kaspersky BRING ON THE FUTURE

Kaspersky Vulnerability & Patch Management

Reduce complexity and strengthen security with centralized IT management tools

Unpatched vulnerabilities in popular applications pose a significant threat to IT security. And it's not just zero-day vulnerabilities that are a problem — growing IT complexity further complicates the task of plugging gaps in vulnerable software swiftly: if you don't know exactly what you've got, how can you secure it?

Managing and administering software updates while constantly monitoring for potential vulnerabilities is one of the most important yet tedious and time-consuming tasks faced by IT departments. By centralizing and automating essential security and configuration and management tasks, such as vulnerability assessment, patch and update distribution, inventory management and application rollouts, Kaspersky Vulnerability and Patch Management saves time and optimizes security.

Vulnerability Assessment and Patch Management
- Detect and prioritize vulnerabilities
- Download, test and distribute patches and updates
- Time-saving software distribution
- Monitor results and run reports

Client management tools
- Hardware and software inventories
- Remote troubleshooting
- Convenient OS deployment

Highlights

Gain full visibility

Full network visibility from a single console eliminates administrator guesswork and provides complete awareness of every application and device, including guest devices, entering the network. This supports centralized control of user and device access to organizational data and applications, in line with IT policies and regulatory compliance requirements.

Enhance security

Increase the effectiveness of your IT security and reduce time-consuming routine tasks with timely, automated patching and updates. Kaspersky Vulnerability and Patch Management provides total visibility, so you know exactly what needs to be done to keep your business safe. Automating the entire cycle of vulnerability assessment and patch management, including vulnerability detection and prioritization, patch and update downloads, testing and distribution, result monitoring and reporting, supports greater efficiency and significantly reduces the burden on resources.

Streamline IT tasks

Kaspersky Vulnerability and Patch Management includes a set of client management tools to automate a wide range of IT administrative functions. Automated provisioning of applications and audited, remote access and troubleshooting help to minimize the time and resources necessary to set up new workstations and roll out new applications.

Manage centrally

Kaspersky Vulnerability and Patch Management is a managed component of the Kaspersky Security Center. All features are accessed and managed through this central console, which uses consistent, intuitive commands and interfaces to automate routine IT tasks.

Vulnerability Assessment and Patch Management

Monitor results and run reports

Kaspersky Vulnerability and Patch Management notifies IT administrators about the status of patch installation and enables them to run reports on scans, look for potential weak spots, track changes and gain extra insights into the organization's IT security – as well as on every device and system across the corporate network. Information about existing exploits and known threats as well as CVEs (common vulnerabilities and exposures) are also available.

Detect and prioritize vulnerabilities

Automated vulnerability scanning enables rapid vulnerability detection, prioritization and remediation. Vulnerability scanning can be delivered automatically or be scheduled according to the administrator's requirements. Flexible policy management facilitates the distribution of updates, compatible software and the creation of exceptions.

Time-saving software distribution

Deploy or update remotely, from a single console. Over 150 popular applications, identified via Kaspersky Security Network can be automatically installed, even after working hours. Save on traffic to remote offices with Multicast technology for local software distribution.

Download, test and distribute patches and updates

Updates and patches can be downloaded automatically through Kaspersky's servers. Before distribution, these can be tested to ensure they won't impact on system performance and employee efficiency. The administrator can limit the list of applicable patches on endpoints to approved patches only. Patches and updates can be distributed immediately or postponed until a more suitable time.

Client management tools

Scan your network to create hardware and software inventories

Automated discovery and hardware and software tracking give administrators detailed insights into every asset on the corporate network. Automated software scanning enables rapid detection of outdated software that may pose a security risk if not kept up to date.

Increase efficiency with remote troubleshooting

For reduced response times, increased efficiency and streamlined support for remote sites, Kaspersky Security Center uses Remote Desktop Protocol (RDP) and Windows Desktop Sharing technology (used in Windows Remote Assistance). Remote connection to client computers through the Network Agent gives administrators full access to the data and applications installed on the client, even if the client TCP and UDP ports are closed.

An authorization mechanism prevents unauthorized remote access. For traceability and auditing, all activities performed during a remote access session are logged.

Convenient OS deployment

Kaspersky Vulnerability and Patch Management automates and centralizes the creation, storage and cloning of secured system images, and supports operating system (OS) deployment to new machines (as well as re-installations). All images are held in a special inventory, ready to be accessed during deployment.

Client workstation image deployment can be made with either PXE servers (Preboot eXecution Environment – also for new machines without OS) or using Kaspersky Vulnerability and Patch Management tasks (to deploy OS images to managed client machines). By sending Wake-on-LAN signals to computers, you can automatically distribute the images out of normal office hours. UEFI is supported.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.