Kaseya White Paper

Download these FREE Kaseya IT Tools Today:

- Security Audit
- Windows Patch Status

Endpoint Security

Fighting Cyber Crime with Automated, Centralized Management

Kaseya

www.kaseya.com

To win the ongoing war against hackers and cyber criminals, IT professionals must do two things: Deploy and maintain endpoint security tools with the latest updates, and ensure the software applications running in their networks have the latest available patches. Failure to do either exposes their IT environments to cyber threats and their organizations to financial losses and embarrassment, while putting their jobs at risk.

Keeping up with patches and updates, however, isn't easy. Vendors pump them out in an endless barrage as they seek to plug newly discovered security holes and improve performance. In distributed, heterogeneous environments with hundreds or thousands of endpoints, it is virtually impossible to manage the process manually. Complicating matters, administrators have to contend with these challenges:

- Mobile and remote users outside network domains often miss patches and updates, putting themselves and other network users at risk.
- Different network components don't always play well with each other, causing interoperability issues and exploitable vulnerabilities.
- Updates and patches, if untested before deployment, can break applications, harming the systems they are supposed to protect.

The only chance that budget-tight IT departments have at effectively tackling all these challenges is by replacing error-prone, time-consuming manual processes with the automation of security audits and patching. Administrators also need to manage these processes from a single dashboard that gives them a comprehensive view of the IT environment.

Easier Said than Done

Cyber criminals are relentless in identifying new vulnerabilities in applications, platforms, systems and browsers – and they dedicate their lives to designing malware to exploit them. With that in mind, it is imperative that organizations keep their security tools and software applications current and patched.

Of course, that's easier said than done. Depending on the technology in place, dozens of updates might flow into a network each month. Often, administrators don't know exactly which antivirus tools are where, what versions of software are running, or which patches are current or outdated. Large distributed networks typically have multiple AV tools and run different versions of systems applications, all of which require version-specific updates. Without a consolidated view and centralized management of the network, keeping everything current and patched is next to impossible.

To complicate matters, patches sometimes cause problems for users and IT staff, breaking applications and deleting files. To prevent these unintended actions, administrators need to follow the best practices of testing patches and updates in isolated settings before deploying them to users.

One of the most common update processes administrators have to manage is Microsoft's Windows Server Update Services (WSUS) – another area where IT staff can run into problems. Some users subvert the process by failing to reboot their machines to complete updates while others, who work outside the network domain, miss the updates altogether.

"Cyber criminals are relentless in identifying new vulnerabilities in applications, platforms, systems and browsers – and they dedicate their lives to designing malware to exploit them."

Kaseya

Users also tend to ignore update prompts if they are too frequent, even though this can lead to file infections, network downtime and data theft. In 2012, vulnerabilities in PDF files and Java code caused a number of infections, hurting user productivity and causing financial losses for employers. In some cases, timely updates would have prevented infections.

Edge of Disaster

Data loss, theft and corruption ultimately are far more costly than financial losses from a security breach. Lost productivity can cost millions and the theft of trade secrets can be devastating. The Ponemon Institute estimates the cost of cyber crime per organization at a yearly $8.9 million. Beyond monetary costs, cyber crime stains an organization's reputation – sometimes irreparably – when private data is stolen or exposed.

IT administrators operate in a realm that often flitters on the edge of disaster. And while they understand the dangers of unpatched software, administrators may feel helpless in the face of relentless hackers and a complex, demanding patch schedule. They have to not only protect their organizations, but also their own jobs and reputation. When a security incident occurs, fingers will be pointed in their direction first.

So even if a breach occurs, administrators must prove they took the proper steps to protect the network and data – that they followed corporate policies and met regulatory requirements. A big part of that involves timely patching and updating.

Fortunately for IT administrators, endpoint security and patch management can be automated and managed from a single, centralized dashboard. This approach removes a lot of the issues that get in the way of protecting networks, while making it much easier to apply standards and comply with internal policies and regulatory requirements.

Automated Endpoint Security

Endpoint security is critical. It is through the endpoint that most successful cyber attacks occur, with hackers preying on the inattention or trust of users to download or open infected files. Effective endpoint security, however, requires knowing which security tools are in use, making sure they are up to date, and enforcing policies and best practices. The Kaseya framework makes all of this possible through a centralized management dashboard from which administrators can automate endpoint security-related tasks.

The dashboard is customizable and offers a comprehensive view of deployed security tools. Instead of resorting to guesswork or long hours of discovery, administrators have information at the ready about which antivirus tools are deployed and on which machines. All endpoints are covered, be they machines within the network domain or notebooks and tablets used outside network walls. Hard-to-reach remote and mobile computers that roam in and out of the network are patched and updated regularly. This is key to preventing infections caused by malware that users sometimes unwittingly pick up outside network firewalls.

