REPORT REPRINT

Uptycs emerges from stealth betting on SQL-based osquery for upending endpoint security

FERNANDO MONTENEGRO

05 JUL 2018

Since being released as open source by Facebook back in 2014, osquery has attracted interest as a component for making it easier to manage Mac, Linux, and eventually Windows endpoints. Still, organizations faced some heavy lifting to put it in production. Startup Uptycs aims to address this challenge, hoping to make a dent in endpoint security.

451 Research®

One consequence of the increased familiarity that security teams have with coding is the rise in open source projects aimed at security use cases. The 'osquery' project, born at Facebook, is an example: faced with having to manage a large fleet of devices, Facebook engineers created a component to simplify that task using structured language as an interface. Still, the osquery agent is but a component in a broader endpoint architecture, and organizations looking to use osquery must deploy infrastructure around it for management, data collection and alerting based on osquery data.

This is precisely what startup Uptycs aims to address by offering a SaaS-based approach to using osquery as a window into endpoint security. The combination of open source agents with cloud-based analytics opens up a number of possible use cases.

THE 451 TAKE

The increased popularity of osquery as an open source agent may indicate what the future of endpoint security could look like: organizations collaborating on technology, with increased adoption of DevOps practices beyond the confines of typical application pipelines. For many, it will not be an easy journey because there's much more to it than just getting an agent installed. Uptycs comes out of stealth looking to address this, hoping that it can unlock the value of osquery in a way that satisfies smaller and larger organizations alike. The challenge for the company will be to maintain differentiation in the face of several competitors, including existing endpoint vendors, newer osquery-focused challengers, cloud workload security offerings and DIY efforts within prospects. Still, if Uptycs can efficiently deliver on the use cases, it may carve out space for itself with those adopting this approach to endpoint security.

CONTEXT

Uptycs is based in Waltham, Massachusetts, and just came out of stealth. The company currently employs roughly 25 people. Uptycs' executive team is led by CEO Ganesh Pai, who comes from Akamai, where he was chief product architect. CTO Milan Shah comes from Core Security, and Uma Reddy is VP of engineering.

The company recently announced series A funding of $10m, bringing its total funding to date to $13m. In addition to original seed investors Comcast Ventures, Genacast Ventures and Founder Collective, the company now also added ForgePoint Capital (formerly Trident Capital Cybersecurity).

Uptycs indicated that some early adopters have converted to paying customers of its SaaS offering. 451 Research estimates current annual recurring revenue to be in the $200,000-500,000 range.

STRATEGY

Because Uptycs bases its offering on top of the popular osquery open source project, the company is pursuing specific sets of customers and distinct use cases.

Initial prospects and customers seem to fit two profiles. One type of organization is the smaller to midsized organization – typically between 200 and 2000 users – that has evolved to rely heavily on cloud services and has very little infrastructure of its own. These prospects usually have made the strategic decision to consider Uptycs a key component of their security-monitoring efforts. Alternatively, larger enterprises – usually in technology – that have been early adopters of osquery are facing more complex deployment questions and are interested in converting their initial efforts to use the technology into a more turnkey approach.

TECHNOLOGY

The osquery project originated at Facebook and has been open source since late 2014. The driving use case was to simplify endpoint security for non-Windows endpoints such as Mac and Linux. Osquery does this by creating a lightweight agent that collects information from each endpoint and exposes that information via a standard structured query language (SQL) interface. The underlying details of each operating system – process information, memory usage, network connection information and many other types of rich, security-relevant details – are exposed via tables that can be queried as if accessing a database.

This is a very powerful concept because it allows for the normalization of queries across the environment and the use of sophisticated queries relying on relational algebra. The open source nature of osquery allows for collaboration by the community for expanding the capabilities of the agent as well as other features required for enterprise use. While initially available for Mac/Linux, osquery was extended to support Windows endpoints in 2016 and continues to be updated by the community.

Osquery has gathered momentum recently, and the first conference dedicated to osquery – Querycon – was just held this year in San Francisco. Participants included vendors such as Uptycs and Kolide as well as organizations ranging from Facebook to Palantir and Stripe Inc.

PRODUCTS

Uptycs picks up on building the fundamentals needed for organizations to use the data from osquery agents. This includes creating back-end infrastructure for performing data retrieval and archival as well as creating the relevant queries and associated reports to implement different security use cases.

Uptycs indicates that its offering can help organizations implement functionality such as file integrity monitoring, endpoint detection and response, investigations, vulnerability management, and infrastructure audit and compliance. These use cases can then be applied to two distinct environments: endpoint devices (primarily Mac and variations of Linux, though Windows is also supported), and server- or cloud-based workloads (virtual machines or containers).

The Uptycs architecture consists of a SaaS offering that implements a TLS-enabled endpoint for the fleet agents to communicate with and different back-end components. In addition to a Web front end for reporting, investigations, API access and operational management, Uptycs implements data archiving and query scheduling, and an analytics engine that integrates external threat feeds and the responses from queries. The system is designed to be scalable to tens of thousands of endpoints or more.

The deployment effort consists primarily of using the Uptycs system to prepare a package with the standard osquery agent and Uptycs-specific credentials, then deploying that package to the fleet. This is typically done via tooling such as Puppet, Chef or Ansible. After deployment, each fleet agent contacts the Uptycs TLS-enabled listener, and is ready to send in data or respond to queries.

Once deployed, the system presents a front end where users can perform ad hoc queries and, importantly, review the results from scheduled queries. These scheduled queries can be customized by users or leverage one of the many 'query packs' that Uptycs has created. These query packs – and their associated scheduling – represent a key component of the system because they provide the foundation for the multitude of use cases supported by Uptycs. Query packs implement queries supporting a variety of audit/compliance targets, and their scheduling has been optimized to balance depth of data collection with resource use.

Uptycs has also implemented functionality to ingest threat feeds and create incident response integration. This integration is done via a mechanism named 'dashbooks,' which implements functionality for mixing textual instructions with queries and other programming logic.

In addition to its main system, Uptycs recently launched a 'Mac EDR' console to simplify security operations for Mac endpoints. It leverages the existing data from Uptycs but presents a simpler interface optimized for operations.

COMPETITION

As Uptycs touches on different use cases – including endpoint security, cloud infrastructure/workload protection and containers – it is up against numerous competitors. In addition to existing vendors, newer osquery-focused vendors also exist. Existing endpoint security vendors have already taken notice of osquery. From Tanium hiring executives with experience at Facebook, where osquery was created, to Carbon Black presenting at Querycon, endpoint security vendors recognize that osquery can play a role in endpoint security. Vendors are likely to compete with Uptycs by offering their existing endpoint detection and response suites. The long list includes but is not limited to Symantec, McAfee, Trend Micro, Sophos, Kaspersky Lab, CrowdStrike, Cylance, Cybereason, Endgame, Sentinel One and IBM Big Fix.

Use cases for cloud workload protection, including vulnerability management and file integrity monitoring, place it in competition with established vendors such as Rapid7, Tenable, Tripwire, Qualys and Cloud Passage as well as cloud-centric ones – Threat Stack, Alert Logic, Red Lock and Dome9.

Uptycs container support also brings it up against other container security vendors such as Twistlock, Aqua Security, StackRox, Layered Insight, NeuVector, and others. Lastly, when it comes osquery-specific competition, there's competition both from internal, do-it-yourself projects at enterprises that build in-house tooling around the osquery agent, as well as external vendors. In this latter group, Kolide is one of the more prominent competitors, including having hosted the recent Querycon conference. Other osquery-focused vendors include DarkBytes, Zercurity and Polylogyx.

SWOT ANALYSIS

STRENGTHS

Uptycs has packaged functionality that supports relevant use cases for using osquery within organizations. Furthermore, product architecture and features such as 'dashbooks' seem to support more advanced use cases.

WEAKNESSES

Osquery is more popular on non-Windows platforms, and broad adoption in most enterprises will require ensuring Windows support is enterprise-ready, both in terms of security functionality and management capabilities.

OPPORTUNITIES

Two trends point to potential increase in popularity for osquery and offerings such as Uptycs' – security teams are becoming more adept at using open source components and organizations have become more comfortable with heterogeneous endpoint fleets.

THREATS

The open source nature of the underlying osquery agent means that there is a relatively low barrier to entry for commercial or community alternatives.