensive library of pre-tested patch packages, ZENworks Patch Management includes features that streamline and automate every aspect of the patch deployment and verification process. This includes:

- **Fast, automatic** patch deployment based on predefined policies, as well as the ability to customize tested patches as needed.
- **A wizard-based interface** that simplifies the process of getting the right patches to the right endpoints quickly and efficiently, plus download percentage reports that provide real-time status updates.
- **Support for phased rollouts** to ensure smooth, error-free patch deployments to large numbers of systems.
- **Rapid verification of patch deployments** that catches deployment issues before they can become security problems.
- **A virtual appliance deployment option** for patch, configuration, asset, and endpoint security management, which simplifies installation and reduces support costs.

Policy-Based Compliance

ZENworks Patch Management allows you to create mandatory baselines for patch compliance based on predefined policies, continually monitor endpoint systems for compliance, automatically remediate systems that don't meet minimum standards, and clearly document improvements in patch compliance. This includes:

- **Patented digital fingerprinting technology** that establishes a security profile for each managed node on your network and facilitates ongoing compliance.
- **21 standard reports** that document changes and demonstrate progress toward internal and external audit and patch compliance requirements.
- **Automatic application of required updates and patches** to new systems and installations to bring them into compliance with predefined patch policies and standards.

Emerging Threat Detection and Remediation

ZENworks Patch Management identifies the software security threats that impact your endpoints to help you prioritize your remediation efforts and track the results. This includes:

- **Identification of vulnerabilities** based on industry-standard Common Vulnerabilities and Exposures (CVEs) imported from the NIST National Vulnerability Database.
- **Customizable dashboards** that show the CVEs impacting your devices, organized by severity, release date, or vulnerable device count.
- **One-click remediation** of impacted devices to automatically apply all patches required to remediate the CVE without needing to find or select the patches.
- **Tracking of remediation progress** for CVEs that shows current vulnerability status as well as increasing or decreasing trend over time.

Learn more at
www.opentext.com

Connect with Us