Centralized management reduces security tasks from days to hours - or even minutes. Scans and deployments can be scheduled off-hours to avoid interrupting users. Through the dashboard, IT staff keeps tabs on the health of the network 24/7 through real-time alerts for various conditions, including missed scans, unpatched machines and out-of-date applications. Alerts for suspicious events at endpoints can be set, giving IT the ability to react immediately by isolating a suspicious machine to prevent an infection from spreading and, if needed, initiate remediation.

In addition to real-time information, administrators get plenty of customizable data to prepare reports on endpoint security status and show compliance with internal policies and regulatory requirements. Automated, centralized management makes administrators' lives easier while giving them the confidence that the network is secure.

"Data loss, theft and corruption ultimately are far more costly than financial losses from a security breach. Lost productivity can cost millions and the theft of trade secrets can be devastating."

"Fortunately for IT administrators, endpoint security and patch management can be automated and managed from a single, centralized dashboard."

Kaseya

Antivirus and Antimalware

As an added benefit, The Kaseya framework integrates with security tools **Kaspersky Labs** and **Malwarebytes** to help protect networks against cyber criminals. Kaspersky Labs antivirus delivers on-demand scanning, spam protection, automatic isolation of infected systems, post-infection recovery, device control to disable external devices such as USB drives, and selection of trusted processes. Malwarebytes technology monitors every process in the network to prevent malicious activity, employing an advanced heuristic scanner to monitor systems in real time. The system quarantines suspicious code before it can spread infection.

Centralized Patch Management

Patch management works hand-in-hand with endpoint security to plug security holes that can put an organization at risk. The Kaseya framework's automated, centralized patch management capabilities remove the complexity and hardships involved in keeping up with large volumes of security and software updates.

With simple mouse clicks, administrators can check patch status, deploy updates and enforce patch-compliance policies. But rather than spending hours going from machine to machine to check on and install patches, administrators can do it all from a central location, keeping all the software and security tools at each endpoint up to date.

The system works out of the box to audit patch status and compliance, taking only minutes to get up and running. Automated scans identify missing and out of date patches and determine where new updates are needed. Interoperability issues that create security vulnerabilities can be identified and addressed. Installation of software components is transparent and can be scheduled to run off-hours, simultaneously to all machines, without disturbing users.

To avoid breaking applications and deleting files, administrators can test patches in an isolated environment before implementing them network-wide. Monitoring and alerts ensure that IT knows when patch deployments fail or when something goes wrong during reboots. Customizable reporting capabilities help administrators keep track of patch status and provide proof of compliance.

Software Deployment and Updates

In addition to patching, the Kaseya framework offers a software deployment option that automates the time-consuming process of deploying and updating applications. Administrators can install and uninstall software from a central console, view deployment status and create installation profiles of packaged software for specific groups of machines. This allows administrators to keep track of application status and when they need to be updated.

Kaseya Security and Patch Options

To help busy IT administrators get a handle on endpoint security and patch management, Kaseya offers a range of options through its IT management framework. In addition, the vendor offers the following tools separately as standalone options:

- **Security Audit** determines and reports on security settings at all endpoints, making it easier to schedule scans, achieve compliance and remove security vulnerabilities associated with unknown antivirus status. Kaseya offers this tool free of charge.
- **Windows Antivirus** adds to Security Audit with a configurable Windows endpoint antivirus solution that has full remote deployment capabilities by single machine or group of machines. This is a subscription-based paid tool.
- **Patch Status** helps administrators determine and report on the patch status of all the endpoints across the network, including Windows update settings and patches. Kaseya offers this tool free of charge.
- **Patch Management** adds to Patch Status with automated, customizable patch deployment capabilities. This is a subscription-based paid tool.

> "With simple mouse clicks, administrators can check patch status, deploy updates and enforce patch-compliance policies."

> "Administrators can install and uninstall software from a central console, view deployment status and create installation profiles of packaged software for specific groups of machines."

Kaseya

The Kaseya cloud-based architecture requires no on-site servers, dedicated hardware or appliances. Instead, administrators manage systems from their offices or data centers, or even while roaming without needing a VPN connection.

Conclusion

IT administration is anything but easy, especially when you have to constantly fend off cyber threats that can shut down a network and cause irreparable business damage. With the automation and centralized management that Kaseya offers for antivirus, security audits, patch status and patch management, tasks involved in protecting networks become easier and more efficient. With Kaseya, IT professionals stand a much better chance at winning the war against hackers and cyber criminals.

> "With Kaseya, IT professionals stand a much better chance at winning the war against hackers and cyber criminals."

About Kaseya

Kaseya is a leading global provider of IT service management software. Our technology empowers any sized IT operation — from individual IT professionals at small-to-medium sized businesses to large corporations and IT service providers — to proactively manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Kaseya

www.kaseya.com