REPORT REPRINT

Tenable hunts threats, sees IT's shadow and explores other bold new frontiers

ADRIAN SANABRIA, PATRICK DALY

07 JUN 2016

The company continues to move beyond the vulnerability management realm, enabling threat hunting and 'shadow IT' discovery use cases via a mix of its sensor options: agent scanning, passive listening, traditional scanning and log analysis.

451 Research®

Vulnerability management was once all about which vendor could detect the most vulnerabilities and how many plug-ins or checks a provider could perform. However, as the amount of data generated by network sensors became too much for security professionals to handle, it became clear that a revised strategy was needed – one that would reduce the information overload placed on security teams and give them actionable intelligence.

Tenable Network Security led the initial charge in vulnerability management with Nessus, a vulnerability scanner boasting over 60,000 plug-ins. Then, the company moved to address information overload with its SecurityCenter Continuous View platform. It is now reinforcing that position with new features such as agent-based threat hunting and 'shadow IT' discovery.

THE 451 TAKE

Tenable's deep investment in the engineer's perspective has earned the respect and loyalty of many practitioners. Its willingness to experiment and find its own path regardless of what the rest of the market is doing has enabled the company to remain relevant and agile while competitors have stagnated, especially as they consolidated their vulnerability management offerings into larger portfolios. This allowed Tenable to grow largely via word of mouth on the quality of its products and reputation.

However, the company's current growth rate and its goal to expand into adjacent verticals have created welcome conditions for outside funding. The trick for Tenable will be maintaining the balance between the boldness necessary to remain relevant in the fast-moving security world and the stability necessary to continue expanding at a fast pace. If the engineers want to make jetpacks, let them make jetpacks every now and then. Just don't bet the business on it until they've been well tested.

CONTEXT

Tenable Network Security has long been established as one of the 'big three' vulnerability management vendors with its Nessus vulnerability management offering, alongside Rapid7 and Qualys. However, the vulnerability management sector has become saturated with players, each claiming to detect more vulnerabilities than the others. While this has added to overall detection capabilities, it has also resulted in a net loss of quality for all involved, resulting in more work than most enterprise security teams could handle. Thus, Tenable needed strategies to validate and prioritize the results produced by Nessus.

For this reason, Tenable evolved from its origins with Nessus into a data and intelligence provider with SecurityCenter (SC), and then eventually launched its current flagship product, SecurityCenter Continuous View (CV). SecurityCenter CV can perform a number of functions and enables use cases such as continuous monitoring, validation against common security frameworks, threat hunting, and shadow IT discovery. Whereas Nessus is a single product, SecurityCenter CV is a platform that integrates the output of all other Tenable offerings to improve visibility into a business' assets and offer actionable intelligence on potential threats.

Founded in 2002 and based in Columbia, Maryland, Tenable has over 650 employees and 20,000 customers worldwide. In November 2015, the company notably landed $250m in a single funding round, almost three times what competitor Qualys raised in its IPO several years ago and more than the recent Rapid7 and SecureWorks IPOs combined. Given its announcements at this year's RSA conference, it would seem that some of this colossal financing has been earmarked toward diversifying SecurityCenter's capabilities and market reach to a point where it clearly no longer makes sense to refer to Tenable as a vulnerability management vendor.

PRODUCTS

Since the release of SecurityCenter, the product has been the focal point of Tenable's strategy. What started with simple asset monitoring and log correlation has evolved into a broad network and endpoint monitoring platform that aggregates data from different sources to provide holistic visibility into a customer's security posture. The platform, known as SecurityCenter Continuous View, combines features from all of Tenable's products, including Nessus, Passive Vulnerability Scanner (PVS) and Log Correlation Engine (LCE). We gave a very thorough overview of SecurityCenter CV's original capabilities in our last report on the company. Since then, however, it has made several changes to the offering.

At RSA, Tenable unveiled several features for SecurityCenter CV. First, it can now hunt for threats to identify and respond to them after intrusion, but before a breach occurs. SecurityCenter CV ingests indicators of compromise from third-party threat intelligence feeds, allowing enterprises to discover threats without paying for additional licenses or having to deal with the notoriously challenging job of leveraging raw feeds. A new Tenable-proprietary endpoint agent, active scanning, passive scanning and log analysis create a baseline for normal activity to help with anomaly detection. In addition to threat hunting, SecurityCenter CV now includes shadow IT discovery capabilities.

PVS, one of Tenable's (unintentionally) best-kept secrets, detects all devices, services and applications in use by watching and analyzing network traffic. It can also often determine when monitored devices have associated vulnerabilities, which might or might not be caught by Nessus or the new endpoint agent. The combination of an active network scanner, credentialed scanning abilities, an endpoint agent, a passive network sensor, hosted (external) scanners and access to application and system logs leaves few – if any – blind spots for SecurityCenter CV. Anything with a bearing on risk, regardless of where assets are located or what type they are, is likely to find its way back to SecurityCenter CV when all of Tenable's varied sensors and data feeds are engaged. ActiveSync and MDM integrations add even more context by feeding SecurityCenter CV mobile asset details as well as additional related policy and software information.

The final addition to SecurityCenter CV is the presence of dashboards to measure NIST CSF compliance. The dashboards leverage existing monitoring capabilities to generate custom assurance report cards (ARCs) on a company's security posture and automate NIST assessments. ARCs measure an organization's current security level, identify gaps and compare against a target to plan future security development. NIST standards were developed to help enterprises make better decisions and optimize security controls, but manually validating CSF compliance is time-consuming. SecurityCenter CV automates the assessment of most technical controls to ensure that they are in place, freeing security analysts for more critical projects. While simply meeting compliance should not be the goal of any security offering, any feature that can reduce the amount of time that practitioners have to spend validating compliance will be positively received.

PARTNERSHIPS

In addition to the latest product developments, Tenable also announced a partnership program at RSA. The company created its Technology Integration Partner Program (TIP) to drive collaboration and deliver its wares to more customers by granting partners early access to its development pipeline. TIP launch partners include Amazon Web Services, CyberArk, FireEye and Gigamon. They will work with Tenable to deliver everything from joint integrations with third-party plug-ins to go-to-market and joint sales initiatives. TIP provides partners with access to Tenable resources through its web portal, solution briefs and Tenable-endorsed webinars and events.

COMPETITION

While Tenable is still considered one of the big three in vulnerability management, it has been some time since the company has been solely focused on a single market. That being said, the same goes for the other two. Qualys continues to introduce products and features that can be added on through existing customer subscriptions. The latest, a web application firewall, integrates naturally with the vendor's web vulnerability scanner, with the ability to block a vulnerability that can't be patched immediately. Rapid7 has also chosen to shift from vulnerability management as a primary focus to the technology as a product line, with a more holistic platform approach replacing the scanner as its flagship offering. In Rapid7's case, this is the Insight line of products with InsightIDR and InsightUBA consuming and correlating data from the provider's other products and offering customers a more holistic approach to identifying and responding to threats.

This trend transcends the vulnerability management incumbents, as well. A large chunk of the security industry seems to be on a path toward platforms and integration and away from isolated point products. Also noteworthy is that each of the big three announced their own endpoint agents within several months of one another.

While businesses continue to mix and match vulnerability scanners, rather than buy the full package, most of the players in this space have created some interesting pairings. BeyondTrust couples vulnerability management with privileged account management. Tripwire pairs it with endpoint security, configuration management, change management and log management. Trustwave combines its managed offering with... a little bit of everything. Alert Logic also recently added vulnerability management (with its Critical Watch acquisition) to log management, threat detection and WAF. Although they address different ends of the market, IBM (with QRadar) and AlienVault have both incorporated vulnerability management with an approach moving more and more toward threat analytics, which is an emerging area that's growing rapidly at the moment.

This idea of threat analytics that we see businesses gravitating toward from different verticals inspired us to build a reference model a few years back that we call Actionable Situational Awareness Platform (ASAP). The purpose of building this model is that most organizations already own parts of this platform, but have gaps. The model helps us identify where those gaps are. At a high level, ASAP has three or four components. At its core is the system of record (usually a SIEM or log management product). Prior to the system of record are data feeds – these could be external intelligence feeds or simply information from other products that is collected and normalized by the system of record. Analytics is responsible for the third component – whether it be threat analytics, user behavior analytics or all of the above. The analytical engine does most of the work in deciding where threats might be and how to address them. The final piece is security and compliance automation. Without significant amounts of automation, security teams of the future won't likely be able to handle a workload and attack surface that only seems to steadily increase.

SWOT ANALYSIS

STRENGTHS

Tenable's expanding automation capabilities allow security professionals to focus on handling compromises rather than managing compliance initiatives, something that many security teams will favor. The company has expanded its reach and visibility into cloud, endpoint, SCADA, BYOD and other areas as technology trends have given birth to new security gaps or needs.

WEAKNESSES

The general perception that Tenable is purely a vulnerability management vendor is proving to be a difficult one to shake. Data quality (resulting in data overload, alert fatigue and false positives) is a core issue that all providers in this market struggle with, and Tenable is no exception.

OPPORTUNITIES

The security analytics market is a popular destination for buyers at the moment, and Tenable has a legitimate claim here, initially taking advantage of the shift toward real-time analytics to reduce false positives, and expanding to other use cases with its approach.

THREATS

As the company leaves its comfort zone and offers products further away from vulnerability management, it will come into contact with new classes of rivals in verticals that it is not familiar with.