Security Operations Teams Get Relief From Alert Overload with the Trend Micro Vision One Platform

New threat defense platform provides centralized risk visibility and prioritizes alerts for faster detection and response

DALLAS, Feb. 9, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity, combats security alert overload and resource constraints with an extensible platform that provides visibility and response from a single console. The new platform, Trend Micro Vision One™, has extended detection and response (XDR) at its core and raises the bar with new capabilities to help security teams to see more and respond faster.

Organizations are struggling with siloed tools, disjointed alerts and stealthy, sophisticated threats, whether they have a Security Operations Center (SOCs) or are relying on stretched IT security teams for SOC functions. Trend Micro has helped hundreds of organizations identify and reduce cyber risk by correlating alerts across the entire IT environment, with the industry-first XDR solution launched in 2019. Now, with Vision One, Trend Micro is solving more complex security challenges with enhanced XDR, new risk visibility, new third-party integrations, and simplified response to threats across security layers.

"Our team had previously been simply overwhelmed with threat alerts they couldn't prioritize, hitting productivity and exposing our organization to extra cyber risk," said Aaron Cunningham, Vice President of IT, Glazer's Beer and Beverage. "We can count on Trend Micro to provide more context and less noise so they can react faster to the threats that matter. Their integration with our third-party SIEM provider means we can also drive value from existing investments."

With Trend Micro Vision One, organizations can maximize efficiency by making less sophisticated security resources operate at a more expert level. The new platform allows them to faster dissect security incidents, identify critical threat patterns and complex attacks and understand their overall security posture and trends, so organizations can proactively identify and assess potential security risks.

According to Gartner, *Innovation Insight for Extended Detection and Response*, March 2020, "Two of the biggest challenges for all security organizations are hiring and retaining technically savvy security operations staff, and building a security operations capability that can confidently configure and maintain a defensive posture as well as provide a rapid detection and response capacity. Mainstream organizations are often overwhelmed by the intersectionality of these two problems."

The holistic threat defense platform is true to its name, offering:

- Visibility & threat intelligence: Cross-layer detection models, along with security risk visibility supported by Trend Micro Research insights, enable enterprises to see complex attacks and particular points of security risk that siloed solutions miss. In preview, are new insights into SaaS application usage, their risk levels and trends over time.
- Purpose-built sensors: Native integrations with Trend Micro security stack across critical security layers.
- Fit with existing infrastructure: Out-of-the-box, API integrations with existing third-party solutions already in use to complement workflows.
- Simplified management: Ability to adjust security policies and drive response actions across security layers from a single console instead of swivel chair management

"Standing upon three decades of innovation, Trend Micro was at the forefront of the fast-growing XDR space. But as XDR solutions flood the market, we are going further and offering more," said Trend Micro COO, Kevin Simzer. "Our Trend Micro Vision One platform helps make good security teams great by easily identifying critical needs and enabling quick actions. This threat defense platform will continue to evolve in response to the changing threat landscape, and the infrastructure of our customers."

In addition to the layered security from Trend Micro, customers can easily connect this new platform into other security technologies such as third-party endpoint protection platforms and SIEM and SOARs, including new integrations with Fortinet, Microsoft Sentinel and Splunk just to name a few. Early adopting customers are ready to act on the developing opportunity to integrate beyond SIEM and SOAR, with solutions like firewalls, ticketing solutions, identity and access management.

This new blog from IDC resulted from a briefing prior to launch and goes into further detail on the new Trend Micro platform. To find out more about Trend Micro Vision One, please visit TrendMicro.com.

About Trend Micro
Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure

their connected world. www.trendmicro.com

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

Additional assets available online: Photos (1)

https://newsroom.trendmicro.com/2021-02-09-Security-Operations-Teams-Get-Relief-From-Alert-Overload-with-the-Trend-Micro-Vision-One-Platform