ESET announces significant updates for ESET PROTECT Platform to help businesses keep ahead of attackers

The addition of Vulnerability and Patch Management powered by OPSWAT, enables businesses to tighten their defenses

DUBAI, UNITED ARAB EMIRATES, July 5, 2023 /EINPresswire.com/ -- ESET, a global leader in cybersecurity, today announces the upcoming availability of a significant enhancement to its unified cybersecurity platform, ESET PROTECT. The enhancement is designed to address both current and future digital security challenges for businesses worldwide. ESET has partnered with OPSWAT, a global leader in IT, OT and ICS critical infrastructure cybersecurity solutions to bring integrated vulnerability and patch management into the ESET PROTECT Platform. ESET Vulnerability and Patch Management has been added to existing ESET PROTECT Complete along with a brand-new tier - ESET PROTECT Elite – to better safeguard small and midsize businesses (SMBs) struggling to keep up with a constantly evolving threat landscape and ensure their systems are correctly patched.*

With centralized management from the ESET PROTECT Cloud console, organizations can easily assess security threats and manage patches across the entire network, ensuring timely detection and remediation of the latest zero-day vulnerabilities. Automated scanning and a wide range of filtering options enable organizations to quickly identify and focus on the security issues that mean the most to them. Further, with automatic and manual patching options, businesses can ensure that their endpoints are updated with the latest security patches in a timely manner.

"Due to the inefficiencies of legacy solutions, many SMBs struggle with managing patches and updates across their entire network. This leaves their endpoints open to attack. Plus, they find it difficult to identify and prioritize vulnerabilities based on severity," comments Michal Jankech, Vice President of SMB and MSP Segment, ESET. "SMBs want an easy-to-use solution that will keep them safe. The customizable patching policies in ESET Vulnerability and Patch Management give businesses of all sizes flexibility and control so that their endpoints can be optimally patched

promptly. This helps them minimize the risk of attack and ensures they can adhere to increasingly stringent cybersecurity insurance or regulatory requirements, plus meet the standard required for various ISO certifications."

ESET Vulnerability and Patch Management scans thousands of popular applications, such as Adobe Acrobat, Mozilla Firefox, and Zoom Client, for over 35,000 common vulnerabilities and exposures (CVEs). These automated scans can be scheduled using fully customizable vulnerability exception settings. Vulnerabilities can be filtered and prioritized based on exposure score, severity, and score over time. Through the ESET PROTECT Platform's cloud-based console, businesses can raise reports on the most vulnerable software and affected devices. It boasts multi-language support and only a light demand on IT infrastructure.

ESET Vulnerability and Patch Management provides a constantly evolving inventory of patches with patch name, version of the app, CVE, patch severity/importance, and affected applications. Businesses can launch immediate updates and begin patching via customizable options or manually when a patch has been identified. They can simplify the patching process further by prioritizing critical assets and scheduling the remainder to off-peak times to avoid disruption. Organizations can take advantage of the Vulnerability and Patch Management multitenancy functionality to enjoy full visibility over the entire network, yet be focused on a dedicated area.

ESET's unified cybersecurity platform, ESET PROTECT, is a single-pane-of-glass cloud console that provides centralized visibility, management, and insight. The ESET PROTECT Platform integrates balanced breach prevention, detection, and response capabilities with the company's industry-leading managed and professional services and threat intelligence. It is simple, modular, adaptable, and continuously innovated. With the launch of ESET PROTECT Elite, there are now five subscription tiers to the ESET PROTECT Platform for businesses of all sizes:

ESET PROTECT Entry – an entry-level solution with competitive pricing that includes endpoint protection, server security, and the ESET PROTECT Cloud console.
ESET PROTECT Advanced – providing first-class endpoint protection with advanced threat defense technology and full disk encryption.
ESET PROTECT Complete – includes the new ESET Vulnerability and Patch Management capability, cloud application protection, and mail security to minimize cyber risks.
New ESET PROTECT Elite – provides increased visibility and decreased cyber risks, ESET Vulnerability and Patch Management, ESET's native extended detection and response (XDR) capability, plus robust multifactor authentication.
ESET PROTECT MDR – an enterprise-grade solution that provides complete cyber risk management, robust threat hunting, and world-class ESET expertise on call. ESET PROTECT MDR combines the capabilities of the ESET PROTECT Elite tier with ESET managed security and professional services.

"As cyberattacks keep evolving and the industry becomes increasingly complex, our enterprise-grade offerings have transitioned to reflect changing business needs and a transitioning threat

landscape," adds Jankech. "Businesses of all sizes are increasingly finding it difficult to detect and patch vulnerabilities promptly to keep ahead of the bad guys. We are here to help. With the launch of ESET Vulnerability and Patch Management, we provide a pathway to swift remediation, helping keep disruption, and costs, down to a minimum for businesses."

"We're excited about this new step in our longstanding partnership with ESET. They've demonstrated consistent leadership in delivering best-of-breed security to the SMB market. Our endpoint technology helps protect over 150 million endpoints worldwide through our enterprise partners. ESET is a perfect partner to leverage our technology in the SMB market" commented Chad Loeven, OPSWAT's Vice President of Business Development.

*For ESET end users this functionality will be technically enabled in late July 2023.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

About OPSWAT
OPSWAT is a global leader in IT, OT and ICS critical infrastructure cybersecurity solutions and Deep Content Disarm and Reconstruction (CDR), protecting the world's mission-critical organizations from malware and zero-day attacks. To minimize the risk of compromise, OPSWAT Critical Infrastructure Protection solutions safeguard both public and private sector organizations with the latest technology, processes, and hardware scanning to secure the transfer of data, files, and device access across critical networks. More than 1,500 organizations worldwide spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations, and protect their reputation, finances, employees, and customers from cyber-driven disruption. For more information on OPSWAT, visit www.opswat.com.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/643056900