Publication date:
26 Oct 2021
Author:
Tanner Johnson, Principal Analyst, Data Security, IoT Cybersecurity

On the Radar: Qualys Cybersecurity Asset Management (CSAM) helps discover and manage cybersecurity risks in IT assets

Brought to you by Informa Tech

Table of Contents :

Summary

Catalyst

Qualys has focused its information protection efforts toward one of the most fundamental yet frequently overlooked aspects of cybersecurity: comprehensive visibility into an organization's assets. Effective insights surrounding various assets form the foundational bedrock and baseline from which all security protections can stem. While many organizations often struggle to establish such a baseline, the Qualys Cybersecurity Asset Management (CSAM) solution is designed to help streamline this process by developing a dynamic and comprehensive inventory of all assets within an organization, in order to more easily and effectively recognize any potential security gaps that may exist and require attention.

Omdia view

The fundamental cornerstone of security for any organization has to be comprehensive visibility. It is impossible to fully protect assets that have not been discovered, assessed, and classified based on attributes and risk to the organization. For example, if simply asked to identify where an organization's data is located, many administrators would likely struggle to answer confidently. Between locally connected hardware components, various networked storage servers, integrated cloud or edge devices, on-premises/off-premises hybrid cloud deployments utilizing OneDrive/Google Drive/DropBox, etc., an organization's data can be housed in countless locations simultaneously, making effective visibility a herculean effort. This evolving ecosystem systematically makes locating critical data assets a significant challenge.

Despite the complexity of this initial task, no information protection strategy can succeed if data assets and their locations are not effectively discovered and monitored. Organizations must discover, identify, and classify their respective data assets that are essential for business continuity, as data visibility is as essential as visibility for any other organizational asset. Often referred to as an organization's "crown jewels," these are the mission-critical data assets and repositories that are crucial to a company's continued operation and would likely cause severe damage if compromised. As a result of the continued demand for comprehensive and detailed organizational asset visibility, combined with the increased frequency of large-scale breaches and ransomware attacks, there is a significant market need for solutions such as the one offered by Qualys.

Why put Qualys on your radar?

By introducing its CSAM solution earlier this year, Qualys is providing organizations with technology to gain detailed insight into their own unique threat landscapes. However, visibility without any corresponding actionable information is effectively worthless to security personnel.

The Qualys Cloud Platform allows organizations to understand more than just what hardware and software components exist within their environments. By developing an inventory of their respective assets, as well as analytics to provide a baseline of what "normal" activity looks like for those assets, the Qualys CSAM helps organizations identify what security risks are associated with these specific components that comprise their respective environments. This proactive approach to visibility provides organizations with actionable intelligence on potential security threats, and potential courses of action, rather than a flood of security alerts and notifications with little to no value.

Market context

While the lack of comprehensive organizational asset visibility has been a problem that has plagued enterprises for years, increased demand from buyers has only recently led to the emergence of comprehensive visibility solutions. Whether this recent market evolution has taken place in response to regular announcements of yet another large-scale breach, concerns surrounding regulatory compliance, or from internal motivators, demand for solutions that promote visibility are as strong as ever. However, as alluded to earlier, visibility on its own provides little substantive value if no additional intelligence can be tied to a respective notification or security alert.

The challenges many organizations face surrounding the establishment of an effective asset inventory can be quite numerous. The security environments of many modern organizations are often considerably complex, and often encapsulate a jumble of disparate services and solutions designed to address a unique security risk or threat. Ensuring proper interoperability of these various solutions is a considerable challenge in and of itself, which only increases the associated difficulties of discovering, identifying, and classifying valuable assets across complex hybrid environments. Additionally, even after these assets have been effectively identified, few solutions focus on providing effective monitoring to ensure data integrity, while maintaining compliance with evolving regulations.

Qualys has entered into an emerging and fast-growing market of vendors competing to provide greater security through the provision of comprehensive and granular insights and analysis into organizational IT environments. Similar vendors in this space include startups like Axonious and Armis, as well as established vendors like Ivanti, ManageEngine, and SolarWinds, with each making acquisitions in the visibility space to broaden their portfolio offerings. However, while each of the above-listed vendors have sought to gain a foothold in the asset visibility market, Qualys has sought to differentiate itself with the inclusion of contextual intelligence into its CSAM offering.

Product/service overview

As challenging as visibility is for the data security efforts of many organizations, even in "normal times," the impact of the COVID-19 pandemic has splintered the traditional concept of a perimeter even further. Almost overnight, the entire global workforce began working remotely; in turn, critical IT assets, including data, became just as distributed. The gap between more mature enterprise security environments and traditional consumer technologies that exist within the home introduced added opportunities for adversaries to gain unauthorized access to critical assets. As these risks have continued to develop, vendors like Qualys have stepped up to address such unique security challenges.

The lack of effective interoperability between disparate security solutions continues to plague the modern enterprise. While many vendors promote interoperability as a component of their respective service, serious challenges continue to remain. These challenges are especially severe when they pertain to the handling of security events involving critical assets. Qualys has sought to address this issue by introducing an all-in-one solution designed to utilize the various native sensors within the Qualys Cloud Platform, to allow clients to monitor their respective threat landscapes more easily.

The Qualys CSAM has four primary elements, with each component offering supplemental support:

- Inventory: establishes an extensive record of all assets within an IT environment including business-critical context, utilizing various options that allow for agents, as well as active scanners, and passive sensors.
- Health: monitors the discovered assets for any unauthorized changes, utilizing various external regulatory requirements and even internal compliance demands. It also monitors for end-of-life assets as well as differentiating commercial versus open-source assets.
- Detect: seeks out any potential at-risk assets or applications to identify their exposure to the internet, presence of risky software, or lack of security tooling such as antivirus/malware, and utilizes comprehensive contextual analysis to determine the best course of action to mitigate the risk.
- Respond: prioritizes alerts for security personnel to address the most critical threats by associating an Asset Criticality Score while recommending remediation actions.

However, while many vendors in this space are recognizing the need to enrich organizational asset visibility as an essential security component, Qualys has already taken the additional steps necessary to incorporate in-depth contextual information into the response efforts. Upon the establishment of a comprehensive inventory of both managed and unmanaged assets, the Qualys CSAM utilizes the in-depth contextual data collected through the Qualys Cloud Platform to seek out at-risk assets and applications. This includes ensuring that assets maintain compliance with ever evolving regulatory requirements. Through these various functions, CSAM promotes the continued monitoring and maintenance of the health of inventoried assets, while allowing security personnel to rapidly identify and respond to security risks in real time.

Company information

Background

Headquartered in Foster City, California, Qualys was founded in 1999 by Gilles Samoun and Philippe Langlois. Upon founding Qualys as a serial investor in Silicon Valley, Samoun went on to be the founder of several SaaS companies, such as NTRlobal, and Salesmachine, and remains the board member for various cloud-based companies, such as CipherCloud. After helping to found Qualys, Langlois went on to found nearly half a dozen other security-related companies, including INTRINsec, WorldNet, Wave Security, TSTF, and P1 Security.

Qualys achieved rapid success with its flagship QualysGuard vulnerability management solution, eventually going public in September 2012, under the leadership of long-time former CEO, Philippe Courtot. The company managed to raise more than $90 million at its Initial Public Offering. Qualys has managed to achieve 28 registered patents, primarily in the category of “Electronic Communication Technique.” While the company has primarily served the enterprise, Qualys has sought to target a wide range of verticals, including compliance and regulatory conscious entities in government, as well as the privacy-heavy requirements present in the healthcare industry.

Current position

With the evolution of QualysGuard, Qualys established itself as the first vendor to offer vulnerability management capabilities through a SaaS delivery model. The company went on to develop more products, with its Intranet Scanner developed in 2002 to seek out vulnerabilities in corporate LANs, as well as its Policy

Compliance offering being launched in 2008. In 2010 the company launched its BrowserCheck service as a means of scanning both browsers and their various plug-ins for potential security vulnerabilities. In 2012, the company extended its Qualys Cloud Platform with a cloud-native design to improve efficiencies across hybrid environments.

Today, Qualys claims over 19,000 customers, stemming from over 130 countries. Qualys clientele includes the majority of each of the Forbes Global 100 and Fortune 10. In an effort to continue to develop its cloud-focused offerings, Qualys has established partnerships with fellow cloud vendors like Amazon, Google, and Microsoft. Qualys has taken its cloud security offerings a step further by becoming a founding member of the Cloud Security Alliance (CSA).

Future plans

While Qualys has established itself as a leading provider of cloud-deployed vulnerability and asset management solutions, the company is always seeking ways to bolster its current capabilities. Qualys has plans to incorporate additional integrations into its service, such as Shodan.io. Such a partnership will allow Qualys clients to label their respective assets more easily, while providing an integration hub that will include additional third-party resources, IT operations solutions, and various security tools.

Qualys is also seeking to make its offering more robust by syncing with configuration management databases (CMDBs). Through such an integration, the CSAM solution will incorporate asset criticality and vulnerability risk scoring, while also looking to integrate into the Qualys Web App Security workflow. Additionally, Qualys is seeking to evolve its monitoring capabilities to include policies related to required software, such as anti-malware and other operational tools. Lastly, Qualys is also looking to make its response abilities more robust by including the ability to quarantine an entire network as a component of a Zero-Trust response action triggered from a perceived threat.

Key facts

Table 1: Data sheet: Qualys

Product/Service name	Qualys CyberSecurity Asset Management (CSAM)	**Product classification**	Cyber Asset Attack Surface Management (CAASM), IT Asset Management, IT Asset Inventory
Version number	2.1.0	**Release date**	July 10, 2021
Industries covered	Banking & Financial, Manufacturing, Insurance, Technology IT Services and Retail	**Geographies covered**	Worldwide
Relevant company sizes	Enterprise, Midsize	**Licensing options**	Asset Discovery & Inventory – Free CyberSecurity Asset

			Management (CSAM) – Per Asset
URL	https://www.qualys.com/apps/cybersecurity-asset-management/	**Routes to market**	Direct, Indirect (MSSPs, partners)
Company headquarters	Foster City, California, US	**Number of employees**	1,600+

Source: Omdia

Analyst comment

Visibility is the cornerstone of all security efforts, but vision without context is effectively meaningless information. The additional and supplemental contextual requirements surrounding visibility have plagued organizations for years, often resulting in the dreaded "notification fatigue" for security personnel looking to respond to alerts absent critical intelligence behind the alert itself. By providing the additional contextual information associated with these alerts, the Qualys CSAM solution is a considerable differentiator from previous visibility products, as it turns visibility information into contextual intelligence.

However, while Qualys is a mature organization that has enjoyed considerable success through its respective product offerings throughout the company's lifespan, it isn't alone in its efforts to bolster security through greater contextual intelligence and response capabilities. Several established companies and startups (many previously mentioned) are either promoting themselves as primarily visibility vendors, or have sought to acquire entities that have developed these more dedicated capabilities natively. However, this practice has resulted in many security vendors transforming into a veritable Frankenstein's monster, requiring full adoption of the entire platform in order to benefit from any single piece of the whole. Qualys needs to be careful to not follow suit.

Despite these concerns, Qualys has made considerable achievements in the domain of threat landscape visibility, and its significant efforts towards third-party integrations are to be commended. Although, with the explosion of connected devices projected to occur as a result of 5G deployments, along with the exponential growth of the IoT itself, the company definitely has its work cut out for it. While Qualys appears to understand the need to differentiate itself in a crowded market through continued innovation and increased capability, the transition over the next few years will be very telling of Qualys's capability to maintain its place in the visibility market.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Data Security Strategies Are at the Heart of Cybersecurity (October 2020)

"Data extortion: Ransomware with an evil new twist" (February 2020)

Fundamentals of Zero Trust Access (ZTA) (February 2020)

Author

Tanner Johnson, Principal Analyst, Data Security

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com