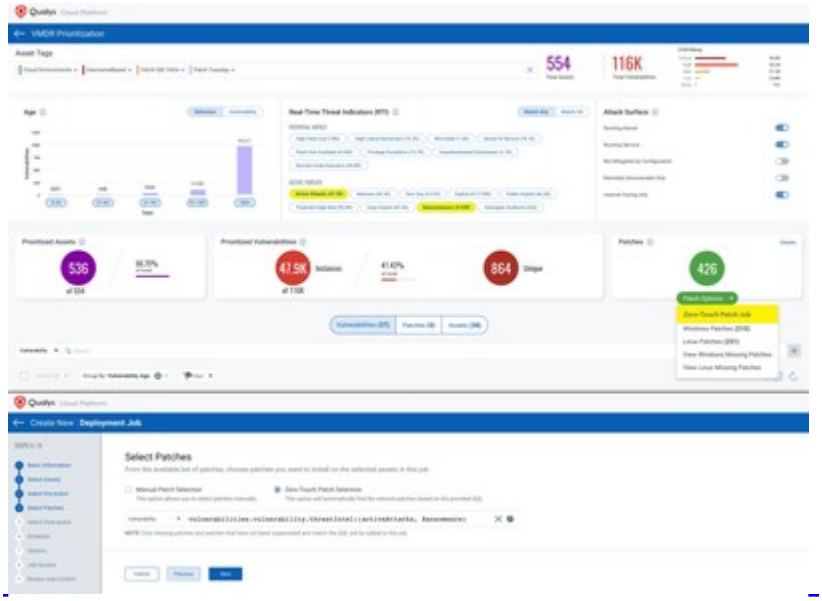
Qualys Introduces Zero-Touch Patching for Proactive Vulnerability Remediation

September 14, 2021

New capability keeps endpoints always up to date with the latest patches to reduce risk from exploits like ransomware

FOSTER CITY, Calif., Sept. 14, 2021 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, today announced it is integrating zero-touch patching capabilities into Qualys Patch Management. Zero-Touch Patch ensures that companies' endpoints and servers are proactively updated as soon as patches are available, reducing their overall attack surface.



Most vulnerability remediation involves multiple teams and processes – first, a scanning tool identifies vulnerabilities, and then they are passed to the patching team for remediation. This is a pain point for organizations and leads to extra resources, costs and longer exposure times. A lack of alignment between vulnerability and patch processes and the manual efforts required for vulnerability remediation are among the key causes of delayed patching.

"Qualys Patch Management helps us quickly patch remote systems based on vulnerability-driven priorities without the need for a VPN," said Surendra Nemani, Head – Security Engineering at Infosys. "What's exciting about the new zero-touch capabilities is the support for third-party apps like Microsoft, Adobe and various browsers. The automation allows us to set up patching in advance, matching patch correlation to prioritized vulnerabilities without the need for the typical back and forth between security and IT teams. It has empowered our platform teams and improved our patch governance efforts. We chose Qualys Patch Management as it is natively integrated into Qualys VMDR and allows cross-platform remediation."

"Endpoint security needs to concentrate on taking intelligence from detection and response workflows for better prevention, and Qualys is uniquely positioned to leverage both vulnerability and threat intelligence insights in its patching solution," said Chris Kissel, research director in IDC's Security & Trust Products Group. "Cleverly, Qualys' approach of taking patch remediation a step further with the addition of zero-touch automation eliminates non-caustic threats like always patching Chrome or iTunes. It is a welcome addition that helps companies reduce their attack surface while also freeing up IT and Security resources to focus on more strategic areas."

Qualys Patch Management leverages the Qualys Cloud Platform and Cloud Agents to help IT and security teams quickly and efficiently remediate vulnerabilities and patch systems. New intelligent automation allows prioritization of vulnerabilities based on threat indicators such as ransomware, matching of prioritized vulnerabilities with known patches, and a zero-touch "set and forget" feature to proactively patch devices and applications per predefined policies – leading to increased productivity. For example, an organization can create a policy to keep Adobe Reader software always patched on all employee laptops.

The new capabilities enable organizations to:

Reduce the Risk From Threats Like Ransomware
Qualys Zero-Touch Patch intelligently identifies and automatically deploys the proper patches and configuration changes required for remediating vulnerabilities. Next, it leverages Qualys VMDR (Vulnerability Management, Detection and Response) to prioritize them based on real-time threat indicators such as ransomware, active attacks, exploitability or lateral movement to help organizations reduce cyber risk.

Accelerate Vulnerability SLA Compliance
The application of patches for compliance is automated to help security teams align with regulatory and internal security policies. By identifying the riskiest products in the environment, organizations can focus automation efforts on those that introduce the most vulnerabilities. In addition, the quick application of low operational risk patches also reduces the overall time to remediation improving vulnerability SLAs.

Lower Cost and Complexity
Endpoints are quickly and consistently patched, via the cloud, without the need for manual intervention and regardless of their location or connection to a corporate network reducing the cost of securing a prominent vector of attack. Eliminating the need to go over VPN for patching can be a significant cost saving.

"With cyberattack volume growing exponentially, integrating automation into your cybersecurity arsenal has moved from a nice to have to a must have," said Sumedh Thakar, president and CEO of Qualys. "As organizations implement zero-trust security frameworks, the ability to automate patching so they can better trust assets becomes a foundational aspect of their cyber defense strategy."

Availability
Qualys Zero-Touch Patch will be available in October as part of the Qualys Patch Management app. If you would like to sign up for the free Patch Management trial, visit qualys.com/patch-management-free-trial.

Additional Resources

- Read the Zero-Touch Patch blog
- View the Zero-Touch Patch video
- Sign-up for the Zero-Touch Patch webinar
- Learn about Qualys Patch Management
- Follow Qualys on LinkedIn and Twitter

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions with over 19,000 active customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes, and substantial cost savings.

The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance, and protection for IT systems and web applications across on premises, endpoints, cloud, containers, and mobile environments. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance. For more information, please visit www.qualys.com.

Media Contact:
Jackie Dutton
Qualys
media@qualys.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-introduces-zero-touch-patching-for-proactive-vulnerability-remediation-301375955.html

SOURCE Qualys, Inc.