Market Insight Report Reprint

Uptycs adds use cases to its security analytics offerings

September 27 2021

by Fernando Montenegro

The increased demands on security teams means there is a need for security analytics at scale, crossing areas such as endpoints and the cloud. This is the space that Uptycs is moving into, as it expands its osquery-based offering into a broader set of use cases, notably cloud workload security and cloud security posture management.

451 Research

S&P Global
Market Intelligence

Introduction

'Necessity is the mother of invention' is a well-known saying. In the context of securing modern infrastructure, the twin demands of depth of coverage as well as security assets at scale has driven security teams to adopt a much more 'engineering centered' approach that capitalizes on the use of structured data, automation and streaming analytics.

This was evident back in 2014, when Facebook originally released the osquery agent, which startup Uptycs used as the basis for its security analytics offering. Now, the company has expanded beyond that use case, and is positioning Uptycs as being able to address additional use cases, including cloud security needs and extended detection and response (XDR).

THE TAKE

One of the key trends in modern environments is the push to handle more scale with automation, be it with claims about AI or more data-engineering-centered streaming analytics. For some larger companies, applying this to endpoints – be they end-user compute or server workloads – was Uptycs' original proposition. The company has built on the foundation it originally created with endpoint-centric use cases to now include cloud infrastructure, container orchestration and other domains, which moves it closer to the heart of what XDR is supposed to address (at least from the perspective of data sources). The key challenge for the company is stepping into a space that is heavily contested by much larger vendors, with larger mindshare and teams doing security operations the traditional way. Beyond checking off the necessary functionality checkboxes, Uptycs will need to find alignment with security operations teams that have a corresponding mindset about increased automation and structured data at scale.

Context

Uptycs is based in Waltham, Massachusetts, and was founded in 2018. The company employs roughly 125 people, with a presence in the US, Canada and India. Uptycs' executive team is led by CEO Ganesh Pai, who comes from Akamai, where he was chief product architect, and Uma Reddy as VP of engineering, with previous roles at Kaybus and Sonus.

Uptycs recently announced series C funding of $50m, bringing its total funding to date to $93m. The latest round was led by Norwest Venture Partners, with further participation by Sapphire Ventures and ServiceNow Ventures. 451 Research estimates current annual recurring revenue to be in the $10-15m range.

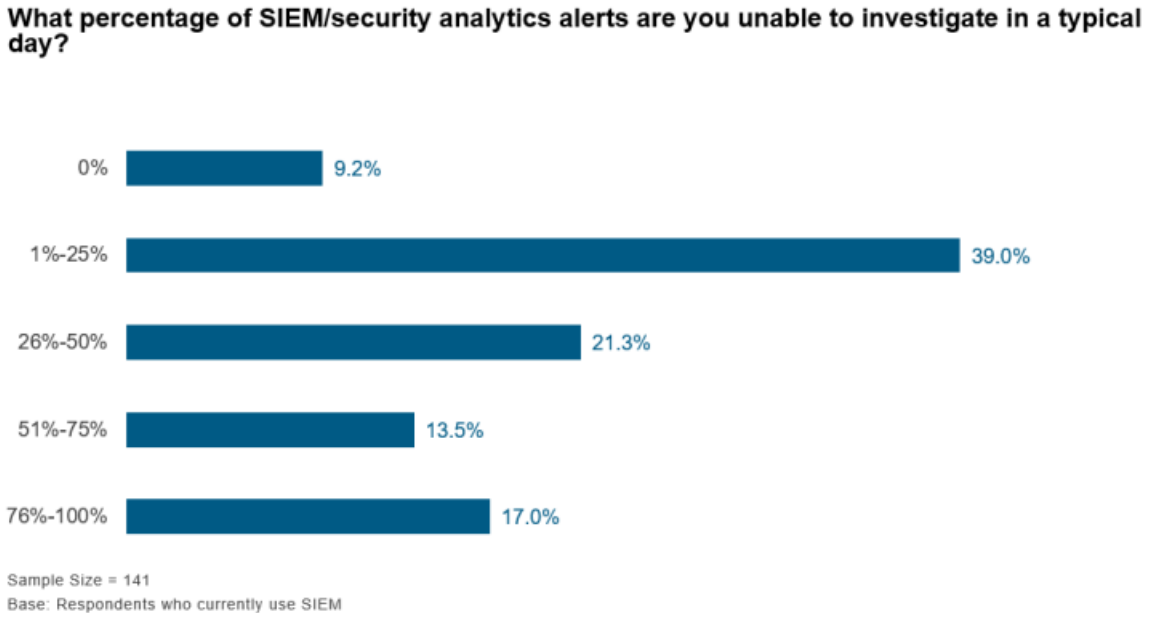
Market

Uptycs initially provided endpoint-focused security capabilities, but has now moved to positioning itself in the extended detection and response (XDR) category. XDR has emerged as an approach closely associated with the evolution of security operations, particularly the use of multiple sources of telemetry for analytics and response.

Vendors in XDR are aligning across three broad groupings: vendors with a managed services background that have custom-built integrated technology stacks that customers can rely on; vendors with products in one or more telemetry sources (endpoint, network, email, cloud and others) that are enhancing their capabilities around analytics and integrations; and vendors with a primarily analytics background that are working on integrating many different telemetry sources. Uptycs fits in between these latter categories.

The potential appetite for XDR arises from the increased demands on security teams. As an example of the demands placed on them, 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations survey found that when these teams are asked how they are faring, less than 10% indicated they are able to investigate all the alerts coming into their systems on a regular day.

Few organizations can handle all inbound security alerts



Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020

Strategy

Uptycs proposes that the needs of modern deployment architectures include a mixture of proactive, reactive, predictive and protective use cases, and that this combination requires a cloud-native security analytics offering, particularly one that can support high degrees of automation by security teams as they look to address issues at scale.

The company continues to pursue security teams as the key stakeholder within the organization, but is focusing on teams that can incorporate more automation and analytics into their workflows. It says this means it has broad applicability across verticals. Uptycs indicated it is growing rapidly both in terms of customer base and deployment footprints within existing customers. It says its next steps are to continue work on newer telemetry sources. Additional cloud platform support, Kubernetes as the control plane for container orchestration, and support for identity management data are three key areas.

Technology

The main idea behind Uptycs is using a cloud-native security analytics infrastructure to interface with different sources of structured data collected via streaming from agents or API collectors, then performing different real-time and historical analytics functions. The company started this by supporting endpoint security functionality using the osquery agent, primarily for Mac and Linux workloads (Windows was also supported), but has now expanded its sources of structured data to additional domains.

Uptycs is currently looking to address different use cases across modern deployments, which often consist of several thousand endpoints and applications in different environments. Focusing on those endpoints, it offers functionality that aligns with endpoint detection and response (EDR) and cloud workload protection, depending on the type of workload. The company has now added support for cloud security posture, asset inventory and insights, and audit, compliance and governance use cases across different types of data. With that, it touches on the needs typically associated with XDR.

Uptycs is consumed as a SaaS. The cloud-based infrastructure powers processing, storage and analytics workflows, while data from sources comes either from agents installed on the workloads – which can be polled periodically or set up to stream event data such as new processes, network activity and file changes – or from the push and pull of structured data from API access to additional data sources. These data sources include the management APIs for cloud providers such as AWS (Azure and Google support is on the roadmap), Kubernetes clusters, and identity providers and SaaS offerings such as GitHub, on the roadmap.

The Uptycs agents support Linux, Mac and Windows environments, and can run in bare metal, virtual machines or containers. They periodically collect data including hardware and system configurations, and user, network and process activity, and can also stream system events. An add-on called Uptycs Protect gives the agent write access for blocking (processes and network domains) and remediation actions. Cloud information can include asset details, activity from API logs (Cloudtrail) and traffic logs (VPC flow logs).

Uptycs aggregates information in a proprietary graph database, but makes information available via normalized tables that are well suited for querying. As data is made available on the centralized storage layer, users can look at both individual asset details and fleet-wide behavior through asset insight pages and queries.

The key functionality supporting EDR use cases includes the querying of numerous endpoint tables covering a wide range of data, from regular hardware details up to process information, creating alerts and behavioral rules that flag on different conditions (Uptycs supports YARA rules commonly used by security operations teams), aligning the information to the MITRE ATT&CK framework, and supporting investigative actions such as carving out files or memory segments (on Linux and Windows systems).

The Uptycs Protect add-on enables remediation on live systems, including disabling users, quarantining a device, killing a process, or deleting a file. It ships with numerous prebuilt rules covering different scenarios and use cases, including MITRE ATT&CK techniques and sub-techniques, file integrity monitoring, some support for application whitelisting, and threat intel correlation.

The new cloud security functionality provides asset visibility into AWS, as well as ingestion of CloudTrail and VPC Flow logs, then provides functionality for asset analysis, configuration analysis (it currently supports approximately 40 AWS services), compliance to CIS benchmarks (other targets are planned) and threat intel correlation for flow logs. Comparable support for GCP and Azure is expected in the second half of 2021.

The company is working to add support for additional data sources, specifically identity data from sources such as Okta, Ping, Microsoft and Google, and user activity data from key SaaS offerings such as GitHub, Office365, Google's Workspace and Salesforce.

Competition

Well-established large vendors in the XDR space include Palo Alto Networks, Microsoft, Trend Micro, SentinelOne, Cybereason, FireEye, VMware, McAfee, Cisco, Check Point, Fortinet, CrowdStrike and Qualys. Other competitors in the space include vendors focused on analytics aspects, such as Hunters, Confluera, Stellar Cyber, Senseon and Kognos.

XDR as a category has also attracted attention from vendors like Securonix, Exabeam, LogRythm, Vectra, LogPoint (via SecBI) and Cynet. Services-centric vendors include ReliaQuest, ArcticWolf, Red Canary, Expel and Secureworks.

The cloud-centric competition for Uptycs brings up many of the same names from XDR offerings (including but not limited to Palo Alto Networks, Trend Micro, Check Point and Sophos), but also more cloud-specific names such as Aqua Security, Lacework, NeuVector, Wiz, Concourse Labs, JupiterOne, Datadog, Fugue and Orca Security. The offerings from the cloud providers themselves – notably AWS, Microsoft Azure, Google Cloud, IBM Cloud and Oracle Cloud – are also competitive within the scope of their environments.

Uptycs is looking to differentiate based on number of use cases and its cloud-native architecture, which it argues is well suited for dealing with both the increased scale that teams must deal with, as well as the increased use of automation within workflows.

SWOT Analysis

STRENGTHS

Uptycs' offering has been built from the beginning with the goals of being able to support large-scale and increased automation, and support for newer use cases fits into this model.

WEAKNESSES

Besides visibility in a crowded market, the key challenge for Uptycs is to balance high-volume ingestion and automation with providing meaningful analytics and capabilities across an organization's multiple use cases, stakeholders and workflows. Its improvements in correlation support will be critical for XDR use cases.

OPPORTUNITIES

As organizations look to address their increased demand for security analytics, the combination of providing structured access to data and being automation-friendly is being looked upon favorably as the building blocks of more modern security operations practices.

THREATS

Two key trends stand out. First, customers indicate they favor streamlining their vendor management, which helps incumbents and larger vendors. Second, the competitive landscape for cloud security use cases and broader XDR is extremely busy, with larger security vendors, startups and services vendors jostling for position.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence