KuppingerCole Report

LEADERSHIP COMPASS

By Alexei Balaganski

April 05, 2022

Container Security

This report is an overview of the market for Container Security solutions and provides you with a compass to help you to find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to securing container-based application architectures.

By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 Introduction / Executive Summary

In less than a decade, containers have undergone an impressive evolution: from a lightweight virtualization technology to the de-facto standard for software distribution to a powerful underlying platform for complex and distributed applications. For many organizations, container orchestration platforms like Kubernetes serve as a universal foundation for deployment, scaling, and management of applications that works consistently across on-premises and multi-cloud environments.

The growing demand for new software architectures has given rise to microservices that allow businesses to develop and deploy their applications in a much more flexible, scalable, and convenient way - across multiple programming languages, frameworks, and platforms. Microservices, containers, and Kubernetes have quickly become synonymous with modern DevOps methodologies, continuous delivery, and deployment automation and are generally praised as a breakthrough in developing and managing cloud-native applications and services.

Unfortunately, this massive change in infrastructure and a major increase in overall complexity (although much of it is hidden from developers thanks to multiple layers of abstraction and convenient tools) has introduced numerous new risks and security challenges as well as new skills needed to mitigate them efficiently.

Initial attempts to repurpose existing security tools for protecting containerized and microservice-based applications have quickly proven to be inadequate due to their inability to adapt to the scale and ephemeral nature of containers. Static security products that focus on identifying vulnerabilities and malware in container images, while serving a useful purpose, do not address the full range of potential risks.

The need to secure containerized applications at every layer of the underlying infrastructure (from bare-metal hardware to the network to the control plane of the orchestration platform itself) and at every stage of the development lifecycle (from coding and testing to deployment and operations) essentially means that container security has to cover the whole spectrum of cybersecurity and then some.

Figure 1: The true scope of container security

This is why for this Leadership Compass, we have decided to focus primarily on the universal container and Kubernetes security platforms, which aim to analyze, monitor, assess, and mitigate risks along the full lifecycle of application containers - starting with developing, testing, and hardening container images to runtime monitoring and threat detection to responding to identified security incidents. At the same time, we expect container security solutions to expand their coverage to multiple layers of infrastructure including hardware, host OS, virtualization, and networking layers.

1.1 Highlights

- In less than a decade, containers have quickly evolved from a simple idea of packaging software for distribution into a universal platform for automating application deployment, scaling, and management.
- Docker containers and Kubernetes orchestration platform have emerged as the most popular standard for developing, packaging, and running modern cloud-native, loosely coupled, highly scalable application architectures across multi-cloud and hybrid environments.
- Universal adoption of containerized architectures has fundamentally changed the ways of collaboration between developers, operations, and security teams, enabling new cloud-native and hybrid DevOps use cases, but bringing new risks and threat vectors as well.

- Repurposing existing cybersecurity tools for the sheer scale and ephemeral nature of modern container platforms is a challenging task for vendors, and these tools are not suited to address the container-specific risks such as securing Kubernetes clusters and registries.
- At various stages of the container lifecycle, different stakeholders are responsible for securing specific parts of container infrastructures, thus creating the potential for additional friction and miscommunication between teams. Removing this friction is one of the primary goals of modern container security solutions.
- The market for specialized container security solutions is growing rapidly with large public cloud providers, large veteran security vendors, and innovative startups offering competing solutions targeted towards customers of different sizes and from various industries. As with many other cybersecurity markets, this segment is undergoing active consolidation, with large vendors acquiring specialized solution providers and integrating their tech into full-range security platforms.
- Both small and fully cloud-native software development teams and large organizations with massive on-prem or hybrid infrastructures can find the solutions most appropriate for their needs: from fully managed natively integrated security controls in container orchestration services to universal, flexible, and open enterprise-grade platforms.
- The overall leaders in the Container Security market are Aqua Security, Palo Alto Networks, and Red Hat.

1.2 Market Segment

Containers are standardized units of software that package application code and all required dependencies into portable images that can be seamlessly deployed in various environments. A container image includes everything an application needs to run - a runtime environment, system libraries and tools, and settings. A single container image can be easily shared between multiple execution environments, as well as instantiated multiple times to support scalability, high availability, and support for hybrid and multi-cloud deployments.

Originally a lightweight form of virtualization, containers have emerged as a more resource-efficient alternative to virtual machines. However, they have quickly become the de facto standard for packaging and deploying applications across heterogeneous infrastructures without any modification. For developers, this creates the opportunity to develop and test their applications as single units that are guaranteed to work the same way across all development and production environments. For operations teams, container orchestration platforms greatly simplify the deployment of complex, loosely coupled applications, both on-prem and in every cloud.

Modern container orchestration platforms build upon this foundation to provide a broad range of additional services that help automate scalability and high availability configurations and provide rich run-time management and analytics capabilities. The Kubernetes platform has emerged as a universally accepted standard for container orchestration abstracts and hides the complexity of resource management across computing clusters and incorporates functions like service discovery, load balancing, runtime monitoring, etc. A number of management APIs allow a rich ecosystem of third-party tools and services to integrate with the service.

All these capabilities have made containers and container orchestration the preferred choice for organizations around the world to develop, distribute and operate their applications at scale. However, the hidden complexity of these multilayer technology stacks has inevitably introduced new risks that have to be assessed and mitigated.

