REPORT REPRINT

Qualys highlights its adaptability to digital transformation at QSC '17

SCOTT CRAWFORD

09 NOV 2017

At the 2017 Qualys Security Conference in Las Vegas, the security SaaS pioneer emphasized its ability to embrace containers, cloud platforms and DevOps trends reshaping the future of IT - and IT security.

Digital transformation has become a watchword in technology, bringing fundamental change to many aspects of IT – change to which security vendors must respond, with capabilities that embrace the native capabilities of 'New IT.' Qualys emphasized this theme at its 2017 Qualys Security Conference in Las Vegas, highlighting its strengths not only as a major player in vulnerability and compliance management, but with the advantages of a vendor born in the cloud.

THE 451 TAKE

Qualys is among the original vendors of IT security vulnerability and compliance assessment, but where others began with an approach that centered on on-premises software and appliances, Qualys differentiated from the outset by coming to market as SaaS. The move was daring for its time, raising eyebrows with the idea that an organization's most sensitive security vulnerabilities could be gathered, stored and managed by a third-party service. Qualys responded with investment to assure customer confidence, augmenting its hosted platform with data protection measures and on-premises offerings.

The strategy worked. Organizations recognized the value of a SaaS provider that could offload the technology as well as have the expertise required to manage and maintain its platform, and the company achieved a significant market presence. Today, Qualys seeks to capitalize on its heritage by addressing the demands of new IT that leverage cloud technologies, 'infrastructure as code' and the automation that characterizes DevOps. Headwinds could include not only established and new competitors, but also the technologies native to cloud and DevOps. Qualys could counter with an ability to consolidate this functionality in a toolset owned by security and compliance operations, building on the company's pioneering SaaS heritage and substantial market penetration. Keeping up with digital transformation, however, will be a challenge not only for Qualys, but for every vendor that must grapple with the aggressive pace of IT innovation.

CONTEXT

Founded in 1999, Qualys is an established vendor in vulnerability management and IT compliance and is a pioneer of security SaaS. Differentiated by this distinction at its founding, Qualys has seen many others arise to provide SaaS offerings for security, in its own markets and elsewhere. Its early investment in SaaS and wide adoption, however, have combined to help it tackle security challenges faced by the hybrid enterprise. Recent years have seen the company expand coverage from on-premises infrastructure and endpoints to both public and private cloud platforms, providing asset inventory, threat protection and insight, file integrity, security for web applications and solutions for DevOps initiatives in addition to vulnerability and compliance assessment for organizations of all sizes worldwide.

Qualys went public in 2012, raising a net of over $87m with its IPO, and today counts more than 9,300 customers in over 120 countries. CEO and chairman Philippe Courtot was an early investor and became CEO in 2001, following a run of startups with successful exits to strategic acquirers. Chief product officer Sumedh Thakar and chief commercial officer Amer Deeba are both longtime veterans with Qualys and its leadership, Thakar joining in 2003 to architect the company's PCI compliance assessment platform, while Deeba worked with Courtot prior to Qualys. The company is based in Redwood Shores, California, with slightly more than half of its 850-plus employees located outside the US, including a significant development presence in Pune, India.

TECHNOLOGY

At the heart of Qualys – both strategically and architecturally – is the Qualys Cloud Platform, the current manifestation of the company's anchor technology in the cloud that enables all its offerings, providing scale and elasticity for data collection, analysis, management and delivery for Qualys applications, and an always-on management platform that centralizes visibility and control across the portfolio. According to Qualys, the company performs more than three billion scans, logs over 100 billion detections, and collects, processes and analyzes more than one trillion security data points per year.

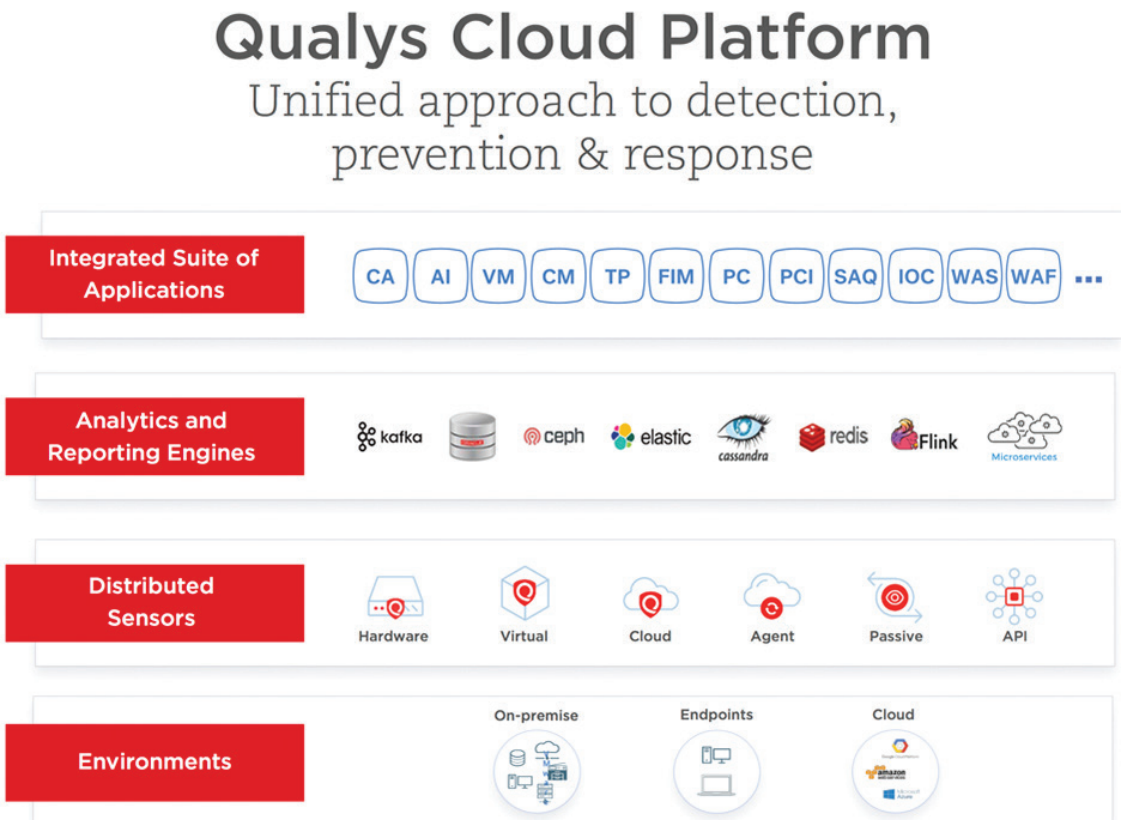
On the data-gathering side, vulnerability and assessment scanning has historically been accomplished through two classes of techniques: remote scanning, which assesses the attack surface visible to the attacker; and 'authenticated' scans, which access the system to perform assessment. Cloud platforms and more modern approaches to 'infrastructure as code' often support API-based information gathering as the primary means of collecting security, compliance and asset data – and Qualys is capitalizing on this opportunity in its 2017 releases, highlighted in more detail below. But many legacy systems (as well as their virtualized instances hosted on cloud platforms) may not support API-based assessment, and as 451 Research data continues to indicate, substantial enterprise investments in legacy, on-premises and hybrid environments aren't going away any time soon.

To overcome these challenges and assure high-quality data gathering from the broadest possible range of environments, security and compliance assessment vendors have introduced lightweight agents that offer consistent functionality across a variety of targets. The Qualys Cloud Agent is Qualys' 'universal' sensor form factor, a small package (the installer is less than 3MB) with support for many common Microsoft Windows, Linux and Apple Macintosh platforms.

Remote scanning, meanwhile, has long been a Qualys capability as it has been for most vulnerability assessment plays, but was recently bolstered with the network-scanning capabilities acquired with Nevis Networks' assets, announced this past August. Qualys also provides internet scanners for external scans, as well as physical and virtual appliances and software form factors for scanning internal environments.

The flexibility and performance of its combined cloud and sensor capabilities (Qualys claims a 2-second response from its Cloud Agents) has allowed Qualys to consolidate and simplify the user experience across a wide variety of applications. Positioned as 'Cloud Apps,' these applications provide coverage for the hybrid combination of legacy infrastructure, cloud assets and endpoints that characterize many organizations. Security applications include vulnerability management, configuration assessment, scanning and defense for web applications, and vulnerability prioritization for threat protection. Compliance applications range from policy assessment and file integrity monitoring (FIM) to support for specific mandates such as PCI. Because assessments discover and catalog targets, asset management is also a part of the portfolio, with applications that support asset inventory and the ability to synchronize findings with organizational configuration management databases (CMDBs).

Web application protections include web application scanning (WAS) capabilities that offer web app discovery and inventory (capability that the Qualys Cloud Platform is well positioned to provide, detecting an organization's approved as well as unapproved apps), progressive scanning, vulnerability prioritization, and support for SOAP and RESTful APIs. Qualys also offers Web Application Firewall (WAF) functionality that couples detection with protection, enabling customers to protect web application vulnerabilities with a single click.



Source: Qualys

Recently introduced Qualys offerings such as the company's new Indication of Compromise (IoC) Cloud App capitalize on trends in threat hunting and security incident investigation and response. The IoC app provides investigators and responders with evidence of malicious activity and vulnerability posture from endpoints, which can reflect both malware behavior and suspicious actions, and can be correlated with additional evidence to reveal threats that might otherwise be difficult to discover and contain.

More provocative still are new offerings that emphasize QSC '17's spotlight on digital transformation. As noted above, today's more modern computing and cloud platforms emphasize API-based interaction to gather asset, configuration, compliance and vulnerability data. This approach is essential to gain up-to-the-moment visibility into highly elastic platforms that can scale on demand. It also overcomes many disadvantages of legacy systems, which may take considerable time across highly varied terrain to gather information that can vary in completeness and accuracy. API-based interactions with more recent 'New IT' platforms can deliver this information not only much faster, but far more accurately.

At the Black Hat conference in July, Qualys unveiled its new CloudView app framework, an extension of the Qualys Cloud Platform that delivers this level of integration with, and visibility into, modern environments that embrace both cloud and DevOps techniques for streamlining and automating the development, deployment and operation of IT. CloudView will be available in beta for AWS beginning this quarter, with Cloud Security Assessment and Cloud Inventory to be the first two apps to take advantage of CloudView capabilities.

Another provocative new offering highlighted at QSC '17 is Container Security, which addresses the growing trend toward infrastructure deployed as containers. Container Security leverages an approach familiar to VM security management, with a container deployed on a hosting platform to discover and monitor the attributes of containers, assure adherence to security and compliance policies, and detect 'rogue' containers in the monitored environment. Container Security is also planned for Q4 beta availability.

STRATEGY

Qualys' farsighted cloud strategy has given it a leg up in serving the hybrid enterprise. The company has long provided coverage for what may today be considered 'legacy' IT – but its cloud roots inform its strategy for tackling the IT of tomorrow. Business priorities for faster, more responsive and more adaptable IT have driven the evolution of cloud and DevOps. Legacy approaches run the risk of becoming a drag on the automation and integration on which the speed and effectiveness of these new techniques depend. Capabilities native to these new approaches must therefore become a hallmark of an emerging generation of security technologies. Qualys' SaaS platform is not the only asset it brings to the opportunity; its own experience in developing for the cloud informs it as to what organizations need from their forward-looking security tools.

But the performance aspect of the speed required to keep up with the agility and instantaneous response afforded by new IT is a tactical problem. The strategic challenge is far greater. As fast as technologies are moving to redefine the nature of IT, even newer initiatives such as serverless computing already threaten to make obsolete trends such as containers that are themselves still maturing. This feverish pace sets a high bar for everyone hoping to stake their future on the future of IT. We will therefore be watching Qualys' moves with interest, considering that the security SaaS pioneer may be a bellwether for the adaptability of today's established vendors to what security will become.

COMPETITION

With the bulk of its business still centered on vulnerability and compliance assessment and management, Qualys faces long-standing competitors including BeyondTrust (which acquired eEye in 2012), Core Security, Rapid7, Tenable and Tripwire. Some of these have also emphasized the role of new IT in shaping digital transformation, a driver emphasized by Tenable's introduction of Tenable.io earlier this year following a $250m funding round in 2016, although of most this investment was made to acquire the shares of the founders who left the company. Others have targeted diversification as a go-forward strategy. Tripwire acquired nCircle in 2013 to complement FIM with vulnerability management, while more recently, Courion acquired Core Security and adopted the Core brand for the resulting combination of access and vulnerability management. Rapid7, meanwhile, has been an aggressive acquirer for years, taking on red team enablement with Metasploit in 2009, mobile security with Mobilisafe in 2012, application security and analytics with NT OBJECTives and Logentries in 2015, and most recently, security automation with Komand earlier this year.

This competitive activity highlights the central role of vulnerability management in security, and the challenges facing players in adapting to new IT. Awareness and mitigation of exposure is closely related to the ability to inventory and access a variety of IT assets, from datacenters and cloud providers to a growing profusion of endpoints. It also touches on system and application security and configuration management, and aligns closely with threat intelligence, security information and event management, and automation to prioritize remediation of attractive or actively exploited exposures. This introduces a wide variety of competitors, but also highlights Qualys' opportunity to become 'one throat to choke' for a variety of customer security challenges.

Among the more strategic players that can both enhance Qualys' appeal and challenge it competitively are cloud and new IT vendors themselves. Providers from Amazon to Docker and Kubernetes offer their own native approaches for defining and configuring new IT, while others such as Twistlock and Aqua Security focus specifically on container security per se. The advantage Qualys has in these scenarios is its ability to consolidate a broad spectrum of security functions typically owned by security operations teams, informed by its own born-in-the-cloud experience.

SWOT ANALYSIS

STRENGTHS

Qualys is a SaaS pioneer in security, but with a successful track record in security for legacy environments. This gives it a highly adaptable platform for securing the hybrid enterprise while informing a strategy for covering cloud and DevOps environments.

WEAKNESSES

A born-in-the-cloud pedigree is useful for new IT only as far as the offerings that result are truly compatible with native techniques, and don't attempt to fit legacy approaches into a new IT box.

OPPORTUNITIES

Digital transformation introduces several new opportunities for security vendors. Qualys' SaaS flexibility gives it the ability to come to market quickly and help its customers keep pace with innovation.

THREATS

Qualys's competitors include not only vendors in its legacy markets, but functionality native to cloud and DevOps environments that can address vulnerabilities and provide assessment directly. Qualys may, however, be able to harness these capabilities within its offering set and consolidate them with functionality owned by security teams.