REPORT REPRINT

Qualys looks deeper into the endpoint with SaaS-based EDR functionality

FERNANDO MONTENEGRO

29 JAN 2018

The company has taken its SaaS-based architecture deeper into the realm of endpoint detection and response with the release of an indicator of compromise application.

THIS REPORT, LICENSED TO QUALYS, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

©2018 451 Research, LLC |

As Shakespeare once wrote "A rose by any other name would smell as sweet." Within endpoint security, we see vendors from very distinct upbringings contesting the endpoint detection and response (EDR) space. Some approach EDR as an expansion from an endpoint protection role, as an evolution of next-gen antivirus or anti-malware.

Other vendors approach EDR from a data-focused pedigree such as data loss prevention (DLP) or e-discovery. Some digital forensics and incident response (DFIR) platforms find themselves expanding into EDR, as do managed security services providers (MSSPs). Last but not least, there's a number of vendors that come to EDR as expanding their existing roles into other security management roles. It is in this last group that we find Qualys, as it looks to leverage its comfortable position in IT security and compliance management as a way to capture some of the space from EDR vendors.

THE 451 TAKE

Organizations looking to improve their endpoint security efforts have a number of options when considering providers for detection and response offerings. A recent trend among vendors has been a stronger focus on providing functionality from a cloud-based back-end infrastructure. This is a model that Qualys – long known for its cloud-based compliance and vulnerability management offerings – has embraced for many years. The addition of an indicator of compromise app to the Qualys Cloud Platform allows it to provide more detection and response functionality with the same footprint used for other functions. This is an interesting development for organizations looking to consolidate not only endpoint resources, but also the number of strategic vendors they possess. The challenge for Qualys, however, will be twofold: it must deliver the functionality required for more sophisticated EDR activities, and it must enable security teams to build the necessary detection and response practices using the concepts and integrations from its platform.

CONTEXT

Foster City, California-based Qualys was founded in 1999. It has been public since 2012, and under the leadership of early investor Philippe Courtot since 2001. The company is an established vendor in vulnerability management and IT compliance, and is a pioneer of security SaaS. It now has more than 9,300 enterprise and business customers spread across 120 countries, being serviced by a staff of approximately 850.

The workforce is split, with approximately half being outside the US, with a heavy presence in Pune, India. In addition to CEO Courtot, senior leadership includes longtime executives Sumedh Thakar and Amer Deeba. In 2017, the company made its first two acquisitions – both technological tuck-ins – since going public. It picked up assets of Nevis Networks, looking to build up its network access control capabilities, as well as assets from Netwatcher, which it expects to improve its threat intelligence capabilities.

PRODUCTS

Qualys' key distinguishing feature and one of its most strategic assets is the use of a cloud-enabled delivery architecture, centered on what is known as the Qualys Cloud Platform. At a high level, the Qualys Cloud Platform is the integration of several functional layers, spanning a multitude of environments, at massive scale, providing multi-tenant-enabled functionality servicing a number of security-related needs.

Each layer can be improved independently – supporting new environments, new underlying technologies, or adding new functionality. The platform supports on-premises, hybrid and cloud-based environments, from which data is collected via remote scans (authenticated or non-authenticated), via telemetry gathered from lightweight agents or, as recently announced, via API-based queries if the target environment supports it. Data is then stored

using a variety of use-case-appropriate technologies such as graph databases, NoSQL and relational databases, messaging queues, and more. Finally, a number of customer-facing applications rely on these data stores to provide security functionality.

This approach has provided Qualys with the flexibility and scale (the company claims numbers in the billions of scans and trillions of data points) to quickly evolve the platform, because the pace of technology change remains strong. The security applications offered by the platform run the gamut from maintaining current asset inventories – a perennial thorn for every organization – to performing vulnerability management, compliance management, configuration management and file integrity monitoring, to name a few. Application interfaces are accessed via common web front ends, and SOAP and RESTful APIs are available for some use cases.

It is by adding a new indicator of compromise (IOC) app on the Qualys Cloud Platform that the company finds itself wading into EDR waters. The new IOC app is targeted at investigators and responders looking for evidence of malicious activity or vulnerability posture from endpoints. The main use cases focus on threat hunting, suspicious activity monitoring and detecting malware families. The application leverages the existing Cloud Agent, which has been enhanced to collect EDR-friendly telemetry.

It can now collect additional information on files, processes, mutexes (mutual exclusion objects), registry changes and network information. The data is sent to the Qualys Cloud Platform, allowing organizations to review information from endpoints even if the endpoint in question is presently off-line. As with other Qualys applications, data is presented to the user in a web-based dashboard, and uses a number of pre-defined and customizable widgets. These widgets provide information at a glance, and are the launching point for drilling down into incidents or obtaining more detailed information.

The pre-defined widgets cover public advisories and suspicious behavior patterns identified by Qualys' Malware Labs team. Widgets can be customized by analysts using the existing Qualys Query Language, which can also be used to perform ad hoc searches. As it ramps up its threat-centric offerings, Qualys has grown its Malware Labs team, which conducts research into malware families and writes content to support the platform.

Qualys expects to build a stronger communications channel with its IOC customers since it plans to support customer-submitted samples in the future. As Qualys makes further improvements on this new application, it plans to offer better API support, as well as better integration with SIEM and orchestration platforms such as Splunk, QRadar and ServiceNow. While the IOC application currently uses OpenIOC for codifying behaviors and threat intelligence, the company hopes to improve its support for additional standards such as CybOX and STIX/TAXII. The company also indicated it plans to address case management capabilities, currently only available in Qualys' file integrity monitoring application.

STRATEGY

By virtue of its architecture, Qualys already offers many interesting features that one looks for in an EDR offering – a low-footprint agent, hassle-free back-end infrastructure, good support for device mobility and data enrichment from other sources, among others. Adding functionality to its existing agent to capture the additional data used in EDR and threat hunting scenarios is a logical expansion of its capabilities.

In doing so, Qualys is exploring the economies of scale and efficiencies that an existing (or potential) customer may get by choosing to add an incremental feature to a platform versus deploying an entirely new product. As it complements its portfolio with recent acquisitions in the network security and threat intelligence spaces, Qualys expects the strength of its efficiently delivered security portfolio to raise its profile as a viable strategic partner for enterprise customers, helping them consolidate their IT security and compliance stack in one platform and a single-pane-view UI.

COMPETITION

Qualys has a long history in the disciplines of vulnerability management, compliance assessment, and other supporting IT security and compliance. Along the way, it often finds itself competing with BeyondTrust, Tenable, Tripwire and Rapid7, all of which have a similar approach of 'agent on endpoint providing telemetry.' Qualys' positioning of its EDR capabilities seems to step beyond this traditional pool of competitors into the deeper waters of EDR.

The EDR field is heavily contested by a number of vendors. Crowdstrike, FireEye, Carbon Black and Cylance are well recognized names in this space, as are Cybereason, SentinelOne and Endgame, to name a few. Notably, Carbon Black recently increased its focus on cloud-based delivery, but when compared to Qualys, Crowdstrike stands out as a cloud-focused endpoint security competitor offering protection, detection and response.

Crowdstrike also seems to be further along in pursuing a broader platform play that provides 'apps' – it recently incorporated vulnerability management into its feature set. The larger established – but by no means complacent – vendors such as Symantec, Trend Micro, Sophos, Kaspersky and the recently reborn McAfee all have EDR capabilities that target the same problem space, albeit approaching from a different security-based pedigree than a vulnerability management one.

Microsoft has been adding cloud-based security functionality, and should be considered a possible competitor. Furthermore, Tanium and IBM (with BigFix), alongside Ziften, 1E Security and a host of others, are representative of broader IT vendors with offerings in EDR. Qualys' message of fast responses to queries about asset inventories and current state of the enterprise is something usually mentioned by these vendors as well.

SWOT ANALYSIS

STRENGTHS

Qualys has had significant experience with cloud-based delivery of security functionality. The IOC app is a low-friction addition to those on the Qualys cloud, and the application can look to additional data from other applications as it enables analytics or alerting.

WEAKNESSES

Against more established competitors, Qualys' EDR functionality is still evolving, and needs to quickly cover ground in areas such as integrations and better support for case management.

OPPORTUNITIES

As customers seek to rationalize their vendor management practices, having a strong foothold in an adjacent practice is very positive. Also, there's strong momentum behind simplifying delivery using cloud-based services.

THREATS

Benefits notwithstanding, customers may have stronger strategic relationships with other vendors, making the adoption of Qualys' offering less likely. The constant evolution in the threat landscape may impose significant demands in quickly improving EDR capabilities.