IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Trustwave Introduces Elevated Crowdsourcing to the Mix by Adding Security Colony into their New MDR Offerings

June 17, 2022

By: Craig Robinson, Cathy Huang

IDC's Quick Take

The Managed Detection and Response (MDR) market offerings are not monolithic as there can be different levels of features within a providers' portfolio as well as vast differences between the growing number of Managed Security Service Providers (SPs) that have an MDR service. Trustwave's latest offering announcement includes some standard items that other managed security SPs can also claim to offer, but the inclusion of the Trustwave Security Colony offering is a differentiator.

Product Announcement Highlights

Trustwave announced on June 14, 2022, the next iteration of their two-tier offering of MDR services, which have evolved to include enhanced features and capabilities along with a new naming convention that starts with the base package. Trustwave MDR is targeted at small and medium enterprises while MDR Elite is for larger organizations..

Trustwave MDR includes standard MDR features, such as 24x7 monitoring, detection, prioritization, and investigation of their clients' hybrid multi-cloud environments for active threats and anomalies. 7 global SOCs provide response and the Trustwave SpiderLabs threat intelligence team can reverse engineer malware and performs threat hunting throughout their client's environment.

Trustwave MDR Elite layers on additional capabilities by bumping up the 5 million events per day (MEPD) of cloud-based security telemetry ingested for the Trustwave MDR offering up to a scaling EPD model, starting at 20 MEPD and supporting data collection from over 350 technologies with one-year standard of data retention. Both offerings include unlimited EDR telemetry ingestion and support via bi-directional API for over 35 cloud-based security tools. The Elite offering adds on service level objectives of 15 minutes for mean-time-to-acknowledge (MTTA) and 30 minutes for mean-time-to-respond (MTTR) for critical severity incidents with the response personalized to client-defined response protocols. Both services include a 99.9% platform availability SLA.

Trustwave Security Colony is a common offering between both MDR offerings that is a differentiator. This subscription offers a resource library with documents and videos to give guidance on a variety of cybersecurity needs, such as DevSecOps, incident response, cloud security, policy documents, security testing, and more. Topics in their video library include threat and response forecasting, privacy and GDPR, business email compromise, and other topics. Free, open source, and commercial tools are made available in their vendor risk assessment offering. Maturity assessments, ransomware readiness assessments, breach monitoring round out their online portfolio, and a personal security consultant is also available to answer quick questions.

IDC's Point of View

IDC recognizes that the MDR market is maturing, and the managed security SPs and MDR providers are seeking out ways to differentiate their offerings from their competitors. Common marketing talking points, such as advertising 'full' response rather than just issuing a ticket into their clients help desk system to research or resolve a potential attach, providing full remediation, or quicker times to acknowledge, detect, and respond to alerts are common ways that managed security SPs and MDR providers utilize to show off their capabilities.

Whether an organization is utilizing an MDR service to provide the critical 'DR' features of detection and response to alerts in their ever- expanding risk surface, or if it is utilizing an XDR platform and utilizing their own staff to do the monitoring, detection and response functions, there are still other cybersecurity functions that need to be performed. Building out playbooks, doing risk assessments, understanding the security standing of key suppliers, or undergoing periodic maturity assessments are just a handful of the tools that are part of Trustwave's Security Colony.

CISOs and CIOs, especially in the mid-market, will be able to testify about the pain points of building from scratch, or borrowing from another trusted colleague in the cybersecurity arena, a policy document or assessment checklist that they can utilize to provide some structure around their program. Trustwave has essentially crowd-sourced, from their own practitioners, the documents and tools that CISOs can quickly adopt to elevate their cybersecurity program.

The hidden gem of Trustwave Security Colony finally gets its day in the sun by being packaged up in both tiers. Yes, having a dedicated client success manager in both tiers is nice, and the security engineers that sharpen the analytics, rules and policies for optimal performance and detection is a welcomed feature, but the true differentiator in this announcement is the inclusion of Trustwave Security Colony.

The two-tier of MDR services (i.e. MDR and MDR Elite) are well positioned in the respective market segments, reflecting Trustwave's mature understanding of different buying preferences of the customers. Trustwave has previously said that they were going to shift their strategic focus onto advanced offerings such as MDR, and this announcement shows that they focused on elevating their position in an increasingly competitive market.

Subscriptions Covered:
Security Services