Written by Alice Marshall
08 August 2019

Trend Micro now offers detection and response capabilities integrated across email, network, endpoint, server and cloud workloads, giving enterprises broader visibility of risk posture while connecting minor events from different security silos.

The result, the company says, allows customers to detect more complex attacks that otherwise remain unnoticed. After all, a 2018 SC Media survey, security teams receiver over 10000 security alerts daily, while the Verizon 2018 Data Breach Investigations Report states “the mean time to identify a breach increased to 197 days and containing a breach increased to 69 days,” leaving criminals nearly 9 months hiding in an organisation and causing damage.

“The threat landscape is unrelenting and the skills gap is nearly unsolvable, so we have done more to help,” Trend Micro says. “Business security cannot rely on endpoints alone. Unlike legacy EDR offerings that ignore certain key threat vectors like email, we scale across more sources for the most complete detections generated as early as possible.”

The comprehensive XDR solution applies expert analytics to deep data sets collected from Trend Micro solutions across the enterprise, making faster connections to identify and stop attacks. The company adds in 2019 it identified a high number of attacks using lateral movement, with most bypassing the endpoint altogether, highlighting the need for centralised visibility. In addition, having one version of the security truth and a standardised schema for interpreting alerts makes life easier for security teams.

XDR is available as a managed service to augment an in-house team with Threat Micro Experts. Managed XDR provides 24/7 full threat analysis, threat hunting, response plans and remediation recommendations.

Go Trend Micro First to Deliver XDR Across Email, Network, Endpoint, Server and Cloud Workloads