REPORT REPRINT

AlienVault rides the cloud to unify security management

ERIC OGREN

14 MAR 2017

Security operations are in danger of being left behind, guarding on-premises networks while SMBs migrate their critical applications to the cloud. AlienVault's USM Anywhere offers centralized security information and event management for resource-constrained organizations embracing Amazon and Microsoft cloud architectures.

451 Research®

The complexities of managing security are excessive for most organizations that cannot envision staffing expensive security operations centers. For such organizations, investing in on-premises security management products is often a nonstarter. AlienVault starts where the customer's infrastructure is already going – with a low entry cost, cloud-based security operations service that is positioned to secure application infrastructures as they transition to cloud and hybrid environments.

THE 451 TAKE

Meeting compliance mandates as organizations shift applications and regulated data into the cloud often serves as a major incentive to reevaluate an organization's security information and event management (SIEM) strategy. Our research shows security teams in larger enterprises commonly use support of cloud applications to bring in new SIEM vendors to coexist with their legacy land-locked SIEM deployments. Implementing security management as a service allows growing organizations of all sizes to avoid the expenses and headaches of acquiring, deploying and maintaining even more security products. AlienVault has extended its security management capability with AlienVault USM Anywhere's ability to offer customers centralized management for on-premises infrastructures and for workloads executing in Amazon Web Services and Microsoft Azure Cloud. The new product features allow organizations to meet security and compliance goals as their infrastructure evolves into the cloud. Mission-critical security management applications should be in step as mission-critical applications migrate to the cloud and hybrid-cloud architectures.

CONTEXT

AlienVault recognized that enterprises with no readily available team of security experts to chase security alerts have been underserved by the security industry. These organizations still require many of the same security management features as large enterprises for compliance and security oversight. The ability to manage data for compliance, analyze stored data to better detect threats, and efficiently respond to security incidents are prime tenets of AlienVault installations.

The company was founded in 2007 in Madrid, Spain, and has since opened worldwide headquarters in Santa Clara, California. The vendor has raised approximately $118m in investment capital. Prior to the launch of USM Anywhere, AlienVault's key differentiators were its open source capability and its Open Threat Exchange (OTX).

The open source licensing for AlienVault technology has helped penetrate managed security service providers, a key channel for reaching resource-constrained organizations. The open source model allows MSSPs and enterprises with experienced security teams to more easily customize AlienVault to the needs of the business.

AlienVault's OTX establishes an environment of sharing threat intelligence. This community resource is fairly unique among SIEM vendors, and helps AlienVault customers identify and protect against emerging threats. AlienVault reports more than 50,000 participants in its OTX community.

PRODUCTS

AlienVault USM Anywhere has features designed specifically to monitor security for cloud and hybrid-cloud architectures in organizations constrained by budget and staffing resources. USM Anywhere delivers the essential features of asset discovery, vulnerability assessment, intrusion detection, applied behavior analytics, SIEM and log management.

The primary benefit of USM Anywhere is the ability to integrate AWS and Azure-based applications into a centralized logical security management tool. Customers can satisfy compliance requirements for security management of the cloud while avoiding the expenses of deploying software and servers in a datacenter. Sensors supporting Amazon Web Services and Microsoft Azure Cloud, as well as hypervisors from Microsoft and VMware, provide application information from both cloud and on-premises datacenters to help organizations centrally manage their security.

Dynamic incident response templates allow AlienVault customers and MSSP partners to help enterprises respond to security incidents quickly and effectively. We like the positioning of automated response features, and the establishment of incident response playbooks to guide non-security professionals. In fact, we can envision the AlienVault installed base setting a community activity center for playbook exchange following the OTX concept.

AlienApps provides a layered capability for AlienVault to deliver customization features. AlienApps is designed to help customers, MSSPs and partners enhance the functionality of USM Anywhere, such as with automatic action responses, data visualization or orchestration of incident response. AlienApps includes features integrating with security tools such as Cisco Umbrella and Intel McAfee ePO. We believe AlienVault can use the concept of AlienApps to deliver future, separately priced add-ons to its customers.

AlienVault Secure Cloud provides a focal point for Elastic-based data storage, security analytics and threat detection. We would expect to see more of the Elastic-based capabilities appear in on-premises versions of AlienVault.

COMPETITION

We have seen securing data and user access to AWS and Azure-based applications drive enterprise evaluations of new SIEM technology. Even large enterprises with a deployed SIEM product often pause to reevaluate the incremental costs of managing security for cloud applications. It makes sense for medium-sized businesses to be sure any SIEM product can enable AWS and Azure workloads.

We see AlertLogic, Rapid7 and SumoLogic as the closest competitors to AlienVault USM Anywhere. Each offers SIEM services at favorable price points, and is designed explicitly for the needs of midmarket enterprises with compliance requirements. The AlienVault Secure Cloud environment positions AlienVault to host additional security applications to derive more value from their customers, similar to the AlertLogic and Rapid7 approaches.

Most of SIEM are product sets designed for the needs of large enterprises with trained security operations teams and robust security budgets. Products from vendors including Hewlett Packard Enterprise ArcSight, IBM Q1, Intel/McAfee, LogRhythm, RSA and Splunk tend to be platforms requiring customization and training before customer value can be realized. While they offer support for AWS and Azure, the products are designed to scale to the needs of large enterprises.

Interesting sets of competitors are starting to arise with disruptive storage approaches based on Elastic and Hadoop architectures. Traditional SIEM vendors have consumptive pricing models built on the amount of data under management. However, data volumes with modern products have exploded, making traditional SIEM products pricey. One of the primary attractions of products from Exabeam and Securonix, for example, is disruptive pricing tiers for the low-value, high-volume data that dominates security management.

SWOT ANALYSIS

STRENGTHS

AlienVault USM Anywhere allows security teams to manage the security of their AWS and Azure cloud-based applications as if they were on-premises. We also like that the service enhances enterprise security operations without the need for administering software updates.

WEAKNESSES

We believe AlienVault can get more mileage out of AlienApps, perhaps introducing specialized applications integrated with USM Anywhere, and over time commodifying those applications according to market conditions.

OPPORTUNITIES

There is an opportunity to displace incumbent SIEM vendors based totally on the ability to simplify management of AWS and Azure applications. Organizations are concerned with how they meet security obligations in the cloud, and AlienVault USM Anywhere may give them reason to reevaluate their SIEM strategies.

THREATS

Larger SIEM vendors with greater brand recognition and marketing budgets will compete for medium-sized businesses.