REPORT REPRINT

Alert Logic continues to expand and evolve its MDR services and capabilities

JANUARY 13 2021

By Aaron Sherrill

Alert Logic has introduced a number of new capabilities and advancements to its MDR platform over the last few months. The company believes its consistent and rapid pace of innovation and cloud coverage helps to ensure organizations are well-equipped to address and adapt to the ever-evolving security landscape and improve business outcomes.

451 Research

S&P Global
Market Intelligence

Introduction

Managed detection and response (MDR) providers are rapidly expanding and adapting their capabilities to detect and respond to threats, regardless of workload location or underlying technology. At the same time, MDR providers are seeking to simplify the user experience, address a greater number of compliance requirements, digest a broader scope of telemetry streams, augment technology and human intelligence, and grow and expand partnerships. Following this recipe, Alert Logic has introduced a number of new capabilities and advancements to its MDR platform over the last few months. The company believes its consistent and rapid pace of innovation and cloud coverage helps to ensure organizations are well-equipped to address and adapt to the ever-evolving security landscape and improve business outcomes.

451 TAKE

As the MDR sector continues to mature, significant growth opportunities exist for MDR providers of all types and sizes. But those that can quickly adapt and scale operations, detect and respond to threats across a broad number of threat vectors, leverage analytics, meet regulatory requirements, deliver transparency, and provide an integrated and automated platform from the cloud should find themselves with a clear market advantage. With the continued progression and evolution of its MDR capabilities, Alert Logic is seeking to detect and respond to threats across the entire expanding enterprise attack surface and deliver the outcomes that organizations are striving to achieve. The company's MDR service provides a growing range of capabilities that enable organizations to detect and mitigate threats across their diverse IT environments, regardless of their level of expertise. The company appears to have momentum moving into the new year, and expansion of the platform's capabilities and integrations to provide a broader range of incident response capabilities could prove to be beneficial for both its partners and enterprise customers.

Context

Founded in 2002, Alert Logic is headquartered in Houston with offices in Austin, Texas; Cardiff, UK; London; and Cali, Colombia. The company reportedly provides services to over 4,000 organizations globally, touts 20% YoY growth, and says it has no debt.

Alert Logic's SaaS-enabled MDR platform is designed to reduce both the likelihood of attack and the impact of successful attacks. The platform's coverage spans clouds, networks, applications and endpoints, providing real-time insights into risks, vulnerabilities, remediation activities, configuration exposures and compliance status.

Over the past few months, Alert Logic has introduced a number of new capabilities and advancements to its MDR platform designed to enhance visibility, simplify the user experience, accelerate response, and expand insights into security blind spots. The newly released capabilities aim to ensure organizations are well equipped to address and adapt to the ever-evolving security landscape.

Automated response: Alert Logic recently announced the availability of expanded and enhanced automated response capabilities on its MDR platform starting in Q1 2021. With embedded security automation and orchestration capabilities and manual approval processes, the company is aiming to provide a safe bridge for organizations to transition to automated response in a methodical manner. Initially, automated response will be able to block attackers, isolate hosts, disable user accounts

and remediate certain vulnerabilities. Automated response capabilities will be available for public cloud (AWS and Azure) infrastructure in Q1, and the company has plans to expand into on-premises infrastructure (including EDR, Active Directory and firewalls) in Q2.

Alert Logic's automated response capabilities will include a library of predefined playbooks and templates, as well as a playbook builder for customers to create custom automated response actions. The company is also planning to release an accompanying app to enable customers to review and approve automated actions from anywhere.

File integrity monitoring (FIM): FIM detects unauthorized changes to operating systems, content and application files, and system registries. Alert Logic's FIM monitors file creation and modification dates and times, unauthorized access to files, security permission changes, registry changes, and changes in system binaries and configuration files. In addition, FIM helps organizations meet regulatory and compliance requirements for PCI-DSS, SOX, NIST SP 800-53, HIPAA, SOC 2 and HITRUST.

Web log analytics (WLA): According to Alert Logic, custom web applications are prevalent in most organizations. Unfortunately, most of these web apps are fraught with vulnerabilities that provide attackers weaknesses to exploit and potentially gain access to critical assets. WLA, a log-based threat-detection tool, is designed to gain visibility into web applications, discover anomalous activities and detect attacks.

Log review: The company has enhanced its log review capability combining machine learning and human expertise to detect incidents based on an organization's trends and patterns at the account, user and host levels, as well as provide guidance, customer tuning recommendations and manual verifications.

DevNet developer portal: Alert Logic says it has seen an increase in the number of customers seeking to embed and extend its MDR platform deeper into their organization's security fabric. While Alert Logic's MDR platform is built on an API-centric architecture, the new developer portal includes a toolkit of command-line tools, programming language integrations, in-depth documentation and use cases to help customers embed and integrate the platform quickly. Alert Logic sees the portal as a key feature for enterprises with sophisticated security teams, as well as MSPs and MSSPs looking to provide added value and automate managed detection and response at scale.

Connectors: With universal webhooks and email connectors, Alert Logic can now connect to many third-party ticketing systems such as Jira and ServiceNow, as well as messaging systems such as Microsoft Teams, Slack and PagerDuty. The platform can directly send incidents, observables and response notifications, enabling customers to streamline and automate coordination efforts and follow incidents from start to finish. Notifications can be granularly configured based on characteristics such as payload type, severity and attack class to ensure that only pertinent information is being communicated.

AWS Network Firewall integration: Alert Logic recently announced integration with AWS's new Network Firewall, a managed network firewall service that enables AWS customers to detect and block malicious activity across AWS virtual private clouds. Through the integration, Alert Logic is providing web application threat-detection coverage and access to Alert Logic rules, eliminating the need for users to research, develop and maintain individual rulesets or monitor for attacks.

Expanded partner program: In August, the company added a new tier to its Partner Connect program, designed specifically for MSPs. The expanded program provides MSPs with a number of benefits, including access to flexible licensing, go-to-market toolkits and campaigns, branded security assessments, and SOC integration and automation.

Competition

Competition in the managed detection and response space is broad and diverse, ranging from pure-play MDR providers to systems integrators. Alert Logic's most direct competition comes from other pure-play MDR providers such as eSentire, Arctic Wolf, Perch Security (acquired by ConnectWise), Red Canary, Expel, Critical Start, Paladion (acquired by Atos) and Proficio. But the company also faces competition from a growing number of traditional security technology vendors that are broadening their portfolios with security services such as MDR. These include vendors such as Sophos, Rapid7, Cisco and TrendMicro. At the same time, MSSPs, SIs and VARs – including Verizon, Lumen, SecureWorks, AT&T, Booz Allen Hamilton and Accenture – are seeking to capture a part of the growing MDR market.

SWOT Analysis

STRENGTHS

Alert Logic is a well-known brand in the security services market. The company's SaaS-enabled MDR platform supports AWS, Azure, Google's Cloud Platform, hybrid and on-premises environments, providing comprehensive coverage for increasingly diverse IT ecosystems.

WEAKNESSES

Alert Logic's recently expanded automated response capabilities closes a gap in the company's MDR offering. The company will need to rapidly expand its automated response capabilities to incorporate a broader range of security technologies and response use cases.

OPPORTUNITIES

Expanding partnerships, especially with service providers like MSPs and MSSPs, will broaden the company's market reach and be a force multiplier in its expansion efforts. The company's new partner tier for MSPs/MSSPs along with its automated response capabilities should be attractive for service providers that have unique needs and are seeking capabilities that can help them scale their operations.

THREATS

Managed detection and response is a growing area of interest from organizations of every size and industry, fueling both startups and M&A activity. The various approaches to MDR, and now XDR, will require Alert Logic to continue expanding the capabilities of its platform and demonstrate its advantages over other approaches and vendors.