WatchGuard Speeds Zero Day Malware Breach Detection from Months to Minutes

New AI-based breach mitigation capabilities enable IT solution providers and midsized businesses to automatically detect and remediate zero day threats and evasive malware within minutes

SEATTLE – July 23, 2019– WatchGuard® Technologies, a global leader in network security and intelligence, secure Wi-Fi and multi-factor authentication, today announced a series of major updates to its threat correlation and response platform, ThreatSync, with latest release of Threat Detection and Response (TDR). These enhancements include accelerated breach detection, network process correlation and AI-powered threat analysis, enabling managed service providers (MSPs) and the organisations they support to reduce breach detection and containment timeframes from months to minutes, automate the remediation of zero day malware and better defend against targeted, evasive threats both inside and outside the network perimeter. "As cyber criminals increasingly leverage advanced, targeted attacks with evasive characteristics designed to circumvent basic anti-malware protections, midmarket organisations without adequate security expertise and resources rely heavily on trusted IT solution providers to rapidly and effectively respond to attacks," said Brendan Patterson, vice president of product management at WatchGuard. "These new ThreatSync capabilities arm MSPs with the tools they need to provide malware detection and response (MDR) services by detecting breaches in minutes and automatically mitigating advanced attacks for their customers, all through their existing TDR deployments." According to the Ponemon Institute, the mean time to identification (MTTI) for a security breach is 197 days, while the mean time to containment (MTTC) is another 69 days after initial detection. In Q1 2019 alone, zero day malware capable of escaping traditional antivirus (AV) solutions accounted for a massive 36% of threats, according to WatchGuard's latest Internet Security Report. With each passing day a security threat goes unnoticed, its potential to inflict both financial and reputational harm on an organisation increases drastically. The tight correlation between the Firebox appliances, TDR host sensors on endpoints, and WatchGuard's ThreatSync platform enables MSP's to offer automated mitigation for zero day malware attacks and automated identification of unknown processes connecting to malicious destinations. This means customers can rest easy knowing their trusted IT solution provider can detect breaches and remediate threats in just minutes. Key ThreatSync features now available via TDR include: Host Containment and Automated Response– ThreatSync quickly contains any host machine that's been compromised, shielding it from the rest of the business network. As soon as a threat is identified, Host Containment automatically takes action to control infections before they spread. Once contained, ThreatSync eliminates the malware by automatically killing processes, quarantining malicious files, and deleting associated registry keys. Accelerated Breach Detection– ThreatSync immediately identifies malicious files on all protected endpoints, and automatically begins remediation. This adds correlation with endpoint security that is not present in most comparable network security solutions. When users download unknown files from the web, the Firebox first submits them to APT Blocker, WatchGuard's next-generation cloud sandbox, for advanced analysis while host sensors on victim endpoints actively monitor them and the results are correlated with ThreatSync. Network Process Correlation– ThreatSync not only identifies and blocks connections to malicious destinations, but it also automatically responds to unknown processes responsible for them. With ThreatSync, malicious outbound connections blocked by WatchGuard's Firebox appliances are correlated to reveal the initiating endpoint and process, where the process is automatically terminated. This feature provides MSPs and network administrators with detailed contextual information on the network destination, service name, host name and process, allowing them to successfully respond and prevent future instances. Artificial Intelligence Analysis– ThreatSync uses new AI capabilities to automatically analyse and triage files, identifying those that possess suspicious characteristics before directing them to APT Blocker for further analysis. This minimises the time IT administrators spend managing alerts and prevents truly suspect files from going undetected, which allows MSPs and midsized organisations to identify and block real threats faster and with more confidence. Today, ThreatSync is licensed as part of the company's TDR service, which comes standard in all Total Security Suitedeployments. For more information, visit www.watchguard.com/TDR. About WatchGuard Technologies, Inc. WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com. For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard on Facebookor on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org. Subscribe to The 443 – Security Simplified podcast at Secplicity.org, or wherever you find your favorite podcasts. ###

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au
Patricia Gibson
02 9922 6820
mailto: patricia@basspr.com.au