IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Qualys Moves into the Burgeoning EDR Space

August 25, 2020

By: Mark Child, Konstantin Rychkov

IDC's Quick Take

Vulnerability management giant Qualys is expanding its focus and moving into the endpoint detection and response (EDR) space. The move mirrors a trend seen among existing EDR players that are seeking to capitalize on the capabilities of their solutions to provide vulnerability detection functionality.

Product Announcement Highlights

Historically, Qualys's solutions used an agentless approach, instead relying on appliances deployed on premises. In 2018, the vendor launched an expansion to its Cloud Agent (initially released in 2015) and spent the ensuing months tuning it — after which, adoption grew rapidly. That marked an initial step toward EDR, comprising an indicators-of-compromise (IoC) app on the Qualys Cloud Platform, available via SaaS deployment only. With the transfer of agents to on-premises architecture in the following year and the expansion of its functionality with API integrations, Qualys took a major step toward a comprehensive EDR offering. To date, around 40 million Qualys agents are deployed worldwide for inventory, vulnerability management, and configuration management. The vendor now aims to leverage those Qualys agents, backed by newly added malware detection capabilities, to deliver EDR. Qualys stresses that the value of deploying EDR for endpoints is limited if the user doesn't already have patch management and vulnerability management for those machines. This is primarily due to an inability to manage the response without those capabilities.

This EDR solution is Qualys's own in-house development, and the vendor is also very close to securing an OEM agreement for a third-party endpoint protection platform (EPP). The vendor would gain little by inventing its own EPP engine with so many mature platforms already on the market. Mirroring a broader market trend, over time, the vendor plans to expand toward an XDR approach, bringing in more data points and telemetry to enrich its analyses. The first frontier in this transition is deeper visibility into network reachability, which is currently used for forensics. Looking ahead, in 2021, the vendor plans to add more SIEM-like capabilities — for correlation, visibility, and alerting.

A key benefit of adopting Qualys EDR will be the enablement of existing customers to consolidate their security stacks and rationalize the numbers of agents they deploy. The majority of Qualys customers already have vulnerability management. Adding inventory and configuration management to that enabled them to replace one of their suppliers. Qualys EDR represents the next move in that consolidation process, allowing customers to replace McAfee, Symantec, CrowdStrike, or Sentinel One, for example. Qualys argues that none of its EDR competitors has a mature vulnerability management capability; none of them can yet do patch management; and all are far from offering inventory and configuration management. An alternative architecture, for those attached to their current EPP providers, is based on open API integration with the existing endpoint solution.

Qualys EDR provides most of the standard functionalities that clients expect from an EDR solution; however, the vendor feels that it can differentiate itself through some key capabilities:

- **Complete asset inventory** — looking at all software running on all machines, vulnerabilities, configurations, patch history, and so forth
- **Contextual analysis** — taking into account, for example, the nature of each device, whether it is a database server, the CEO's PC, etc.
- **Addressing the estate** — when a pattern or vulnerability is found, determining what similar machines could face the same issue and launching a job to address all those machines

What this really means is that metadata from the environment is sent to the Qualys Cloud Platform, where IoCs can be contextualized and prioritized by correlating them with external threat intelligence feeds from various sources (so customers don't need to rely on a single malware database or pay for external feeds). This context will drive the prioritization of response by highlighting the exploitability of the systems being monitored, along with threat persistence and potential impact. Moreover, discovered misconfigurations are mapped across the entire environment, enabling the application of centralized actions to the patch.

One challenge for many EDR vendors is pushing data out to other SIEMs; so Qualys provides an API for that. Qualys EDR provides out-of-the-box support for most major SIEMs, such as Splunk, Micro Focus, and QRadar. The data formats to date have primarily been XML and CSV, but the vendor is moving to full JSON availability due to demand from security teams to simplify their work on push and pull requests. Qualys provides 30 days of data retention for active data (for dashboards), while passive data (metadata on incidents) can be kept for an unlimited time. Forensics data attached to malicious files or activity is retained for a year.

From the customer side, operating an EDR tool is always a point of discussion; consequently, Qualys is building in automation capabilities as the solution develops. In the initial stage, some rules-based response capabilities are already in place — primarily, for passive response. However, with Qualys's context-rich approach, those can be built up over time to deliver progressively greater automation and reduce the operational burden for the client.

Qualys also seeks to address what it sees as four of the biggest EDR challenges:

- **How to find out which assets have/should have EDR deployed and which don't:** Qualys addresses this by adding inventory as one of the first steps — in other words, to look at the machines and then deploy on the priority ones, such as developer servers.
- **Machines not on the VPN:** EDR approaches fall into two camps, on-premises and cloud-based. But customers struggled with machines that were not on the VPN. Qualys's Cloud Agent solves this architectural issue via physical presence on the device (with less than 3MB required) and communication with the Qualys platform for analysis, which it does directly, through the internet, so that the new updates and quick response actions are not missed — even when the host is not on a VPN.
- **Threat intelligence (TI):** Qualys provides in-house researched detections and enrichments from its other apps, as well as native integration of threat intelligence feeds from leading third-party sources so customers do not have to rely on a single feed. Qualys allows ingestion of up to five TI sources without charge.
- **Which approach to take to EDR:** Many EDR tools use what can be described as an "EDR chase" approach: When they detect a compromised endpoint, they take control of that and then follow the chain from there. An alternative approach is to look at the main threats and malicious

activities — as well as other telemetry, such as vulnerabilities, missing patches, misconfigurations, and approved or unapproved software and versions thereof — for all endpoints and correlating them with external threat feeds. This is essentially taking Qualys's traditional approach and applying it to EDR. Remedy via such an approach is distributed centrally to machines that are vulnerable.

Capabilities for addressing all these challenges are already in place with the Qualys EDR solution. The beta version is already available, and EDR will go live on September 15. Following that, as noted above, Qualys is working on an OEM agreement for EPP, for which it is aiming for a November release. Qualys is already seeing interest from its partners, which would like to leverage Qualys's solutions, including EDR, as an MDR offering.

IDC's Point of View

Qualys's ambition to become an EDR vendor emerged in 2018 as an IoC app on an SaaS platform. Within two years, that vision was first shaped into a vulnerability management detection and response (VMDR) offering and then further expanded with Cloud Agent enhancements into a comprehensive EDR solution. The main feature — linking core EDR functionality with vulnerability and system visibility — is a compelling driver of interest for this new solution. IDC notes the trend of XDR vendors expanding their integrations with vulnerability management tools, but Qualys comes to this space with a native bond of functions under one agent that can be deployed on premises and in virtual, container, and cloud environments.

Vulnerability management with systems inventory can become a catalyst for collaboration between IT and security teams. Qualys EDR is a working product with a holistic approach to preventative security; development of the solution is ongoing, with further features to be launched in 2021. Qualys Cloud Platform dependency on IoC correlation will limit private cloud implementations, but it will create substantial thrust for MSSP participation and additional service provisioning. The biggest question marks are EPP capability and flexibility for third-party integrations, which PoCs will be able to clarify.

Qualys is entering the EDR space with an attractive offering — one particularly for companies that place a high priority on vulnerability management. This is therefore an opportunity for the vendor to expand its footprint within its installed base. Unfortunately, not all organizations have such a focus. Nevertheless, weaving in threat intelligence enables Qualys to combine in-house context and vulnerability management-driven prioritization with external context (i.e., the global threat landscape), representing an opportunity to achieve something greater than the majority of the market to date.

Subscriptions Covered:
European Security Strategies