Qualys readies its next-gen vulnerability management offering

Publication Date: 29 Jan 2020 | Product code: INT005-000087

Rik Turner

Ovum view

Summary

Qualys is launching Vulnerability Management, Detection and Response (VMDR), an upgrade to its widely used vulnerability management service that is designed to incorporate an expanded set of requirements.

The idea is to deliver an end-to-end, seamless and integrated cybersecurity workflow. VMDR therefore addresses the full vulnerability lifecycle: asset discovery (finding what is on the network), vulnerability assessment (showing what exposures organizations have), prioritization (surfacing what threats are most serious and how to reduce risk most efficiently), and response (delivering patches and other remediation).

Keen observers will also note that VMDR extends the xDR spectrum of detection and response technologies Ovum has been describing for the last two years. First applied to threats rather than vulnerabilities, the spectrum of capabilities has grown from endpoints (with EDR) to network (NDR) and cloud, although the CDR acronym has not gained currency. Now Qualys is extending it to vulnerability management.

Qualys is the 800lb gorilla of vulnerability management

With 28 million of its software agents deployed globally, 12,200 enterprise customers, and 1,300 employees, not to mention annual revenue in excess of $300m, Qualys is very much the heavyweight in the vulnerability management world, where its most direct competitors are Tenable and Rapid7. Founded in 1999 and traded on Nasdaq since 2012, it has also been an innovator in its segment, offering the technology in software-as-a-service (SaaS) mode since it came into existence.

Qualys became a significant player in vulnerability management at a time when the state of the art entailed deploying a scanner (a physical or virtual appliance) to survey all the servers, desktops/laptops, and software installed on a given host, compare it against a list of known vulnerabilities, and prepare a report of what needed patching on the system. Scans could easily produce thousands of discovered vulnerabilities in an enterprise. A security team would then run through the report, attempt to decide which vulnerabilities needed patching first, identify which patches were needed and how/when to deploy them, and so on. Vulnerability scans were run periodically, with their frequency varying from monthly to weekly or even daily, depending on the organization. Qualys developed VMDR to unify and streamline this entire process from discover to patching.

Vulnerabilities have mushroomed in recent years

However, the vulnerability landscape has changed over the last decade or so, and with it the expectations of a vulnerability management system. The Common Vulnerabilities and Exposures (CVEs) List, which is maintained by Mitre and feeds the US government's National Vulnerability Database (NVD), shows a steady upward trend in the number of CVEs reported since it began in 1999, from 894 in that first year to 12,174 in 2019.

The trend for vulnerability discovery is clearly upward, with 1,362 growth just in CVEs reported annually over the last two decades. However, while the number of vulnerabilities has mushroomed, the number of them that are actually exploited is around 2%, making the security team's job is tantalizing. The analogy often drawn is of finding a needle in a haystack, but it might more accurately be compared to finding which needle, in an ever-expanding pile of needles, is going to be used to penetrate the infrastructure and do damage.

Most important is the way in which organizations respond to the deluge of vulnerabilities, zero-days, end-of-life systems and applications, and other security risks that emerge and evolve daily. Businesses need to analyze a wide range of data to make informed decisions about which threats require immediate response and how to mitigate risks.

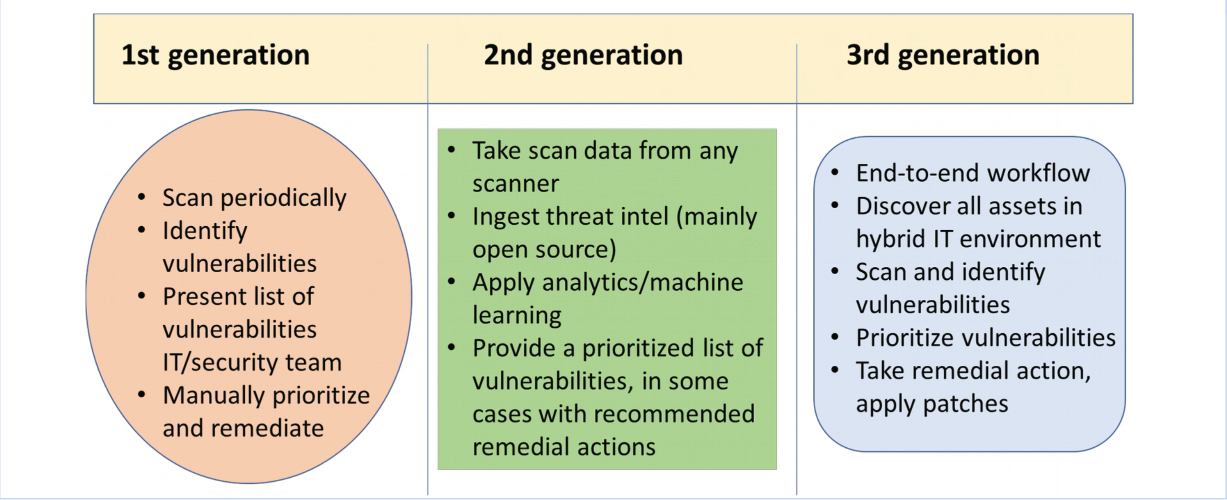
"Next-gen" management has emerged in response

Because of this evolution in the landscape, it is not surprising that new vendors have emerged over the last decade with a "next-gen" approach to vulnerability management, focused on prioritization of the vulnerabilities in a customer's scan data, regardless of which scanner they are using.

This next-gen approach also draws on threat intelligence to aid in prioritizing the most active and serious threats, in particular pulling data from open sources such as Exodus, ReversingLabs, or Proofpoint, as well as hacker forums, exploit-kit directories, and real-time exploitations as they occur across the global attack surface. Machine learning (ML) algorithms are applied to this data to gain a more complete understanding of when and where attacks are likely to take place, and priorities can be determined. They then proceed to highlight remediation requirements, generating workflow information that explains the actions needed and a playbook for how to carry it out.

The beauty of this business model is that it is independent of which scanner a customer happens to be using. The next-gen vulnerability management vendor provides an intelligence layer that sits atop any scanning infrastructure to facilitate the work of a security team by surfacing which vulnerabilities need to be prioritized and which can be left until later or even ignored altogether. This technology can therefore be sold into customers of one of the Big Three vulnerability management vendors and marketed as an enhancement that can use the scan data their technology provides.

Figure 1: Evolution in vulnerability management



1st generation	2nd generation	3rd generation
• Scan periodically • Identify vulnerabilities • Present list of vulnerabilities IT/security team • Manually prioritize and remediate	• Take scan data from any scanner • Ingest threat intel (mainly open source) • Apply analytics/machine learning • Provide a prioritized list of vulnerabilities, in some cases with recommended remedial actions	• End-to-end workflow • Discover all assets in hybrid IT environment • Scan and identify vulnerabilities • Prioritize vulnerabilities • Take remedial action, apply patches

Source: Ovum

The empire strikes back with prioritization and patching

Conversely, the weakness of this business model is that it introduces yet another point solution into the security stack and vulnerability management process, requiring its own set of integrations, “swivel-chair” workflows, and other inefficiencies. Established vulnerability management players now deliver a prioritization capability of their own and offer their customers the ability to derive still more value from their existing scanning infrastructure, without needing to deploy technology from another provider to do so. This is the vulnerability management equivalent of “The Empire Strikes Back”, and this is what we see now from Qualys.

Both Tenable and Rapid7 have also added prioritization capabilities to their vulnerability management products in recent years, but Qualys’ market clout makes its move even more significant. Where Qualys seeks to differentiate is in the ability for its platform not only to perform risk-based prioritization, but also to remediate and apply patches, even doing so in an automated way once the customer is comfortable with the approach.

Having built a large customer base using its capabilities via installed agents, Qualys has moved to expand the range of services on what it now refers to as the Qualys Cloud Platform, which enables customers to activate myriad additional services with virtually zero effort, including File Integrity Monitoring, Web Application Scanning and Firewalling, Indication of Compromise, Cloud and Container Security, and more to come. In February 2019, for instance, it launched Patch Management, another critical capability for managing a company’s security posture and one that contributes to the vendor’s ability to remediate and in future automate remediation.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

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

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo