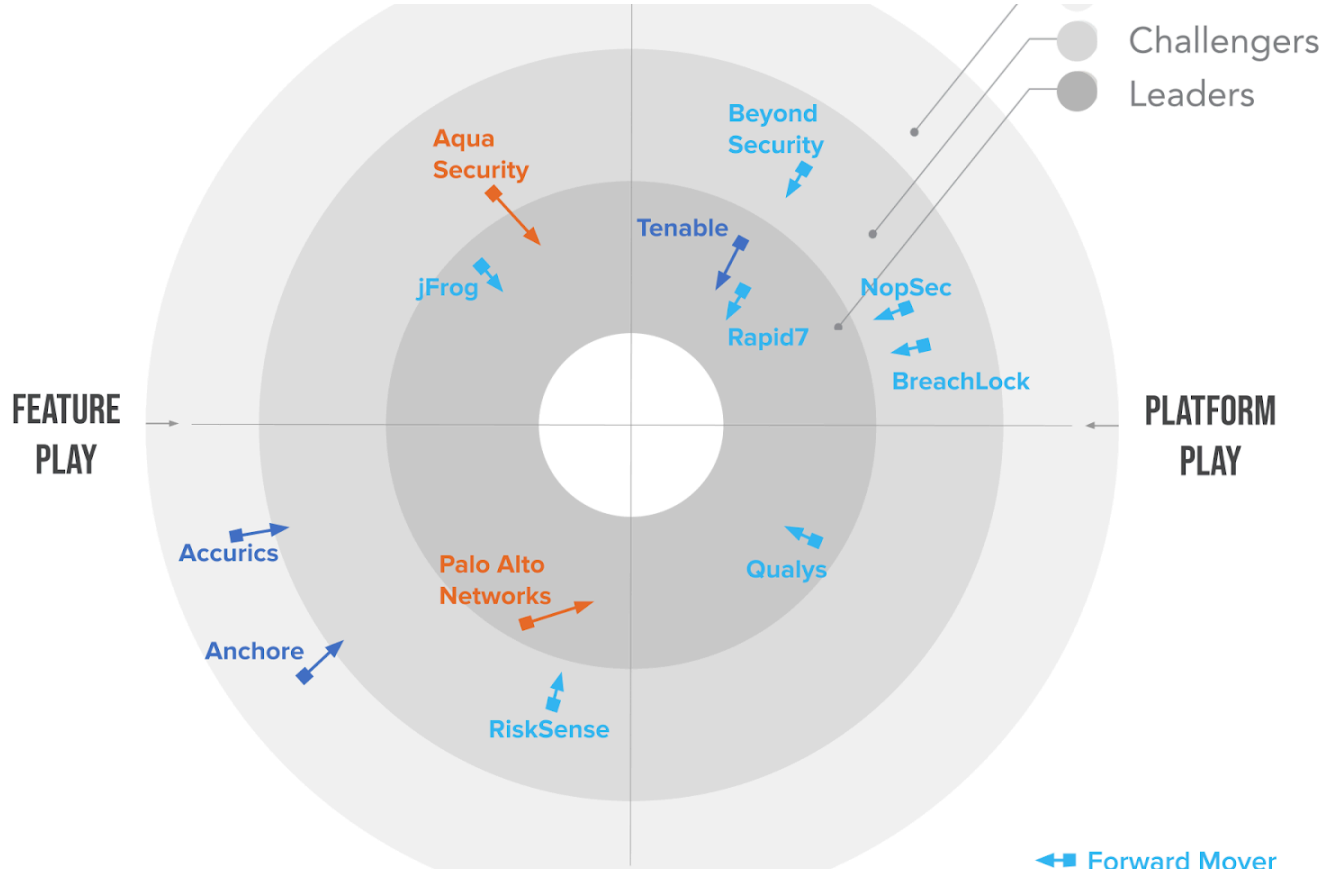
GIGAOM



Iben Rodriguez, Geoff Uyleman
May 17, 2021

GigaOm Radar for Vulnerability Management v1.0

Solutions for Cloud-Native Containerized Workloads

GigaOm Radar for Vulnerability Management

Solutions for Cloud-Native Containerized Workloads

Table of Contents

1. Summary

The challenges facing IT decision makers when it comes to modern vulnerability management include the integration of DevOps practices and increasing complexity of IT systems.

With DevOps practices and cloud deployments becoming more widespread, the risk posed by vulnerabilities and insecure configurations in legacy workloads and web applications in the cloud continues to increase. In addition, modern IT systems have grown larger and more complex, which makes grappling with large amounts of data increasingly difficult, even as security personnel struggle with the overload of events that can make it difficult to extract actionable intelligence related to business risk and threat context.

When making decisions about vulnerability management products, IT decision makers should consider solutions that can address security issues at scale and reduce the overall vulnerability lifespan, from initial discovery to the final stages of remediation, patching, or image rotation. A successful vulnerability management program prioritizes vulnerabilities based on local context and outside threats to provide actionable insights to developers in their preferred workflow tools for more efficient resolution.

Modern vulnerability management tools focus on security bugs discovered not only during runtime, but also in the build phase of the software design lifecycle (SDLC) when software artifacts are developed. Shifting security left is an automated vulnerability detection and response capability that gets integrated into the developer toolkit as plugins in the IDE or as part of the CI/CD pipeline process. Issues are resolved as soon as possible to avoid the cost and complexity impact of doing this later on in the lifecycle. The SDLC security program aims to optimize the process of building applications, including architectural reviews, static and dynamic code analysis, and the use of software composition analysis (SCA) to examine all artifacts for known vulnerabilities, and to rotate images continuously from development through test to production.

In modern IaaS and PaaS delivery models, vulnerability management tools support the inspection of code that is responsible for the deployment, integration, management, security configuration, and overall compliance of the cloud infrastructure, including microservices. Infrastructure-as-Code should be included in the scope of your vulnerability management program to ensure that pipeline components used to run application microservices are deployed securely.

We have found that the best solutions can ingest vulnerability and local asset information, as well as threat management data, from various sources so as to prioritize recommendations. For patch management, image rotation, or other remediative strategies to be effective, we must prioritize the issues that matter most to your organization. This requires local context, such as critical vulnerabilities found within high-value assets that may contain sensitive data, systems that are exposed to the internet, and determining whether vulnerable packages are actively used by applications. Prioritization also requires external threat intelligence sources that can enrich detections with information about recent vulnerability exploits, and any vulnerabilities known to be exploited for ransomware attacks or that can spread across your network (wormability). This information can help

filter out the vulnerabilities that matter most so you can focus on patching and adopting remediative controls to mitigate the possibility of attacks.

Each of the vulnerability management tools we evaluate in this report interacts with different phases of the SDLC. It is important to consider potential feature gaps in coverage when evaluating vulnerability management tools. Visibility into the respective phases of the application lifecycle can provide valuable insights, but it could also result in redundant findings when tools overlap. Duplicate data needs to be correlated and decisions on remediation should be prioritized based on risk, taking into account the threats being faced on a day-to-day basis.

These newer tools help us to be more effective with the limited resources of today's cybersecurity teams. This is a great opportunity to take a fresh look at how the security operations center (SOC) is staffed and how duties and responsibilities are defined. When bringing on new staff or negotiating a contract with a managed service provider, be sure the upcoming threat landscape is covered from a policy compliance and vulnerability management perspective for the entire SDLC, extending from the developers' workstations to the build environment to the kubernetes server.

This Radar Report evaluates the capabilities of notable players in the space against the points laid out in the Key Criteria Report.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Vendor Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

For a better understanding of the market and vendor positioning, we describe here the relevant verticals and segments for vulnerability management solutions. **Table 1** offers an overview of this information.

Verticals

We address six specific verticals, and many of these map to regulations that determine the kind of vulnerability management controls that need to be in place. Because the underlying vulnerability management tool operates the same way regardless of vertical, we do not assess vendors on their vertical-specific solution in this report. However, we do briefly describe the relevant verticals for vulnerability management solutions.

- **Technology**: Many large technology companies are publicly traded and outsource their vulnerability management programs to ensure compliance with regulations such as Sarbanes-Oxley (SOX) Act of 2002, General Data Protection Regulation (GDPR), Gramm-Leach-Bliley (GLBA), HIPAA, California Consumer Privacy Act (CCPA), etc.
- **Finance and FinTech:** Financial services agencies are subject to both private and public regulations depending on their function and country of operation. In many cases, government bailouts have placed a heavy burden of security controls that must be followed in order to continue operations. Membership in other industry groups can also require a significant investment in various audit reports.
- **Retail**: Many online businesses accept that they must balance the risk and cost of fraud against the additional friction and user inconvenience posed by strong security controls. Security programs need to adjust the balance of controls continually to maximize profit while protecting intellectual property and loss of reputation.
- **Media**: Digital rights management (DRM) controls handle much of the protection against theft. For online entertainment companies, a vulnerability management program mostly serves to protect against insider threat and human error as DevOps teams deploy more and more complicated technology using a hybrid cloud infrastructure.
- **Public Sector**: Government organizations are required to implement rigorous vulnerability management practices due to the highly sensitive data they process. In many cases, these regulations even describe the tools and methods that should be used.
- **Manufacturing and Utilities:** Industry 4.0 and Industrial IoT will make businesses in the manufacturing sector more dependent on IT, and in turn, more susceptible to cyberattacks. Vulnerability management will play a growing role in securing these verticals.

Market Segments

We've identified three market segments that need to adopt vulnerability management tools differently depending on their underlying infrastructure.

- **Large Enterprise:** The challenge for large enterprises is hybrid IT systems that include everything from on-premises devices to ephemeral cloud workloads. Suitable vulnerability management tools for these environments must be able to cover a lot of ground, performing scans to reach all corners of the IT estate. Established companies often have to deal with technical debt resulting from mergers and acquisitions, and as such, the IT landscape can be complicated. Often, companies need a dedicated, full-time team to coordinate vulnerability management efforts across the various infrastructure footprints and vendor technology.
- **Mid-Market:** While medium-sized companies do not have IT systems that are as complex as large enterprises, they also have limited cybersecurity resources. This means that a shift-left approach is a dealbreaker for mid-sized businesses. When incident response teams are spread thin, an airtight codebase is the most important layer of protection against known attacks. A managed SaaS based solution is a good fit for a mid-sized enterprise with limited full-time staff.
- **Cloud-Native/Startup:** The remediation of vulnerabilities found in containerized applications is performed via image rotation. Container vulnerabilities are detected through the decomposition of container images and scanning its components against known vulnerability databases. There are hundreds of thousands of entries in the commonly used vulnerability management tools used for containers. Microservice-based applications can benefit from the security control programs offered by their public cloud provider for a one-stop solution.

Deployment Models

In addition, we recognize the following four deployment models for solutions in this report.

- **Physical and Virtual Appliances:** Some vendors offer physical scanners, which customers install and operate alongside their other hardware. In the Infrastructure-as-a-Service model, the customer is responsible for most of the infrastructure's security. Platform as a Service products, such as Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS), or Google Kubernetes Engine (GKE) require substantial in-house security expertise for successful vulnerability management and incident response. For this report, we assess each vendor's ability to deliver both physical and virtual appliances under a single metric.
- **Software as a Service:** SaaS reduces the number of infrastructure components, but the customer remains responsible for secure access and Identity and Authentication Management (IAM) configuration, as well as for setting up proper security guardrails for web applications, and the inspection of API traffic. The customer is exposed only on the application layer, as the security of the underlying infrastructure is the responsibility of the CSP.
- **Software Agents:** In this model, an agent is deployed as an application plugin, a Kubernetes

sidecar, or a utility container for traditional IT applications. Agents integrate into third-party applications, source code management (SCM) tools, the IDE, or they become part of the CI/CD tool kit. Agents can also be deployed as part of IaaS or PaaS because of their similarities to on-premises IT. Lightweight snippets of code can be included in the Infrastructure as Code (IaC) for runtime-focused Dynamic Application Security Testing (DAST) functionality, including Interactive Application Security Testing (IAST) and Run-time Application Self Protection (RASP) use cases.

- **Vulnerability Management as a Managed Service:** We have decided to include managed service as a deployment model due to the practical differences when consuming the service. As a managed service, the underlying tools will use one or more deployment models as described above. Responsibility for vulnerability management and policy compliance can be contracted to a third party. When outsourcing your vulnerability management program, make sure all components are clearly specified and that the vendor contracts remain up to date. This deployment model may require supporting multiple products to provide end-to-end scanning coverage to accommodate the entire SDLC from code development through testing and deployment to running in a production go-live environment.

Table 1. Vendor Positioning

	MARKET SEGMENT			DEPLOYMENT MODEL			
	LARGE ENTERPRISE	MID-MARKET	CLOUD-NATIVE/ STARTUP	IAAS/PAAS	SAAS	SOFTWARE AGENT	MANAGED SERVICE PARTNER PROGRAM
Accurics	++	+++	++	+++	+++	++	++
Anchore	+++	+++	++	-	+++	++	++
Aqua Security	++	+++	+++	++	+++	+	+++
Beyond Security	+	++	+++	+	+	+	+++
BreachLock	++	+++	++	-	+++	+++	-
JFrog	+++	+++	++	+++	+++	-	++
NopSec	++	+++	++	++	++	++	++
Palo Alto Networks	+++	+++	++	+++	+++	+++	+++
Qualys	+++	+++	++	+++	++	++	+++
Rapid 7	+++	+++	++	++	++	++	+++
Risk Sense	++	+++	++	++	++	++	+++
Tenable	+++	+++	++	++	++	++	+++

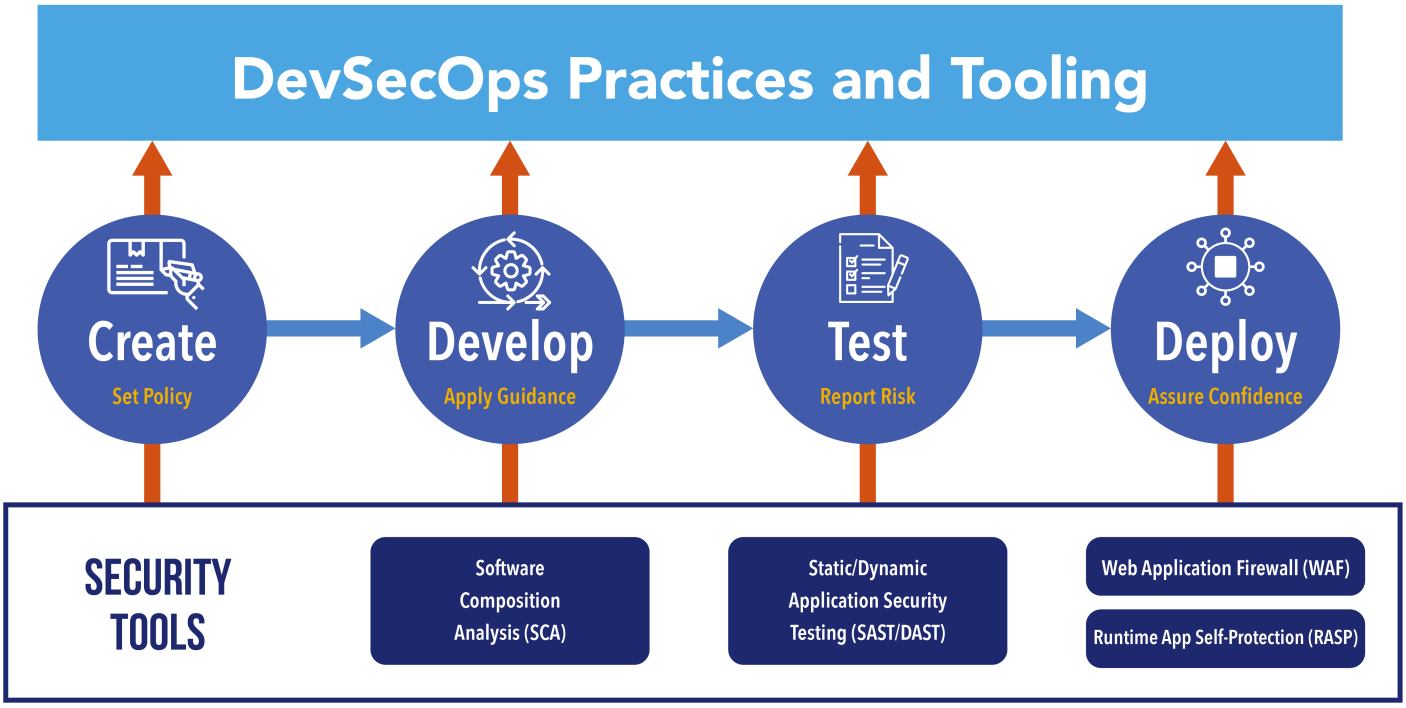
Source: GigaOm 2020

+++ Strong focus and perfect fit of the solution
++ The solution is good in this area, but there is still room for improvement
+ The solution has limitations and a narrow set of use cases
- Not applicable or absent.

3. Key Criteria Comparison

Following the general indications introduced with the "Key Criteria for Vulnerability Management," **Table 2** summarizes how each vendor included in this research performs in the areas that we consider differentiating and critical for modern data protection. The objective is to give the reader a snapshot of the technical capabilities of different solutions and define the perimeter of the market landscape.

Here is a summary of the Key Criteria mapped to the SDLC. Refer to the Key Criteria report for a more in-depth description.



Source: GigaOm 2021

Figure 1. DevSecOps Practices and Tooling

DevSecOps involves a specific set of practices and tooling that evolves as an application moves through the SDLC from development to production go-live. Be sure to check out the report from Gigaom Director of Research, Jon Collins, for more about DevSecOps. The set of practices and tools includes four action items.

- **Create:** Security policies must be established as part of the application design. This first step must be repeated and updated on a regular cadence.
- **Develop:** Assist development teams to integrate these policies into their source code management process directly in the IDE or in the CI/ CD. SCA tools need to be used as soon as possible to scan for open source vulnerabilities in your code.

- **Test:** Rapid feedback from IAST and Dynamic Application Security Testing (DAST) tools during the User Acceptance Testing (UAT) phase of the SDLC enables developers to report on risks discovered prior to release.
- **Deploy**: SRE teams look at the test results to ensure continuous security and reliability of platforms and applications. Organizations may use CSPM, CWPP, RASP, WAF, and API security testing solutions to ensure confidence and protect against real-time threats in production.

Table 2. Key Criteria Comparison

	KEY CRITERIA				
	STATIC APPLICATION SECURITY SCANNING	DYNAMIC APPLICATION SECURITY SCANNING	SOFTWARE COMPOSITION ANALYSIS	API SECURITY TESTING	MACHINE LEARNING
Accurics	+++	+	+	+	+
Anchore	-	+	+++	+++	+
Aqua Security	-	++	+++	-	+++
Beyond Security	+++	+++	-	+++	+
BreachLock	-	++	-	+++	+++
JFrog	-	-	+++	-	++
NopSec	++	+++	-	-	+++
Palo Alto Networks	+++	++	++	-	+++
Qualys	++	+++	+++	+++	+++
Rapid7	-	+++	++	+++	++
RiskSense	++	+++	-	+++	+++
Tenable	++	+++	++	++	+++

+++ Strong focus and perfect fit of the solution
++ The solution is good in this area, but there is still room for improvement
+ The solution has limitations and a narrow set of use cases
- Not applicable or absent.

Source: GigaOm 2020

Table 3. Evaluation Metrics Comparison

	EVALUATION METRICS					
	ADAPTABILITY AND SPEED	SHIFT-LEFT EFFECTIVENESS	END-TO-END COVERAGE	SOLUTION ECOSYSTEM	LICENSING AND SUPPORT	OVERALL ROI/TCO
Accurics	+++	+++	++	+++	+++	++
Anchore	++	++	++	++	+++	+++
Aqua Security	+++	++	++	++	+	+++
Beyond Security	+++	+++	+++	+++	++	++
BreachLock	++	++	+++	++	++	+++
JFrog	++	+++	+	++	+++	+++
NopSec	++	+	++	+++	+++	++
Palo Alto Networks	+++	+++	++	++	+	+++
Qualys	+++	++	+++	+++	++	+++
Rapid7	++	+++	++	+++	++	++
RiskSense	++	+++	++	+++	+++	++
Tenable	++	+++	++	+++	+++	++

Source: GigaOm 2020

+++ Strong focus and perfect fit of the solution
++ The solution is good in this area, but there is still room for improvement
+ The solution has limitations and a narrow set of use cases
- Not applicable or absent.

By combining the information provided in **Table 2** and **Table 3**, the reader should be able to get a clear idea of the market and the available technical solutions.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 2**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

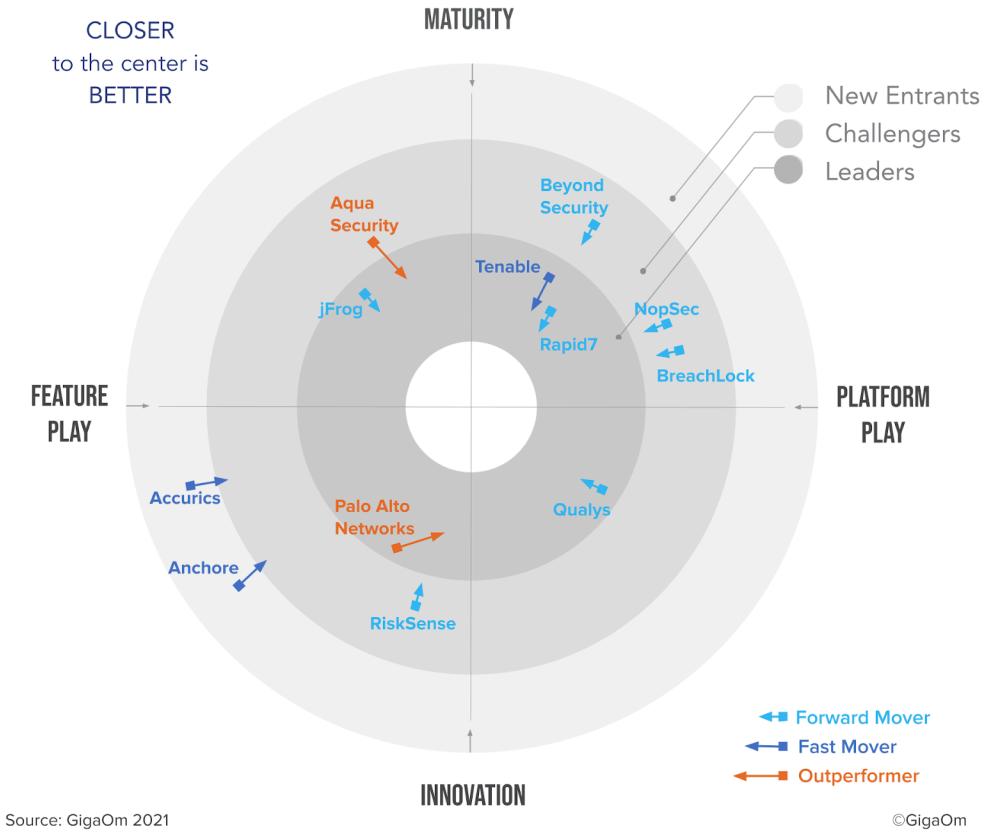


Figure 2. GigaOm Radar for Vulnerability Management

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to center judged to be of higher overall value. The chart characterizes each vendor on two axes—Maturity versus Innovation, and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.

As you can see in the Radar chart in **Figure 1**, the solutions are broadly distributed across every quadrant, with the most active sector being the Maturity and Platform Play quadrant occupied by Leaders Tenable and Rapid7. The distribution reflects the diversity of approaches to managing vulnerability, with some solutions providing a broad platform of functionality that extends and integrates vulnerability management, while others are sharply focused on solving the problem at hand.

Two vendors are notable for their aggressive progress. Palo Alto Networks is a Leader in the Innovation and Feature Play quadrant, and is moving fast based on a spate of important acquisitions. Its hard turn toward the Platform Play quadrant reflects the company's ongoing effort to forge a coherent platform from these acquisitions. Aqua Security, meanwhile, is running hard as a Challenger in the Maturity hemisphere. It is poised to move into a Leadership position based on its broad adoption and wide range of technology integrations and features.

Finally, Qualys has been steadily integrating the technology from its recent acquisition with a robust solution to protect containerized workloads on clusters with hundreds of thousands of services.

Note that many customers will need more than one of these products running to properly cover both legacy and cloud native workloads.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.
The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Accurics Platform

Accurics came out of stealth mode in April 2020 with more than a dozen customers, healthy funding, and a focus on infrastructure-as-code (IaC) security. The Accurics platform enables a self-healing, cloud-native infrastructure by codifying security throughout the development lifecycle, detecting and remediating policy violations, and discovering breach paths via advanced threat-modeling techniques.

Accurics monitors runtime changes using a line-by-line comparison between the code in the IaC repository and the running configuration. The Accurics platform determines the risk of changes in the runtime, and suggests fixes in the IaC. Redeploying the infrastructure through the IaC updates the configuration to the desired state. This provides platform teams with version control for IaC templates.

Accurics supports AWS, GCP, and Azure CSPs, as well as repositories such as Bitbucket, Gitlab, Azure DevOps, and AWS Code Commit. Policy frameworks include CIS benchmarks, GDPR, PCI-DSS, and HIPAA, in addition to home-grown security best practices. Accurics can integrate with SIEM tools such as Splunk, and with CI/CD tools such as Jenkins, CircleCI, and Travis.

Terrascan is a free open source Static Application Security Testing (SAST) tool maintained by Accurics that can detect security vulnerabilities in IaC templates such as Terraform or CloudFormation, and can run locally or integrate with CI/CD tools. It can detect policy violations such as hard-coded secrets and permissive Identity and Access Management (IAM) configurations. Accurics Pro is a paid tier that adds additional security policies and comes with enhanced supervised remediation. The Accurics Team license adds a drift-as-code feature that enables SRE and operations teams to deploy security baselines and version control for the IaC. The Enterprise tier enhances remediation capabilities further with unsupervised mode, as well as breach path and blast radius predictions.

Strengths: Accurics is a best-of-breed solution for static IaC security scanning (SAST) and protection against configuration drift using a rich policy-as-code capability. Accurics delivers a much-needed version control platform for IaC cloud deployments to protect against configuration drift from a secure cloud configuration baseline. The platform allows administrators to roll back insecure or risky changes to their last known secure state.

Challenges: Accurics is a Cloud Security Posture Management (CSPM) tool with a specific focus on IaC code scanning. As such, it successfully addresses CSPM policy compliance use cases for IaC deployments. For a complete vulnerability management solution, additional tools with capabilities such as SCA and Dynamic Application Security Testing (DAST) are needed to address application security in development and at run time.

Anchore Enterprise

Anchore is a startup founded in 2016 by the same team that started the ubiquitous infrastructure

automation tool, Ansible, prior to its acquisition by Red Hat Software.

Anchore provides a fully automated DevSecOps lifecycle management solution focused on vulnerability management and compliance automation by building security for container images directly into software development workflows. The solution aims to remove the majority of accidental or malicious code issues before the image gets promoted to production.

Anchore can assist an organization's efforts to adhere to regulatory standards by hardening infrastructure using a proprietary policy and compliance language. The product enables DevOps teams to shift left in the SDLC using a rich ecosystem of integrations with major tools in container lifecycle stages.

Anchore's open source image inspection and scanning tools consist of two purpose-built tools: Syft and Grype. Syft is a discovery and identification tool that helps generate a software bill-of-materials catalog, and Grype is a vulnerability scanner for container images and filesystems.

Anchore Enterprise is the commercial offering that offers a GUI and support for Windows containers and Kubernetes runtime inventory with an Enhanced Vulnerability Feed. It supports organizations that have multiple development teams and pipelines with compliance and audit-reporting requirements using GraphQL API. Quality Assurance use cases are supported through the use of *allow and deny* lists of images and files to explicitly prevent applications that are out of compliance from running. This feature improves the overall quality and security of the software more effectively than legacy methods do. Additionally, Anchore Enterprise can be used as a centralized service to automate image validation and certification by leveraging out-of-the-box policies.

Finally, Anchore Federal is a purpose-built solution created in collaboration with the Department of Defense for government and defense agencies that operate in air-gapped environments to meet security requirements ranging from DoD IL-2 to DoD IL-6, and compliance that meets TIG and NIST standards and FedRAMP guidelines.

Strengths: Anchore's SCA capabilities not only inspect OS and application packages, but also non-packaged files and software artifacts including third-party libraries, licenses, binaries, credentials, API keys, metadata, secrets, passwords, and other sensitive information. This includes GEM, NPM, PIP, and Java archive files. Anchore scans all container layers and checks dockerfiles.

Challenges: Anchore is a strong contender when deep Software Composition Analysis (SCA) capabilities for scanning containers are required. Other IT assets, however, such as physical or virtual machines remain out of scope for this solution, and need to be managed by a different tool.

Aqua Security Platform

Operating since 2016, Aqua Security might be best known for its popular open source image vulnerability scanner, Trivy. Selected by Gitlab as its default scanner, Trivvy has gained momentum

and is quickly becoming the standard for vulnerability scanning in cloud native environments. The Aqua Security Platform supports comprehensive scanning of virtual machines, containers, and serverless functions, and enables SCA through application dependency detection in container images.

With Kubernetes Security Posture Management (KSPM), Aqua can help reduce the attack surface for containerized workloads, reduce administrator errors, and protect against common attack vectors described by the MITRE ATT@CK framework. Aqua supports regulatory compliance enforcement for PCI DSS, NIST, CIS, and HIPAA, among others, and can allow only the images and workloads that pass compliance checks to run in production.

Aqua's vShield technology is a differentiating feature unique to Aqua that gives security teams more runway to patch vulnerabilities. It acts as a compensating runtime control for containers with vulnerabilities that cannot be fixed immediately. vShield provides a virtual patch that prevents the exploitation of the vulnerability without requiring the stopping of services. Machine learning can determine the potential attack vector of the CVE, and the impact it might have on production.

Aqua's CyberCenter threat intelligence feed provides additional context to detection results, leveraging a regularly updated vulnerability database that is composed of several external sources and enriched with the company's own research. The Risk Explorer feature provides a compound view of prioritized risks in the environment, taking into account containers, images, clusters, and networking risks.

Aqua Dynamic Threat Analysis (DTA) can detect sophisticated supply chain attacks in container images by running them in a secure sandbox to trace and analyze their runtime behavior and detect multiple Indicators of compromise (IOCs), such as container escapes, malware, cryptominers, code injection backdoors, and network anomalies.

Aqua provides API-based integration with Jira, PagerDuty, Slack, and ServiceNow, and supports all major CI/CD tools including Jenkins, Azure DevOps, Bamboo, Gitlab, and more.

Aqua's SaaS-based offering works across all major clouds, but it can also run on-premises. Free trial and POC licenses are available, and paid licensing is subscription-based, paid annually.

Strengths: The Aqua platform has solid support for dependency scanning, provides out-of-the-box policy controls in its UI, and is fully API-driven for external customization. It also provides a complete multi-application Role-Based Access Control (RBAC) model, which enables teams and stakeholders across an enterprise to use the platform while maintaining segregation of duties both between teams and between different roles within teams.

Challenges: Aqua is focused on DevOps pipeline optimization, and is particularly strong for containerized and serverless workloads; as such, it doesn't perform traditional infrastructure or network vulnerability assessments. Support for SAST, API, and IaC scanning is lacking.

Beyond Security

Founded in 1999, Beyond Security is an automated penetration testing and compliance company based in Roseville, California. Its beSECURE product is a complete vulnerability assessment and management platform that can be expanded with its static code analysis capabilities, beSOURCE, to shift security left during devtime in the SDLC. beSTORM provides DAST capabilities that can be used by SRE teams during UAT for fuzz testing web applications to test unexpected, partial, or invalid inputs to the data structure and web-based APIs. beSTORM includes a self-learning function that lets the user teach it custom protocols to detect security vulnerabilities.

beSECURE integrates with leading asset management systems to import assets automatically for scanning. Network reconnaissance periodically scans subnets to detect assets and highlight new ones through a blind spot detection mechanism that can infer and report the existence of assets referenced in configurations. The reporting capability can be customized based on manual or automatic rule-based tagging.

Reports include all Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) information, as well as priority assignments based on assets or via specific rules to change the weight of certain assets or vulnerabilities. Policy-based reports are available as well to external benchmarks and standards (OWASP, the various CIS benchmarks, HIPAA, GDPR, and so forth). beSECURE allows risk re-prioritization through automated triggers and business-logic-based reporting to find vulnerabilities across business functions rather than just with CVSS scoring.

The service can be delivered via SaaS, or hybrid/on-premises with hardware or VMs. There is also an MSP offering that can scale to thousands of customers with millions of IP addresses. Beyond Security supports all cloud platforms and integrates with more than 100 other security tools. The licensing depends on the number of assets scanned and can be expanded on demand.

Strengths: Beyond Security delivers a strong platform to reduce threats in real time. Lightweight agents make visible and secure IoT, IT, OT, BYOD, and other supported endpoints on the network. Sensors that collect and correlate endpoint, application, cloud, and network telemetry data essentially make Beyond Security an eXtended Detection & Response (XDR) solution.

Challenges: The product does not offer SCA capabilities, but these can be added with third-party integrations. Beyond Security may be lacking in marketing, but end users who try out the platform are usually quite pleased with the results.

BreachLock Platform

BreachLock is an AI-powered solution that provides full-stack Penetration Testing as a Service, covering applications and network and cloud workloads. It offers a cloud-native SaaS solution without client environment limitations, and targets the financial services, government, computer software, and healthcare market segments.

BreachLock offers a continuous vulnerability scanning and penetration-testing platform with actionable results for public clouds, applications, and networks. The BreachLock platform uses a centralized asset inventory that is shared across the SaaS platform's capabilities. Due to its modular approach, BreachLock allows clients the flexibility to switch particular capabilities on or off for specific assets in the inventory. The BreachLock platform has an auto-discovery feature that works seamlessly with AWS, Azure, and GCP clouds.

The platform provides CVE scanning for infrastructure components and web applications, and assigns priorities to assets and discovered vulnerabilities. Application scanning capabilities go beyond CVE based checks and actually fuzz the applications with customized payloads to discover application-centric unknown vulnerabilities. BreachLock provides risk ratings that are scored on default CVSS, and vulnerability data is enriched with additional evidence and context.

For policy compliance, Breachlock supports common frameworks, such as PCI DSS, NESA, HIPAA, GDPR, and CIS Benchmarks for AWS, Azure, Google Cloud, Docker, and Kubernetes, with a cloud audit module on the roadmap. BreachLock offers seamless integration with DevSecOps and CI/CD, and out-of-box integrations with tools such as Atlassian Jira, Trello, Slack, and Jenkins.

BreachLock's proprietary penetration-testing automation engine dynamically tests web applications (DAST), networks (external and internal), and APIs.

Strengths: BreachLock provides Exploit Database-based detection of vulnerabilities, with asset management, automated patch validation, CI/CD integration, and support for external ticketing systems. BreachLock is highly scalable and uses AI as a force multiplier across all features. It is the only solution offering Penetration Testing as a Service, as well as a hybrid option with manual penetration testing via certified OSCP and CREST experts. The SaaS console interface streamlines human pen testing.

Challenges: BreachLock currently lacks a devtime coding solution (SAST, SCA) to provide real-time feedback to developers. For source code language support (Python, Java, C, C++, COBOL, and the like), other static code analysis tools are needed. Customization can be a challenge, and existing vulnerability management programs would need to significantly revamp their workflows to take advantage of its AI-powered features.

JFrog Xray

A longtime leader in the vulnerability management space, JFrog is widely deployed at major institutions across the globe. It supports both legacy, on-premises Windows- and Linux-based applications, and modern cloud-native apps built on Kubernetes containers. The JFrog DevOps Platform enables vulnerability management primarily via its JFrog Xray solution, enabling SCA capabilities on top of JFrog Artifactory – the platform's central, universal, package management/repository solution which functions as the "Database of DevOps" for managing all software binaries and container images in the organization.

JFrog Xray scans both “traditional” binaries and OSS packages as well as container images with deep recursive scanning of all layers of the image, including the operating system. As a result, JFrog stands out as a compelling solution for established enterprises seeking to adopt a hybrid, universal solution to support a cloud-first posture, be it in on-premises, hybrid cloud, or multi-cloud deployments.

Xray scans binaries recursively to identify all open source software (OSS) components in the different binaries or container levels and detect any known security vulnerabilities or license compliance issues. JFrog Xray provides continuous impact analysis with notifications of new vulnerabilities by alerting the user and helping to identify which binaries are affected. Users can define different policies for different binaries in the organization—based on CVE severity or other rules—to detect and eliminate critical vulnerabilities in production, test, or development.

Xray plugins integrate with Jira, Jenkins, Azure Devops, Bamboo, and TeamCity. A number of IDEs, such as Visual Studio Code, IntelliJ IDEA, WebStorm, GoLand, Eclipse, and Microsoft Visual Studio, are supported.

A dedicated team of analysts at JFrog is responsible for building and maintaining the Xray knowledge base with data about OSS packages, their known vulnerabilities, and their licenses. In addition to using the vast number of open source or publicly available resources such as NVD and others, JFrog has partnered with a company of security researchers, Risk Based Security, to include VulnDB as one of Xray’s knowledge base sources.

Teams can review their own security and compliance violations using a “Watch” which can be scoped per application/teams/environments/repositories, and more. JFrog Xray integrates into the developer’s code editor and alerts the developer when a vulnerability that comes from an OSS dependency gets introduced while writing code, along with the steps for remediation to patch the vulnerability. Identified violations can trigger the creation of a ticket in any system (such as JIRA), via a Webhook integration.

JFrog Xray can also integrate into CI/CD tools to scan a build, and fail it based on security or risk information, if the user wishes to do so. Uniquely, it can even block developers from the initial download of OSS dependencies with known vulnerabilities or those that have not been scanned yet, as the most strict rule for central management of security and governance in the organization.

Strengths: SCA solutions like Xray are ideal for finding known vulnerabilities in open source libraries in the images used in containerized workloads, such as those deployed on Kubernetes for hybrid, on-premises, and multi-cloud environments. Jfrog Xray scans images in the background as part of the DevOps CI/CD pipeline. ML-driven impact analysis recursively scans and identifies the parts of the system affected by potential vulnerabilities.

Challenges: Xray does not offer DAST functionality or web application runtime scanning and lacks support for Ansible and Terraform code. Also, Xray does not support scanning API communications, so it requires deploying alternate solutions to have full vulnerability management coverage in the SDLC.

NopSec Unified VRM

NopSec helps companies identify and fix vulnerabilities and risks leading to potential cyber exposure. The company does so by providing visibility into process ownership across the vulnerability management lifecycle for infrastructure, endpoint, security, and application teams. NopSec also offers a managed vulnerability management service that can help to quickly stand up an end-to-end vulnerability management program from detection to remediation in a single SaaS platform.

The Unified VRM platform provides complete visibility by aggregating infrastructure, endpoint, and application vulnerabilities in one place, with prioritized remediation based on your business and threat contexts. Infrastructure scanning discovers network topologies and scans for vulnerabilities both from the cloud and via virtual scanner appliances offered by partners deployed on public and private clouds.

NopSec Unified VRM helps to reduce noise and eliminate false positives through risk-based prioritization, leveraging machine learning algorithms. This feature allows security professionals to prioritize the most important vulnerabilities to fix first across infrastructure, endpoints, and applications. Additional attack surface reduction can be achieved through a combination of technologies, ranging from digital footprinting, to reconnaissance, to ingestion of pen-test results, and correlating between system- and human-detected vulnerabilities.

Unified VRM provides scanner-agnostic ingestions from on-prem and cloud infrastructure, web application (DAST, SAST), container, and OT scanners, and can correlate asset priority recommendations. Unified VRM has a microservices-based architecture and each microservice is deployed with auto-scaling policies in place to dynamically adjust capacity up or down according to conditions.

There are three licensing levels for enterprises: Essential, Complete, and Journey, as well as two types of partner-program licensing models: a technology partnership for integration within an ecosystem such as AppScan or ServiceNow, and a channel or distribution partnership to deliver an outcome such as an embedded application for customers.

NopSec partners with its customers to increase the maturity of its vulnerability management program from simple patching and remediation to threat-based analysis, and finally to a full risk-management program with continuous patching and automation.

Strengths: The managed risk-based vulnerability management (RBVM) program in a box allows customers to access the cloud platform and customer success engineers and domain experts from NopSec's Red Team. User-friendly dashboard enables less-experienced users to manage remediation of critical vulnerabilities. ML algorithms combined with threat intelligence tools can leverage tagging to configure scanning, prioritization, and remediation for quick customer response.

Challenges: NopSec does not offer its own scanners. Instead, additional contracts with NopSec partners are needed to complete the solution. There is no support for cloud-native scanners, but

integration with AWS Inspect and GCP is on the roadmap. Currently, NopSec does not offer real-time blocking or runtime protection.

Palo Alto Networks Prisma

Palo Alto Networks (PAN) is a leader in vulnerability management and risk assessment across cloud infrastructures and applications. Its cloud native security platform, Prisma Cloud, ingests APIs from cloud services across Alibaba Cloud, AWS, Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI) to provide singular visibility into cloud accounts. Built-in policies monitor the security and compliance posture of resources, while an audit trail is maintained in the CMDB that tracks any changes in a resource as soon as it is deployed. Its Resource Query Language (RQL) enables users to gain deep insights into network topology, configurations, and events across multi-cloud, multi-object environments.

Since 2019, PAN has integrated and enhanced the technology from Evident.io and RedLock to offer a more comprehensive CSPM solution. Twistlock and PureSec have also been included as part of the SaaS platform to secure container and serverless workloads. PAN now also includes Aporeto tech for identity-based micro-segmentation and machine protections. Most recently, Bridgecrew was acquired to shift security left in the application lifecycle and to give Prisma Cloud customers the ability to integrate security controls early in their SDLC.

Bridgecrew's popular open source IaC scanner, Checkov, is now part of the PAN portfolio and can be used to scan cloud infrastructure code in Terraform, CloudFormation, Kubernetes, ARM templates, or a serverless framework to detect misconfigurations.

Integrated vulnerability data from Defender agents as well as third-party sources, combined with additional threat intelligence sources (AutoFocus) and cloud service providers (GuardDuty) supply the data necessary to automatically rank every security event by level of severity to determine the impact on security posture.

Prisma Cloud supports 16 prebuilt compliance frameworks, including HIPAA, GDPR, Soc2, and MITRE ATT&CK, as well as custom policies. It is certified to implement the AWS, Docker, Kubernetes, and Linux CIS benchmarks, as well as custom compliance checks for Istio and Windows.

Alerts can either be resolved via Prisma Cloud or sent to numerous different tools for integration with existing remediation processes. Integrations include Security Hub, SQS, Cortex XSOAR, Splunk, Jira, PagerDuty, ServiceNow, Slack, and many others, and there is also general support for Webhooks.

Vulnerability details include library and package information, vendor fix details, and status, risk tree, and risk severity details. All of these findings are available in central dashboards, in third-party dashboards via the API, or in native CI tooling. DevOps tools supported include BitBucket, CircleCI, GitHub, GitLab, Hashicorp, Jenkins, and Microsoft Azure Devops Pipelines.

Strengths: Findings from integrations with third-party DevOps tools can be onboarded into the Prisma Cloud console to be included as policy alerts that go to DevOps engineers for investigation. Prisma Cloud features runtime protection for workloads including hosts, containers, and serverless, as well as auto remediation of policy violations with both built-in and customizable playbooks. The Vulnerability Explorer analyzes data based on environmental context observing containers during runtime to prioritize remediation recommendations.

Challenges: The incident response team still needs an external system such as ServiceNow or Splunk to triage incidents. Most customers will need to configure alert rules to send event data to a SIEM for enrichment and correlation with additional sources. This task can entail a significant effort to keep up to date with new cloud APIs and corresponding policies.

Qualys VMDR

Qualys is familiar to most security professionals as a market leader in vulnerability assessment, remediation, and patching of critical vulnerabilities across hybrid IT infrastructures.

Qualys VMDR has a number of sensors that work together to discover and inventory assets in hybrid IT environments, including devices and applications that are on-premises or mobile, as well as endpoints, cloud objects, containers, certificates, and OT and IoT. Sensor options include lightweight agents, passive listeners, virtual scanners, internet scanners, cloud connectors and many more. Assets can be synchronized with a CMDB, and enriched with information about running services, software versions, and open source licenses.

VMDR continuously scans for vulnerabilities including policy compliance violations using a comprehensive signature database. Users can correlate inventory scans with real-time threat indicators, leveraging machine learning models and innovations. Necessary patches get flagged and ranked according to priority. Automated workflows can kick off vulnerability patching using Qualys Cloud agents or third-party integrations.

Qualys can assess security-related misconfigurations and support regulatory compliance requirements by automatically evaluating requirements against multiple standards which are updated daily. Data from inventory scans is correlated and vulnerabilities are prioritized using real-time-threat indicators (RTIs) (e.g., actively exploited, exploited by malware, etc.), and multiple attack surface options (such as running vs. non-running services, internet facing assets). Impacted assets are automatically mapped using Threat Protect. Customers can select reports from the many prebuilt policies such as CIS, COBIT, ISO 17799 and 27001, NIST SP800-53, ITIL v2, HIPAA, FFIEC, NERC-CIP, PCIDSS, and more.

Qualys shifts security left in the CI/CD pipeline with a cloud-native DAST scanner that catalogs, crawls, and tests web applications on the network. Qualys' Web Application Scanning (WAS) is a service that crawls and tests web applications while searching for malware, including zero-day threats, via behavioral analysis. WAS can be integrated into DevSecOps environments for automated scanning jobs in the CI/CD environment using a native plugin for Jenkins. Deep scanning for OWASP Top Ten

risks as well as SOAP and REST API scanning are supported.

Qualys Container Runtime Security provides behavior visibility and enforcement capabilities for running containers. Through instrumentation with probes injected into the container, granular policies can be enforced to govern behavior. Threats can be detected and blocked based on a deviation from a policy of the container, and runtime events can be monitored via UI or API. Use cases include container security best-practice enforcement, file access monitoring, and network access control. Web application vulnerability data from penetration tests can be consolidated with Qualys scan results to get an end-to-end view of your infrastructure and application security posture.

Qualys scanner virtual appliances are available for VMware as well as most popular public cloud providers (AWS, Azure, and GCP). Microsoft Azure customers benefit from integrated Qualys vulnerability scans with results showing up in the Azure Defender dashboard.

Strengths: Qualys offers public cloud provider API integration with CloudVIew connectors to correlate basic cloud infrastructure resource information with data from network scans and agents installed on Linux and Windows servers. Qualys excels as a vulnerability management tool for Linux and Windows workloads and has extensive support for other types of assets such as networking devices, hypervisors, databases, and firewalls. Qualys has stepped up its CSPM game and now supports configuration scans via API for popular cloud platforms included CIS benchmarks, Kubernetes best practices, and general Cloud Security best pratices.

Challenges: Policy compliance coverage for cloud-based workloads is less than optimal, with Google GCP coverage lagging Amazon AWS and Microsoft Azure—an issue common to many products. Qualys lacks a SAST solution at this time. Policy compliance checks are done once an hour, leaving gaps in coverage similar to other cloud providers. Supplementing with event-based policy violation alerts is recommended for the most critical configuration errors.

Rapid7 Vulnerability Management & Application Security

Rapid7 is a market leader with a comprehensive security suite covering vulnerability management (InsightVM), application security (InsightAppSec), cloud security (DivvyCloud), detection and response (InsightIDR), log management (InsightOps), and orchestration and automation (InsightConnect).

Deployments can be hosted in a customer's private network and data center (Metasploit and Nexpose) and can be run from the cloud-hosted Rapid7 SaaS as a managed service as well.

InsightVM provides cloud and virtual infrastructure assessment, container security, and integrated threat intelligence feeds. The Insight agent is a lightweight sensor that continuously monitors and collects telemetry data from any assets in the cloud or on-premises. The agent also can be used for Rapid7's endpoint threat detection and log management solution. The automation-assisted patching workflow integrates with IBM BigFix and Microsoft SCCM to patch and verify discovered vulnerabilities.

Both InsightVM and InsightAppSec collect policy compliance audit information to report on an organization's customized policies as well as on industry standards such as CIS, HIPAA, SCADA, PCI-DSS, OWASP Top Ten, and other regulatory requirements.

InsightVM works with CI/CD pipeline tools like Jenkins to determine whether container builds should be marked as failed, unstable, or passed, based on vulnerabilities associated with the packages and layers of a container image. Risk prioritization is achieved via a proprietary Real Risk algorithm that enriches CVSS base metrics with asset impact, exposure type and length, and exploitability of the vulnerability.

For DAST capabilities, InsightAppSec automatically crawls and assesses web applications for vulnerabilities such as SQL injection, XSS, and CSRF. In addition, APIs such as SOAP and REST web services can be tested with InsightAppsec.

In May of 2020, Rapid7 acquired DivvyCloud, which provides CSPM capabilities for Amazon AWS, Microsoft Azure, and Google GCP, as well as IaC security scanning.

Rapid7 has also integrated development efforts to work with Snyk to provide SCA capabilities to track vulnerabilities in open source packages used during runtime.

Strengths: The Rapid7 suite of products offers a compelling one-stop shop with native interoperation of SIEM, SOAR, and EDR functionality. InsightVM integrations improve flexibility and make it easy to adapt to different architectures. Rapid7 works with DevOps tools to improve any development and deployment process. Rapid7 offers unique and valuable runtime protection (RASP) and web application firewall services (WAF) through its acquisition of tCell.

Challenges: For end-to-end coverage, multiple products must be licensed to reap the benefits of Rapid7's security suite integration. The solution lacks SAST support, so alternate approaches are needed to fill the gaps.

RiskSense RBVM

RiskSense was founded in 2015 to help organizations identify, score, and prioritize critical security weaknesses of internal and externally facing assets with prescriptive remediation action plans.

For customers who already have vulnerability management scanners deployed, the risk-based vulnerability management (RBVM) solution can be deployed as a SaaS subscription to aggregate data from existing infrastructure, application, and code scanners, as well as asset management and manual findings such as penetration results. The RBVM platform provides a single pane of glass to assess and report on risk metrics across your entire IT estate through threat contextualization and the segmentation and labeling of data. Automation playbooks can be used to kickstart remediation workflows by leveraging out-of-the-box integration with incident management platforms such as BMC Remedy, ServiceNow, and Atlassian.

The RiskSense Vulnerability Management as a Service is a fully managed solution that provides vulnerability scanning, security rating, and penetration testing without any need to invest in the individual vulnerability management components.

RiskFusion is an industry-leading proprietary threat, vulnerability, and exploit database that is correlated with machine learning-enabled contextualization to produce best-in-class vulnerability risk scores based on accessibility, business criticality, and probability of exploitation.

The RiskSense platform ingests vulnerability data from all leading network and application vulnerability scanners, including Tenable, Qualys, WhiteHat, Rapid7, Veracode, and others.

Strengths: The fully managed solution provides a number of immediate benefits to customers. As it is an elastic service, customers can start small and easily scale up (or down) as business needs dictate. A wide range of integrations and AI features mean this platform is versatile and easy to use.

Challenges: While RiskSense does integrate with SAST, SCA, and DAST scanners, there is no native integration with IDEs (like Visual Studio) or CI/CD pipeline tools (like Jenkins). The ability to perform policy compliance on code used to build infrastructure—using tools like Terraform, Ansible, Chef, Puppet, and others—is also missing, so other solutions are needed to fill these gaps.

Tenable tenable.io

For more than 20 years, the Tenable Nessus network scanner has been used by large enterprises and SMBs alike to detect vulnerabilities in both infrastructure and application software. Tenable maintains a strong leadership position with its Cyber Exposure platform. By using supervised machine learning algorithms to rate the priority of vulnerabilities, Tenable effectively addresses risk profiling and prioritization requirements in vulnerability management programs.

Tenable.io Web Application Scanning is a purpose-built DAST scanner designed for active interrogation of modern web apps. In addition, passive scanning and network monitoring are a core constituent of the Tenable Vulnerability Management offering through Nessus Network Monitoring used to discover assets and vulnerabilities in real time. Through the use of test access point (TAP) or Switched Port Analyzer (SPAN) ports, use cases that involve operational technology (OT) devices such as programmable logic controllers (PLC) and remote terminal units (RTUs) that monitor IoT devices are served. Tenable supports many industrial networking protocols not typically available in other products, thanks to the acquisition of Indegy in 2019.

The Tenable Vulnerability Priority Rating (VPR) calculations are assigned on the basis of threat recency, intensity, exploitability, age, and sources. In addition, Asset Criticality Rating (ACR) is a score in the Tenable Lumin dashboard that can be used to determine the criticality ratings of inventoried assets. This analysis is performed on the basis of business purpose, device type, connectivity, capabilities, location, and third-party data associated with the asset.

Tenable.io Container Security, combined with Tenable.io Vulnerability Management and Tenable.io Web App Scanning, provides end-to-end coverage in the stack and can be used in the SDLC to manage vulnerabilities from host infrastructure to the application code. Through a partnership with Snyk, Tenable extends its capabilities to include SCA also through an integration with their intelligence vulnerability database. Tenable.io Container Security offers two modes of operation: Either the image bill of material inventory data is sent to a cloud scanner or the scanner connects to a container registry and the images are scanned there. The product also integrates with numerous third-party container image registries for daily assessments. Users can integrate Container Security into their CI-CD systems as well using APIs to assess new image builds.

Both Docker images and Open Containers Initiative (OCI) image formats are supported.

Strengths: Tenable boasts broad asset coverage, including OT devices. Its Predictive Prioritization and VPR risk-based vulnerability features help remediate critical vulnerabilities. Tenable boasts a large research team that provides actionable vulnerability disclosures and supporting data to prioritize patching of high severity and exploitable vulnerabilities. The Cyber Exposure platform can run on-premises or fully managed in the cloud. Exposure.ai is a very large data lake that contains more than 20 trillion aspects of vulnerability and threat data, and more than 20 million threat artifacts maintained by tenable.

Challenges: Frictionless assessment is offered only for AWS, with more limited options for customers using Azure and GCP. Nessus does not support integration of third-party data sources or device scanners.

6. Analyst's Take

As cyber threats become more complex and sophisticated, modern IT environments are also seeing the diversity and the number of IT assets grow substantially. The scope of any vulnerability management program must be adjusted to cover a growing and more varied protect-surface.

Vendors have innovated their products by shifting security left and enabling DevSecOps teams to build secure applications from the beginning through integration with development operations, and to help incident response teams prioritize remediative efforts on the basis of risk assessments that take local context and external threat landscape parameters into consideration.

However, we still see many gaps when it comes to providing end-to-end coverage to support the entire protect-surface. While some products are point solutions that need to be integrated with other products in the ecosystem, others are more comprehensive and can be delivered as part of an overall security platform. The decision to buy a comprehensive solution from a single supplier or build a customized solution with multiple components from various vendors can determine operational risks down the road when product upgrades will be required or when economies of scale are introduced.

The increase in local assets and external threat information has led to an exponential growth in raw data, detections, and alerts. Machine learning and artificial intelligence techniques are innovations necessary to reduce the complexity of correlating different internal and external data sources, and to minimize the time spent by analysts on finding attacks hidden in a sea of false positives and investigation backlogs.

With today's fresh understanding about supply chain attacks in software from trusted vendors, we can see that threats facing an organization should inform not only the teams responsible to help prioritize vulnerability patching and remediation, but also be considered as part of regular architecture reviews and identity management audits. IT decision makers should consider expanding their mandates to include policy compliance audits and monitoring of service account usage for normal versus anomalous behaviors. Policy compliance with hardening benchmarks like those offered by CIS for cloud providers and Kubernetes is an important part of a comprehensive vulnerability management program.

While modern IT environments require both preventative and detective controls, vulnerability scanning is ultimately only a preemptive measure against cyberattacks. Scanning and patching known vulnerabilities is necessary, but not sufficient, to mitigate attacks in progress. Assuming that an intrusion into your environment is only a matter of time, IT decision makers would be well advised to focus on indicators of compromise (IOC) by leveraging additional intelligence from a wide range of metadata sources, such as DNS, proxy, and network flows to detect and characterize an attack in progress. These tools work as failsafe detective controls that inform users after a compromise has taken place and can be effective in evaluating the success of any preventative controls that might be in place.

7 About Iben Rodriguez

Iben Rodriguez began his security career in the 80s maintaining the data communication systems used by military reconnaissance overseas, and followed this with stints in the global pharmaceutical and fabless semiconductor industries. He has been an advisor to executive teams from both enterprise and government organizations, such as AT&T, Brocade, CA, Cisco, eBay, Ericsson, Google, Huawei, Intuit, Juniper, Microsoft, US Navy, Pentagon, Spirent, and VMware.

Iben helps financial services customers connect cloud security solutions using DevOps methods. He works with Center for Internet Security (CIS) on the Amazon AWS, Google GPC, Microsoft Azure, and VMware ESX benchmarks, and is active with Linux Foundation, OPNFV, Palo Alto Networks, VMware, and HyTrust

8 About Geoff Uyleman

Geoff is an IT architect with 25 years of experience delivering secure workloads in the cloud and in the data center. His background ranges from system engineering and product management to leadership in agile collaboration and DevSecOps.

He was part of the StorageNetworks team around the year 2000–a company that pioneered backup-as-a-service for enterprises by delivering remote storage services across metro fibre from a nearby co-location facility–something we would call a private cloud today. Over the years, Geoff has worked with technology vendors such as Cisco, eBay, PayPal, and StorageTek. And in addition to service providers such as AT&T and Sprint, he has also helped European government agencies and the military in their digital transformation journey.

Geoff assisted the research and development efforts at the Xerox Palo Alto Research Center related to sustainable datacenter operations. His research topics of interest are cloud, security, and blockchain technologies, as well as applying quantitative methods to solving problems in the digital humanities.

Geoff graduated Cum Laude from Brigham Young University with a BA in philosophy and logic.

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright