WatchGuard Unveils Trusted Wireless Environment Framework to Help Businesses Build Fast, Scalable and Secure Wi-Fi Networks

New independent report from Miercom reveals most top Wi-Fi solutions can't automatically detect and prevent all six wireless threat categories

SEATTLE, WASH – September 18, 2018 –WatchGuard® Technologies (http://www.watchguard.com), a leader in advanced network security solutions, today launched its new Trusted Wireless Environment framework, a guiding resource businesses and solution providers can use to build Wi-Fi services that offer market-leading performance, scalable management and verified, comprehensive security capabilities. This new initiative seeks to upset the status quo in the wireless market, which has prioritised performance over security for far too long. Organisations that build Trusted Wireless Environments can enjoy the performance and scalability they need to run their business, while at the same time ensuring protection against today's most dangerous Wi-Fi attacks. "Wi-Fi networks have always served as low-hanging fruit for cyber criminals looking to steal valuable information, primarily because vendors and businesses alike have made the mistake of looking at Wi-Fi security capabilities as an added benefit, rather than a primary feature," said Ryan Orsi, director of product management at WatchGuard Technologies. "We're seeing a massive, industry-wide need to fundamentally reevaluate what we expect from Wi-Fi products, so we're advocating that businesses of every size – and even competing vendors – examine our framework for what it takes to build and operate a Trusted Wireless Environment. WatchGuard's cloud-based secure Wi-Fi products are truly unique in that they offer both industry-leading performance and unrivalled protection against every known category of Wi-Fi security threats, all delivered in a package that's easily managed and highly scalable." Trusted Wireless Environments WatchGuard's Trusted Wireless Environment framework helps organisations develop complete Wi-Fi networks that are fast, easy to manage, and most importantly, secure. Organisations today are faced with the inherent responsibility of establishing Trusted Wireless Environments that protect their employees, their customers, and their intellectual property from hackers who can easily exploit the weak or non-existent security of traditional Wi-Fi networks. Some chose to tackle this effort in-house, however, many small to midsize businesses and organisations elect to outsource their IT, including their Wi-Fi, to a trusted partner, which puts the responsibility for protecting that organisation on the VAR, MSP, or MSSP serving that client. The three core pillars of a Trusted Wireless Environment include: 1. Market-Leading Performance: Businesses should never be forced to compromise security in favor of achieving the level of Wi-Fi performance required to support user connections and client density within their wireless environments. 2. Scalable Management: With easy set-up and management, businesses should be able control their entire wireless network – regardless of size or complexity – from a single interface and execute key processes to safeguard the environment and its users. 3. Verified Comprehensive Security: Many vendors operate under a haze of ambiguity when it comes to advertising security capabilities offered by their Wi-Fi solutions. Businesses need proof that their security solution can provide automatic protection from the six known Wi-Fi threat categories, allow legitimate external access points (APs) to operate in the same airspace, and restrict users from connecting to unsanctioned Wi-Fi access points. Assessing the Security Capabilities of Top Wi-fi Solutions According to new research from Miercom (http://miercom.com), a leading, independent product test centre, WatchGuard's cloud-managed secure Wi-Fi solution is the only product on the market capable of automatically detecting and preventing every type of Wi-Fi security threat. These findings came from a new independent security assessment (https://www.watchguard.com/wgrd-resource-center/wifi-security-report) that examined four top Wi-Fi products for their ability to effectively prevent the six major Wi-Fi security threats: rogue access points, rogue clients, neighbouring APs, ad-hoc networks, evil twin APs (those with spoofed SSIDs), and misconfigured APs. This is the first Miercom assessment to analyse Wi-Fi products from a security perspective, illuminating significant issues with the built-in security of many wireless APs. "Following our in-depth security assessment of competing wireless products, Miercom is pleased to award WatchGuard's cloud-managed AP420 Wi-Fi solution with the Miercom Certified Secure accreditation for vastly superior performance in the detection and prevention of the top wireless security threats today," said Robert Smithers, CEO of Miercom. "It's clear that the performance comparisons we typically see for Wi-Fi solutions are missing key security criteria that could help customers make more well-informed buying decisions, so we believe the results of this never-before-done test speak to a critical need within the industry to reassess traditional Wi-Fi products from a security perspective." Miercom's independent assessment determined that WatchGuard was the only Wi-Fi vendor able to automatically detect and prevent all six wireless attack categories in just seconds, while maintaining performance. "Wi-Fi is an incredibly well-known and mature product category, and since most vendors offer highly similar offerings, it has become increasingly challenging for organisations like ours to meaningfully differentiate in the wireless services arena," said Kevin Willette, CEO at Verus. "WatchGuard's cloud-managed secure Wi-Fi products add a new dimension to our Wi-Fi services, allowing us to educate customers about unnecessary tradeoff between Wi-Fi performance and security found in other products, and offer them a solution that eliminates that compromise. With the Trusted Wireless Environment framework, we can bring clarity to previously ambiguous conversations about Wi-Fi security capabilities, and build wireless networks for customers that are not only fast, but safe and secure as well." In order to begin building Trusted Wireless Environments with WatchGuard's secure

wireless solutions, VARs and MSPs can purchase Secure Wi-Fi (https://www.watchguard.com/wgrd-products/secure-wifi/package-options) or Total Wi-Fi (https://www.watchguard.com/wgrd-products/secure-wifi/package-options) packages today. For more information about the need for greater security in the wireless market, download the full Miercom report here: https://www.watchguard.com/wgrd-resource-center/wifi-security-report.

Additional Resources: · Trusted Wireless Environment Solution Page: https://www.watchguard.com/wgrd-solutions/security-topics/trusted-wireless-environment · Report: WatchGuard Wi-Fi Security and Performance Validation: https://www.watchguard.com/wgrd-resource-center/wifi-security-report · Secure, Cloud-Managed Wi-Fi Brochure: https://www.watchguard.com/wgrd-resource-center/docs/watchguard-secure-cloud-wi-fi-en · Trusted Wireless Environment Solution Brief: https://www.watchguard.com/wgrd-resource-center/feature-brief/trusted-wireless-environment-en

About Miercom Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

About WatchGuard Technologies, Inc. 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: https://www.watchguard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard, on Facebook: https://www.facebook.com/watchguardtechnologies, or on the LinkedIn Company page: http://www.linkedin.com/company/watchguard-technologies. 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: https://www.secplicity.org/category/the-443, at Secplicity.org: http://www.secplicity.org, or wherever you find your favorite podcasts.

ENDS

Contacts

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