Sophos unveils Rapid Response service aimed at helping organizations eradicate active attacks and threats

Analysts - Aaron Sherrill

Publication date: Friday, December 18 2020

Introduction

Drawing on the managed detection and response expertise it acquired from Rook Security last year, Sophos has launched Rapid Response, an incident response service designed to provide organizations with a dedicated team of specialists equipped to quickly stop advanced and active attacks and threats. Sold via partners and delivered by the vendor's analysts and threat hunters, the service aims to offer expert short-term security assistance at predictable rates without retainers or long-term contracts.

The 451 Take

According to 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020 survey, incident response expertise is one of the top security-related skillsets missing from most security and IT teams, second only to cloud platform expertise. This should be unnerving for organizations as they expand their attack surface and rapidly adopt new computing paradigms such as the cloud. A security incident can be a costly event, both financially and through damage to the organization's brand and reputation. And failing to respond to security incidents with knowledge, speed and efficiency can result in a situation that can be worse than the breach itself.

Sophos' recently launched Rapid Response service provides channel partners with a service that should appeal to both small and midsized businesses as well as larger organizations. With a unique flat-rate pricing structure and 45-day engagement window, the remote service helps fill a gap for incident response services in the SMB space and gives the company an additional avenue to expand its managed threat detection services business.

Context

According to Sophos, organizations of every size are struggling to find and retain skilled staff. The company discovered that 81% of enterprises point to finding and retaining skilled IT security

professionals as a major challenge to their ability to deliver IT security, with over one-quarter of organizations identifying it as the greatest challenge they are facing.

This finding aligns with our VotE: Information Security, Organizational Dynamics 2020 survey, where 53% of enterprises report that current infosec staffing levels are inadequate to address the challenges facing their organizations. Unfortunately, only 14% of organizations plan to add to their infosec staff over the next 12 months.

In response, Sophos has designed its services portfolio to fit the needs of customers and fill gaps in expertise regardless of the organization's security capabilities. For organizations that have security expertise, the company offers its Intercept X Advanced with EDR tool for security teams to conduct their own threat hunting, detection and response activities. For organizations that have a lean security team or lack expertise, the company offers Managed Threat Response (MTR), a 24/7 threat hunting, detection and response service delivered as a fully managed, proactive service. And for teams that need help during a security incident, the company now offers Sophos Rapid Response.

Rapid Response

Sophos Rapid Response is an on-demand, fixed-fee, remote incident response service designed to triage and neutralize attacks and threats. The vendor says the service is structured to accommodate businesses of all sizes, including small and midsized organizations, which have largely been underserved by legacy products available in the market. Rapid Response features a simple pricing model based on the total number of users and servers and provides unlimited incident response services for 45 days. Available to both existing and non-Sophos customers, the service is designed to commence response activities within hours of a customer engaging the firm for help.

Officially introduced in October, the service was in beta for nine months. With no marketing, announcements or advertising, Sophos says it experienced tremendous demand for the service throughout the pilot period.

Sold via partners and delivered by Sophos' analysts and threat hunters, Rapid Response leverages Intercept X Advanced with EDR, the vendor's flagship endpoint protection offering, to assess an organization's environment, identify indicators of compromise or adversarial activity, collect data, perform investigative activities, stop damage to assets or data, and prevent any further exfiltration of data. For customers that do not have Intercept X already installed in their environment, the service includes Rapid Deployment – a team of experts that can quickly install the offering in environments that are currently experiencing an active incident. While Rapid Deployment is being performed, the Rapid Response team can begin to take remedial actions to contain and neutralize the threat while the deployment is completed.

Sophos has designed the service around speed. From the moment a customer first contacts the firm for assistance with the eradication of threats and attacks, Sophos notes that its primary goal is to get customers out of the danger zone as quickly as possible.

The vendor reports that a majority of cases are handled within a matter of days – however, it will continue to defend and respond to any cybersecurity incidents during the 45-day subscription term. Once the threat or attack has been eradicated, customers are transitioned to Sophos' MTR Advanced service for the remainder of the 45-day engagement. During this time, the company monitors the customer's environment and offers 24/7 proactive threat hunting, investigation, detection and response. It says this gives customers assurance that threats have been neutralized and that any follow-up attacks will be detected.

This also provides Sophos with an opportunity to convert Rapid Response engagements into fulltime MTR customers. The vendor saw over 50% of Rapid Response customers subscribe to its MTR services during the pilot period.

Rapid Response focuses on the incident response aspect of digital forensics and incident response (DFIR) services and does not include all of the services typically offered in a traditional DFIR engagement, such as forensic imaging, evidence collection, or expert witness services. According to Sophos, less than half of incident response engagements require full DFIR services. However, the firm works closely with DFIR service providers when such services are required by the customer.

Partners

According to Sophos, partners have eagerly embraced Rapid Response. While a few of its partners have the expertise, skills and capacity to deliver incident response services, the majority do not. The service gives partners another service that can further engrain them within their customer base and fills a gap many have in their services portfolio. Although partners receive compensation for reselling Rapid Response, the service often leads to additional opportunities for partners such as MTR services, new projects, and security assessments and consulting.

Competition

Incident response services are offered by a growing number of players ranging from local MSPs and MSSPs that often have limited skills or capacity to global SIs that promise to have feet on the ground within 48 hours. Service offerings often require organizations to engage a provider prior to the need for incident response services to establish a relationship. These services often require customers to purchase other services from the provider, pay for an annual retainer, or prepay for a block of incident response hours. Unfortunately, most organizations do not seek incident response services until they are hit with an attack or experience a breach. In those instances, organizations are seeking a supplier that can deliver incident response services immediately.

Sophos faces competition from a broad range of vendors, including those that specialize in incident response and managed security services, as well as consulting firms, SIs, and product providers. Companies like Accenture, CrowdStrike, Crypsis (Palo Alto Networks), Deloitte, FireEye, IBM, Kroll, Optiv, Rapid7 and SecureWorks offer various forms of incident response services. Sophos will also encounter local and regional players like LBMC, NXTsoft, Praetorian, NetMagic and C-Spire.

SWOT Analysis

Strengths	Weaknesses
Sophos' Rapid Response service should be attractive for both its partner base and its broader end-user organizations. The fixed-fee, 45-day engagement model is unique in a market that is known for open-ended hourly pricing models, annual retainers and, at times, delayed response. As the service is designed to quickly respond to incidents, customer onboarding reportedly starts within an average of two hours of initial contact and triaging occurs within 48 hours.	The lack of full DFIR capabilities will not be an issue for most customers. The focus on incident response enables the vendor to offer services that are cost-effective for small and midsized organizations. However, Sophos may benefit from partnering with a DFIR provider for an advanced incident response offering.
Opportunities	**Threats**
While Rapid Response was just recently launched, Sophos has many opportunities to expand its offerings around incident response, including providing incident response readiness assessments, incident response plan development, and gap assessments. On a broader scale, the firm may find partnering with cybersecurity insurance providers to be a significant market opportunity.	Sophos believes there is high demand for incident response services. As the vendor rolls the service out to a broader market, it may find that demand exceeds its capacity to respond, a threat that impacts incident response suppliers of all types. Sophos will need to continue to mature its offering and ensure that it can scale to meet demand while remaining cost-effective.

Source: 451 Research, LLC