What further differentiates container security as a discipline within the larger scope of cybersecurity is that it spans multiple organizational units and teams, which often have conflicting goals and requirements. Application developers, infrastructure operations teams, cloud engineers, security analysts and incident response units, even auditors and legal experts - at different stages of the container lifecycle, they have a say at how exactly this container should be created, inspected, run, monitored, and protected from various risks.

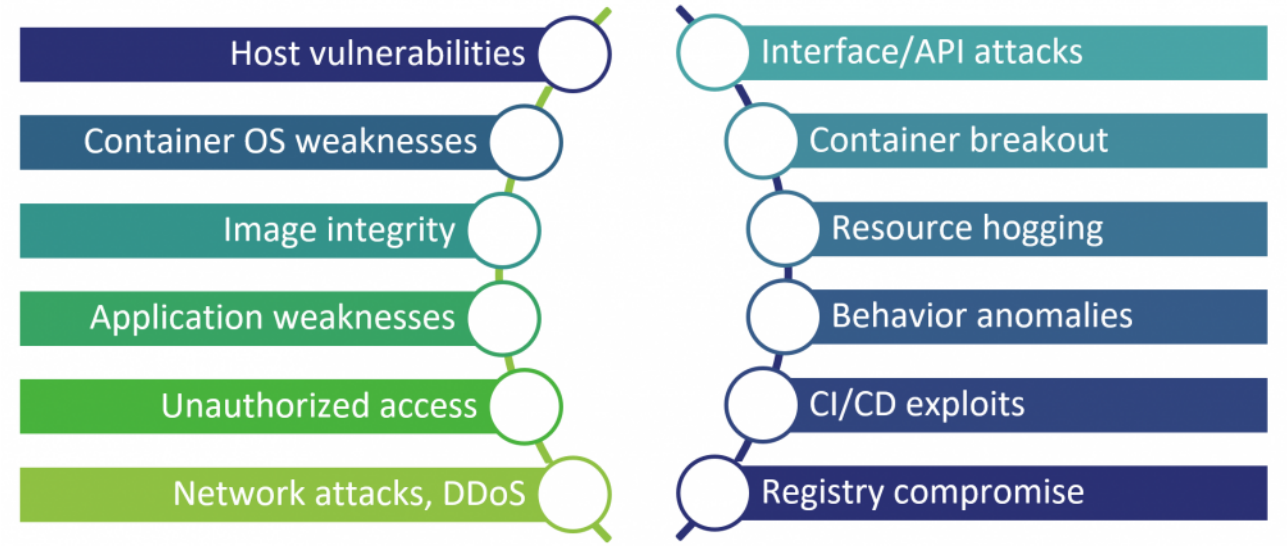


Figure 2: Just some of the risks containers are subjected to

Thus, the primary challenge for vendors creating container security solutions is therefore not coming up with groundbreaking detection or protection technologies, but rather making sure that all these numerous technologies can operate together, fully automated and at the cloud scale, taking into account the ephemeral and stateless nature of containers that differentiates them from traditional endpoints.

Also, whether these solutions are delivered as tightly integrated packages or suites of loosely coupled individual tools, a key success factor for them is the ability to correlate security findings across environments, architectural layers, and, ideally, 3rd party integrations providing additional context for security analysts.

For this Leadership Compass, we are looking for solutions that implement capabilities from one or more of the following functional areas:

- Container image security
- Container registry security
- Orchestration platform security
- Runtime container monitoring
- Threat mitigation and incident management
- Audit and compliance

However, we explicitly exclude traditional security products repurposed or extended to provide additional services for containerized architectures, such as general-purpose vulnerability scanners or network security tools. Also, to avoid potential overlaps with other published or planned Leadership Compasses, we are not addressing such capabilities as API security or tools specifically designed for securing microservices, even though we recognize that such capabilities can be integral to container security platforms as well.

1.3 Delivery Models

The very nature of container-based architectures implies that containers can be found on any platform and in any IT environment - from fully on-prem deployments running on bare-metal hardware to fully managed "serverless" platforms operated by public cloud providers. Various business, technical or regulatory requirements can force organizations to choose different deployment options on a per-project basis, leading to the need to operate, monitor, and secure complex hybrid infrastructures.

Smaller companies that have selected a fully managed serverless container orchestration service from a public cloud provider might have radically different requirements and expertise in their DevOps teams as compared to large enterprises with complex hybrid and multi-cloud application deployments.

Accordingly, cloud security solutions' delivery options might vary from fully managed SaaS offerings already integrated directly into container orchestration services to flexible vendor-agnostic platforms that require substantial deployment efforts to integrate across multiple heterogeneous environments.

However, since modern container security solutions are themselves usually container-based, their deployment can be much quicker and more efficient than traditional on-prem software, which makes the

whole issue somewhat less of a dichotomy than for many other areas of cybersecurity.

Still, companies looking for the solution most appropriate for their container projects should carefully consider both the specific protection, detection, and response capabilities and general aspects like scalability and flexibility, interoperability with existing security tools and third-party solutions, the degree of automation and intelligent decision support, etc.

1.4 Required Capabilities

As mentioned above, the scope of security solutions for containers and container orchestration platforms essentially encompasses nearly every area of cybersecurity - from endpoints (host systems) to network-level and cloud-specific threats to application-level issues - as well as new risks specific to orchestration platforms themselves, as well as container image registries.

Some of these attack surfaces can be already protected with existing security tools utilized by different organizational units - application developers, operations engineers, cloud administrators, IAM specialists, or security analysts - while others are already built into the orchestration services themselves.

Organizations looking to design their own best-of-breed container security solutions from individual components and integrate them into their existing development pipelines and security operations centers should consider the complexity and potential costs of such an approach. On the diagram below one can see just some of the security capabilities that such an architecture should implement, to say nothing about integrating all these functions into a cohesive, unified management and analytics platform.

The other end of the spectrum can be represented by organizations relying solely on basic integrated security controls of cloud-based managed container orchestration services. Some of the solutions offered by large cloud service providers offer quite substantial built-in security functions, which can also be easily extended with 3rd party addons via their marketplaces.

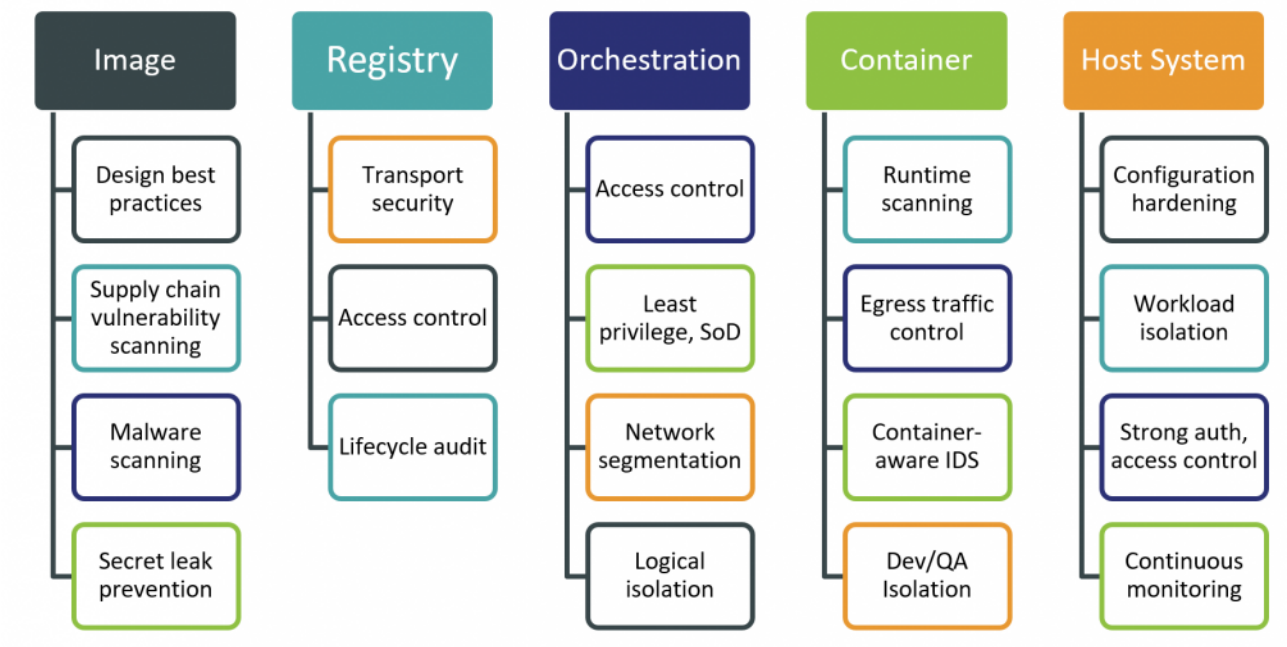


Figure 3: Container security controls

In this Leadership Compass, however, we primarily focus on container security solutions offered by vendors, which can combine prevention, detection, mitigation, and incident response capabilities for each stage of the container lifecycle in a single integrated offering.

Here are the primary functional areas we expect to be provided by such container security platforms.

Container image security: these capabilities integrate directly with existing development environments, helping to ensure that container images start their life according to the modern design best practices. This includes scanning for known or zero-day vulnerabilities in images, preventing them from being infected by malware, not allowing hardcoded credentials to leak into them, etc. The results of container vulnerability scans should be aligned and ranked according to risk assessment models.

Container registry security: providing continuous visibility, access control, and security for container images stored in registries, ensuring that valid images cannot be compromised, and unauthorized access, modifications of images, or infiltration of rogue containers are prevented.

Orchestration platform security: the container orchestration platform itself must be properly secured across all layers of its underlying infrastructure - from securing host systems to implementing network segmentation, workload isolation, and securing all management interfaces. Both proactive hardening and real-time monitoring must be implemented, along with configuration management and comprehensive access governance, enforcing segregation of duties and least privilege principles.

Runtime container monitoring: provides continuous real-time visibility into activities within running containers, utilizing both signature-based detection and ML-powered behavior analytics to identify runtime threats. Container security platforms should utilize the full range of security controls on the host, network,

container, and application levels to block or otherwise mitigate detected threats quickly and automatically.

Incident management: these capabilities allow security analysts to react to identified threats quickly, conduct forensic investigations, reach the right decisions, and, finally, automate threat remediation using a combination of native orchestration controls and specialized security tools.

Audit and compliance: regulatory compliance is a major challenge and simultaneously a business driver for organizations of any size or industry. Security data retention and comprehensive compliance reporting are the basic capabilities here. Out-of-the-box support for regulatory frameworks like GDPR, HIPAA, or PCI is a major differentiator for many customers.

Integrations: container security solutions cannot operate as standalone tools without deep integrations with existing cloud services, container orchestration platforms, DevOps and DevSecOps pipelines, as well as SIEM platforms and other security operations tools. Maintaining an open ecosystem of 3rd party integrations is a key differentiator for vendors.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Compass. The Compass provides a comparison based on standardized criteria and can help identify vendors that shall be evaluated further. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of a pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market

2.1 Overall Leadership

The Overall Leadership rating provides a consolidated view of all-around functionality, innovation, market presence, and financial position. However, these vendors may differ significantly from each other in terms of product features, platform support, and integrations. Therefore, we strongly recommend looking at all the leadership categories as well as each entry in chapter 5 to get a comprehensive understanding of the players in this market and what use cases they support best.

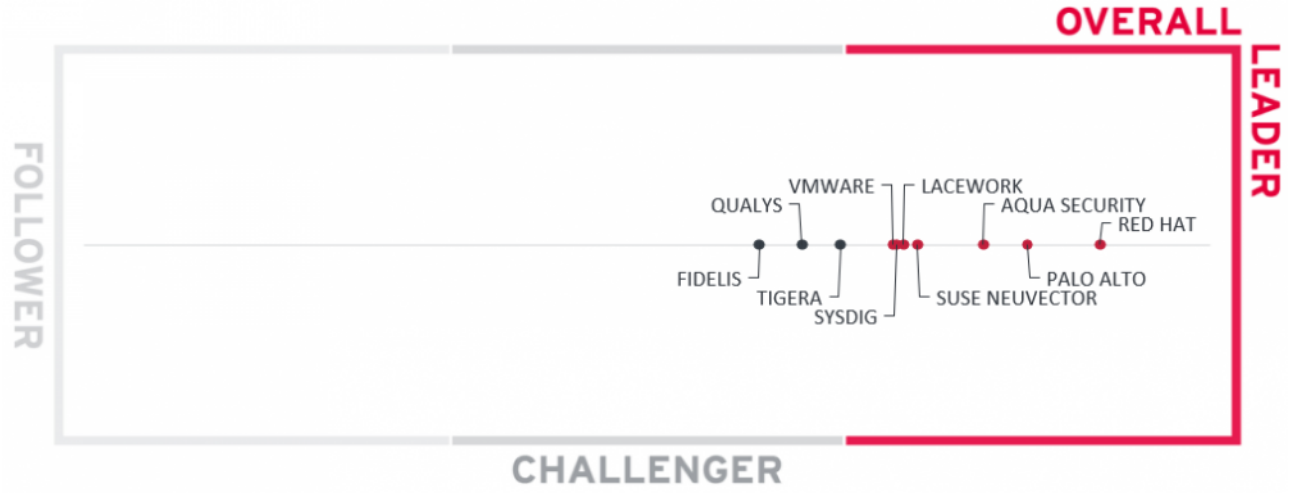


Figure 4: The Overall Leaders in the Container Security market

Seven vendors have reached the status of Overall Leader in our rating.

Red Hat is a veteran vendor of enterprise open-source solutions, including OpenShift, a leading enterprise-grade container orchestration platform. With a massive market presence and proven expertise in container management, enhanced by the recent acquisition and integration of StackRox, a leading container security company, Red Hat is recognized as the Overall Leader in this Leadership Compass.

Palo Alto Networks is a multi-national cybersecurity company, a leading provider of both traditional network security tools and modern cloud-native security solutions. With Prisma Cloud, the company's flagship platform for securing infrastructure, applications, and data in multi-cloud environments, Palo Alto Networks delivers comprehensive security capabilities for cloud-based container orchestration services.

Aqua Security is one of the pioneers among the dedicated container security solution providers. Since 2015, it has been focusing on developing a full-stack cloud workload protection platform that covers the full lifecycle of containers, as well as serverless computing services and even traditional virtual machines.

SUSE NeuVector was previously another pureplay container security vendor, focusing on combining network security and virtualization infrastructure protection to deliver a highly automated security platform for DevOps teams. It is now part of the broader SUSE Rancher product line, providing a complete cloud-native orchestration stack with security being built-in to multiple layers.

Lacework is a cloud security solution provider developing the Lacework Polygraph Data Security Platform, a data-driven cloud security architecture designed to ingest massive amounts of cloud telemetry across public cloud and container environments, uncover anomalies, vulnerabilities, and misconfigurations by applying patented machine learning and behavioral analytics.

Sysdig is a cloud and container security vendor with strong open-source roots. One of the pioneers in container-native monitoring, the company currently offers a unified, open platform for monitoring and securing Kubernetes and cloud infrastructures built on open source, combining cloud security posture management, cloud workload protection, cloud infrastructure entitlement management and infrastructure as

code security in one solution.

VMware is an international cloud computing and virtualization company with a broad portfolio of solutions for both running and securing cloud workloads. With the VMware Tanzu product suite, the company now offers a multi-cloud Kubernetes management and observability platform with a broad set of security capabilities. With Carbon Black Cloud Container acquired in the same year along with the acquisition of Octarine, it has added a visibility, security, and compliance solution for the full container lifecycle.

The remaining vendors populate the Challenger segment. Please note that their current positioning does not imply any significant shortcomings in their products' capabilities. Rather, they might still be working on getting a more substantial market presence outside of their home region, or we would expect to see a higher degree in innovation to keep up with the fast-evolving market requirements.

There are no Followers in this rating.

Overall Leaders are (in alphabetical order):

- Aqua Security
- Lacework
- Palo Alto Networks
- Red Hat
- SUSE NeuVector
- Sysdig
- VMware

2.2 Product Leadership

The first of the three specific Leadership ratings is about **Product** leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services. In the Product Leadership rating, we look specifically for the functional strength of the vendors' solutions, regardless of their current ability to grab a substantial market share.

Besides the group of the overall leaders mentioned above, we can observe several other companies among the Product Leaders.

Fidelis Cybersecurity is a provider of proactive cyber defense and defense-in-depth solutions to safeguard modern IT environments. With the recent acquisition of CloudPassage, a well-known provider of cloud security and compliance solutions, Fidelis now offers a unified, automated security platform for all kinds of cloud workloads, including containers.

Tigera is a cloud-native application security vendor known as the creator and maintainer of Calico Open Source, a widely used container networking and security solution. Building on this open-source foundation, the company offers an enterprise-grade commercial Cloud-Native Application Protection Platform that prevents, detects, troubleshoots, and automatically mitigates risks of security issues for containers and Kubernetes during build, deploy, and runtime.

The only company found in the Challengers segment is Qualys.

There are no Followers in our product rating.

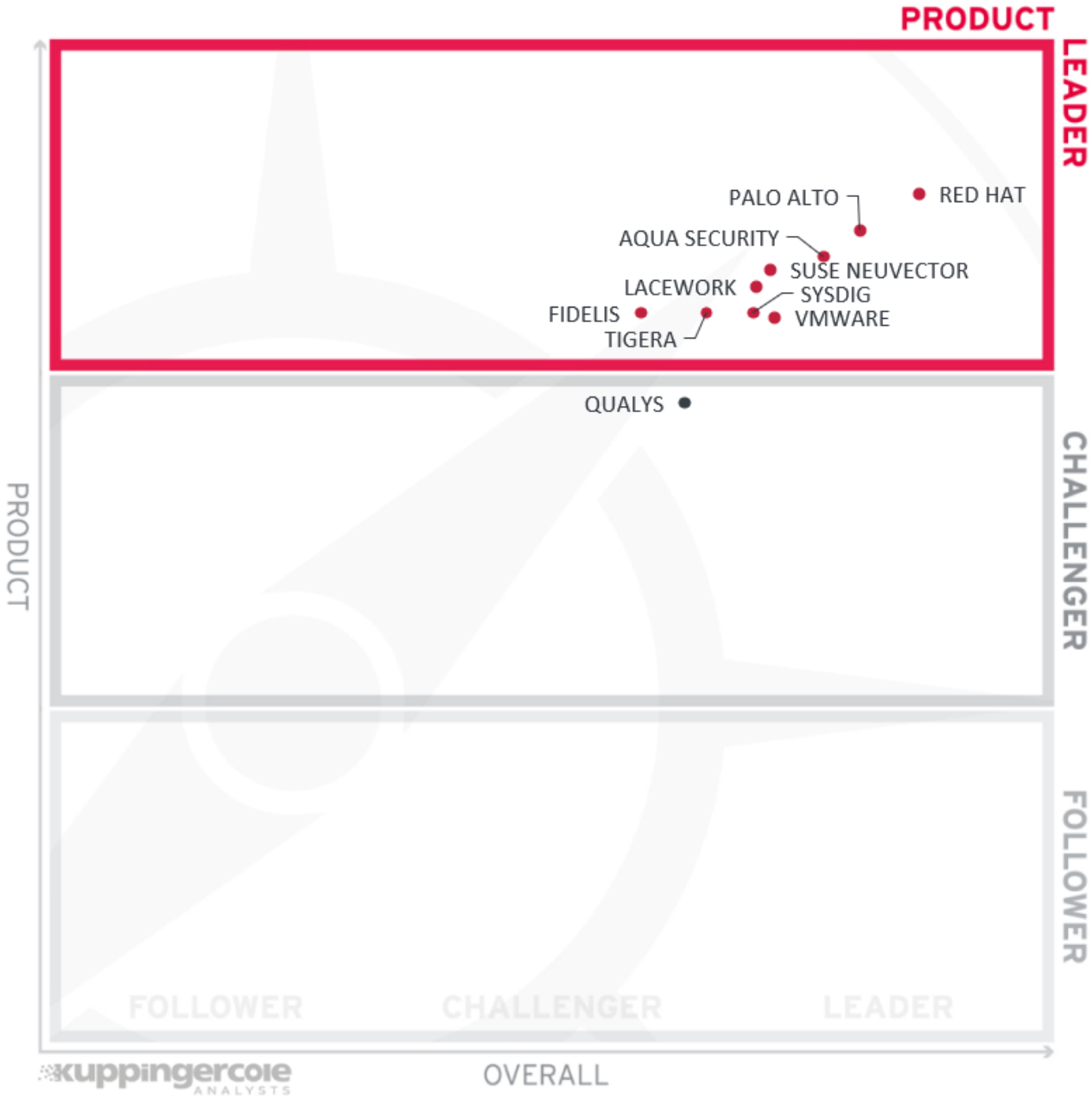


Figure 5: The Product Leaders in the Container Security market

Product Leaders (in alphabetical order):

- Aqua Security
- Fidelis Cybersecurity
- Lacework
- Palo Alto Networks

- Red Hat
- SUSE NeuVector
- Sysdig
- Tigera
- VMware

2.3 Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements.

Innovation is not limited to delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

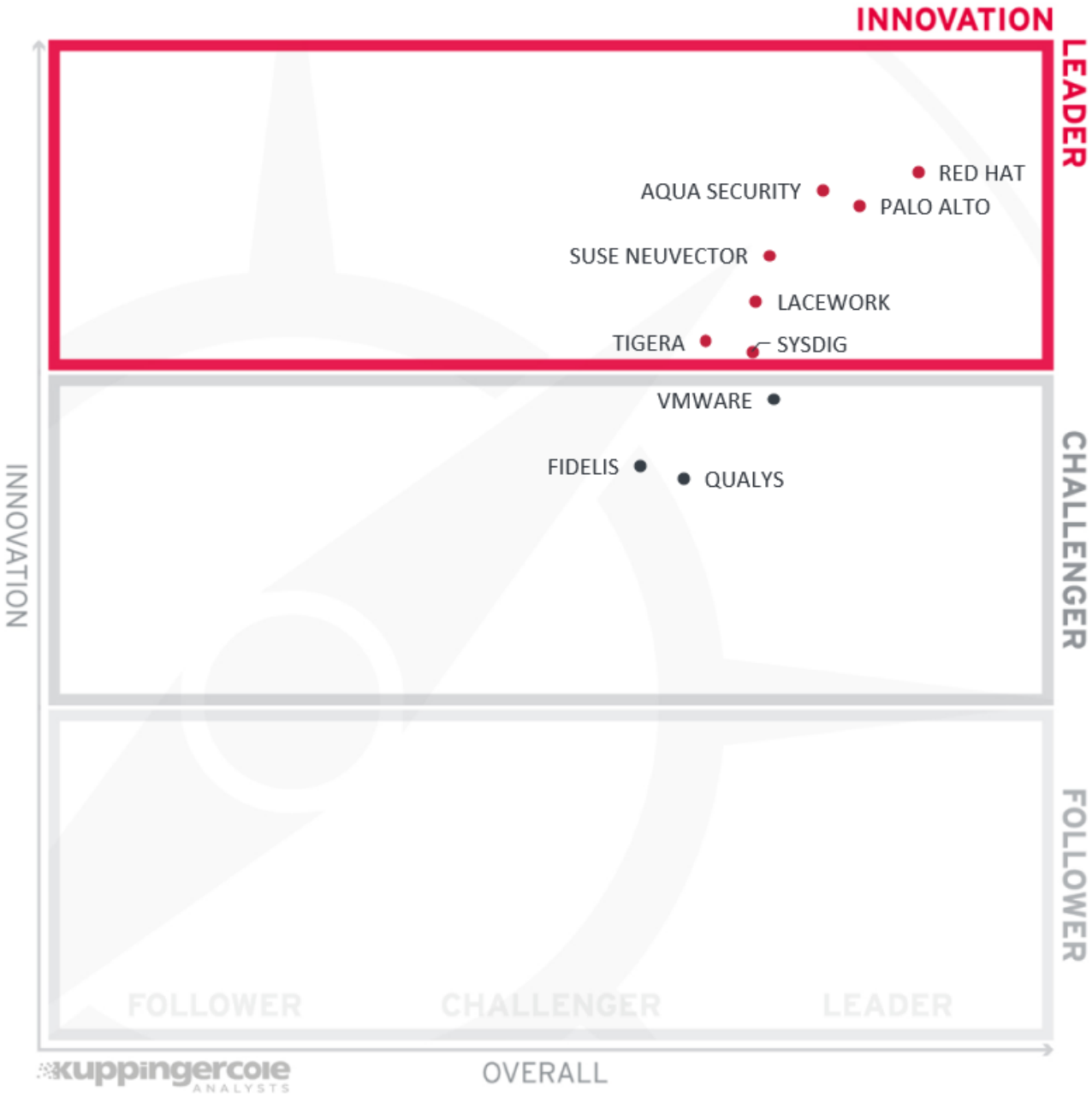


Figure 6: The Innovation Leaders in the Container Security market

In total, seven vendors have been recognized as Innovation Leaders in our rating, reflecting their continuous commitment to implementing new functionality, expanding the coverage to multiple types of cloud workloads, and offering a fully unified user experience for security analysts.

Unsurprisingly three of these vendors are large companies that we also recognize among overall leaders: they have the expertise and financial strength to focus on strong R&D investments. However, the fact that several smaller vendors with more limited resources were able to join them indicates that the container security market is still far from maturity, and the potential to deliver disruptive innovation is still strong even

for smaller development teams.

The remaining vendors are positioned in the Challengers segment, reflecting perhaps the overall maturity of their products that comes with the downside of a somewhat slower pace of innovation. Again, we have no Followers in this rating.

Innovation Leaders (in alphabetical order):

- Aqua Security
- Lacework
- Palo Alto Networks
- Red Hat
- SUSE NeuVector
- Sysdig
- Tigera

2.4 Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers and their geographic distribution, the size of deployments and services, the size and geography of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

Please note that this rating does not reflect the overall market presence of large vendors but is only limited to the market shares of their respective Container Security products. However, even with this statement in mind, large established vendors had fewer challenges achieving the Market Leader status, indicating their massive presence in related market segments, large global partnership ecosystems, and strong brand recognition.

Smaller vendors and startups, however innovative, often need more time to establish their market position. However, companies like Sysdig and especially Lacework has managed to improve their market reach quickly thanks to their successful business development strategies, growing partner networks and through their strong open-source ecosystems.

The remaining companies can be found in the Challengers segment. We're looking forward to seeing how they will improve in the next release of this Leadership Compass.

There are no Followers in our market leadership rating as well.

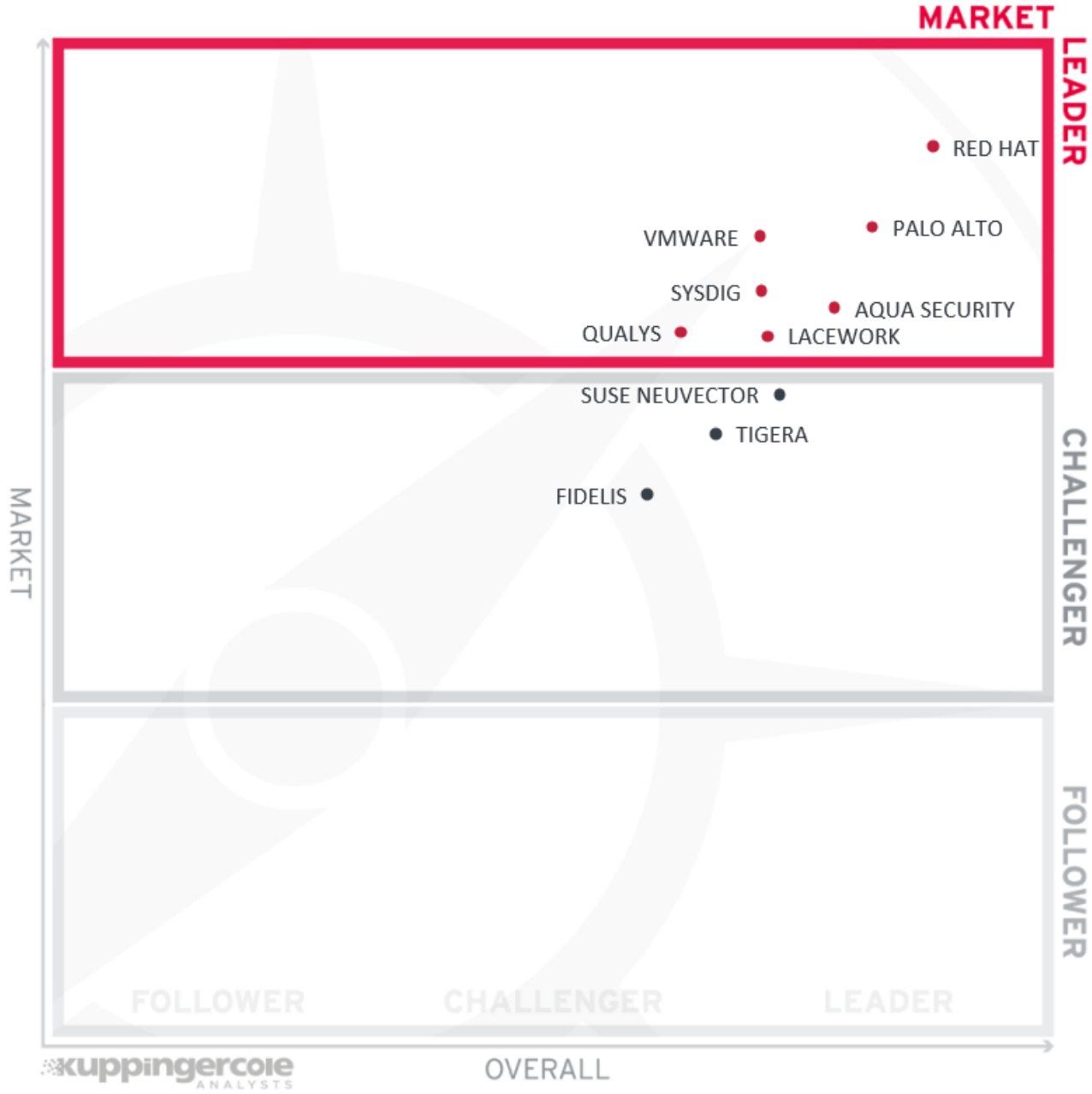


Figure 7: The Market Leaders in the Container Security market

Market Leaders (in alphabetical order):

- Aqua Security
- Lacework
- Palo Alto Networks
- Qualys

- Red Hat
- Sysdig
- VMware

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.

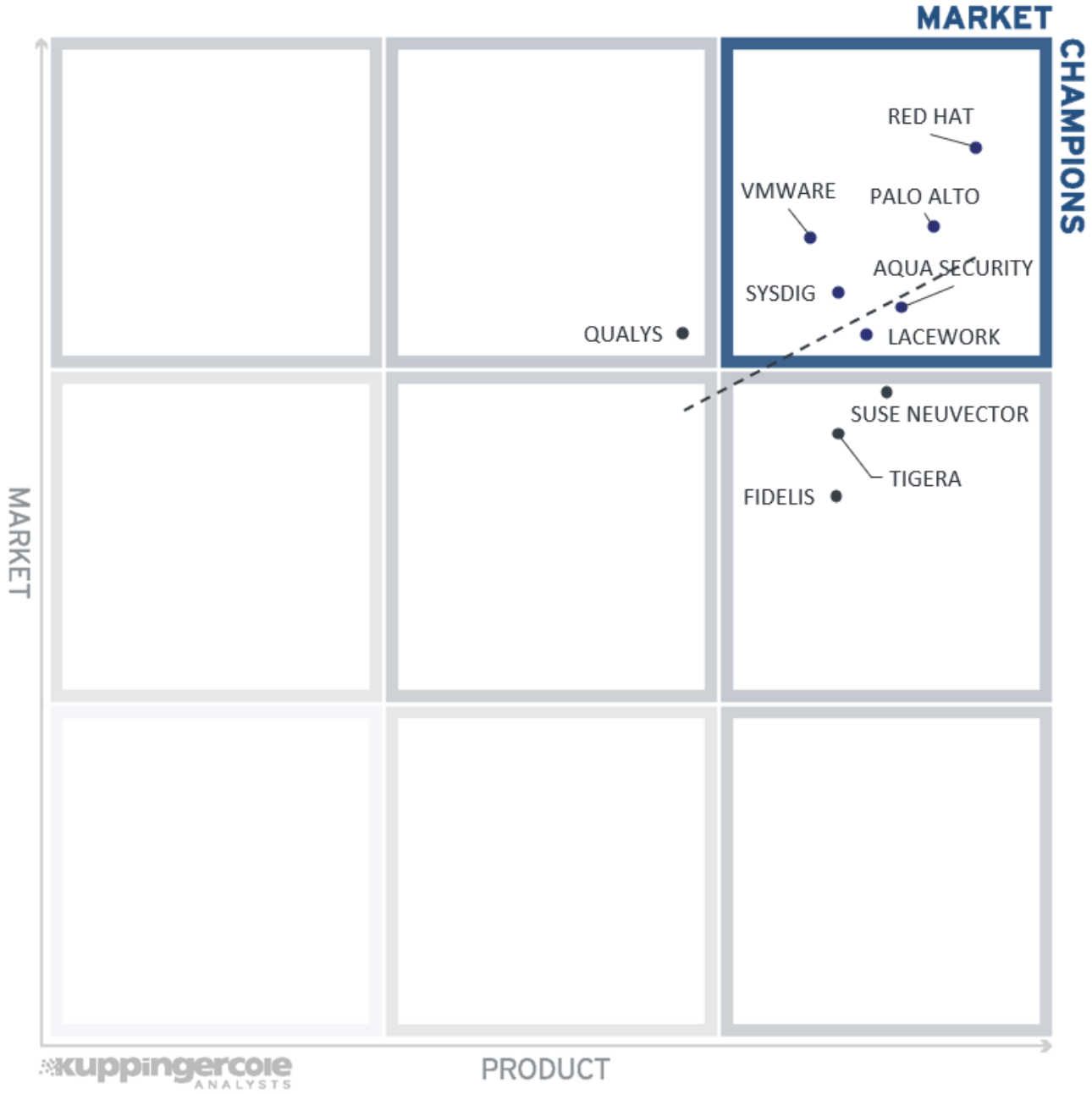


Figure 8: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership. All the vendors below the line are currently underperforming in terms of market share. However, we believe that each has a chance for significant growth.

Among the Market Champions we, unsurprisingly, find large, veteran vendors like Red Hat, Palo Alto Networks, and VMware, as well as Aqua Security, a leading pure-play cloud native security company. Joining them are Sysdig and Lacework, two vendors that have managed to substantially increase their

market presence recently.

The vendors in the right middle box are the companies that have highly rated product offerings but have not yet won the strong market presence they deserve. These include Fidelis Cybersecurity, SUSE NeuVector, and Tigera, who have an opportunity to grow their customer footprint in near future.

The position of Qualys, appearing in the top middle box, indicates that its strong market foothold in traditional security and high brand recognition make it quite successful with its container security offering despite its somewhat lower ratings in several functional areas.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we can see that the overall correlation between the product and innovation ratings is far from perfect, with many vendors appearing away from the dotted line. This is a strong indicator that the market continues to evolve, with different vendors favoring different functional areas and thus making their direct comparison somewhat complicated.

Among the technology leaders, we can again observe the overall leaders - these companies already have mature, fully functional solutions in their portfolio, yet continue to deliver new capabilities at a steady rate of innovation.

Fidelis Cybersecurity and VMware can be found in the top middle box, indicating the overall maturity of their products' functional capabilities that still haven't impressed us enough with unexpected innovative developments.

Qualys is the remaining vendor that can be found in the middle box, showing average results along both rating axes.

Notably, there are no companies in the right middle box, indicating the lack of fresh startups without mature solutions in our rating.

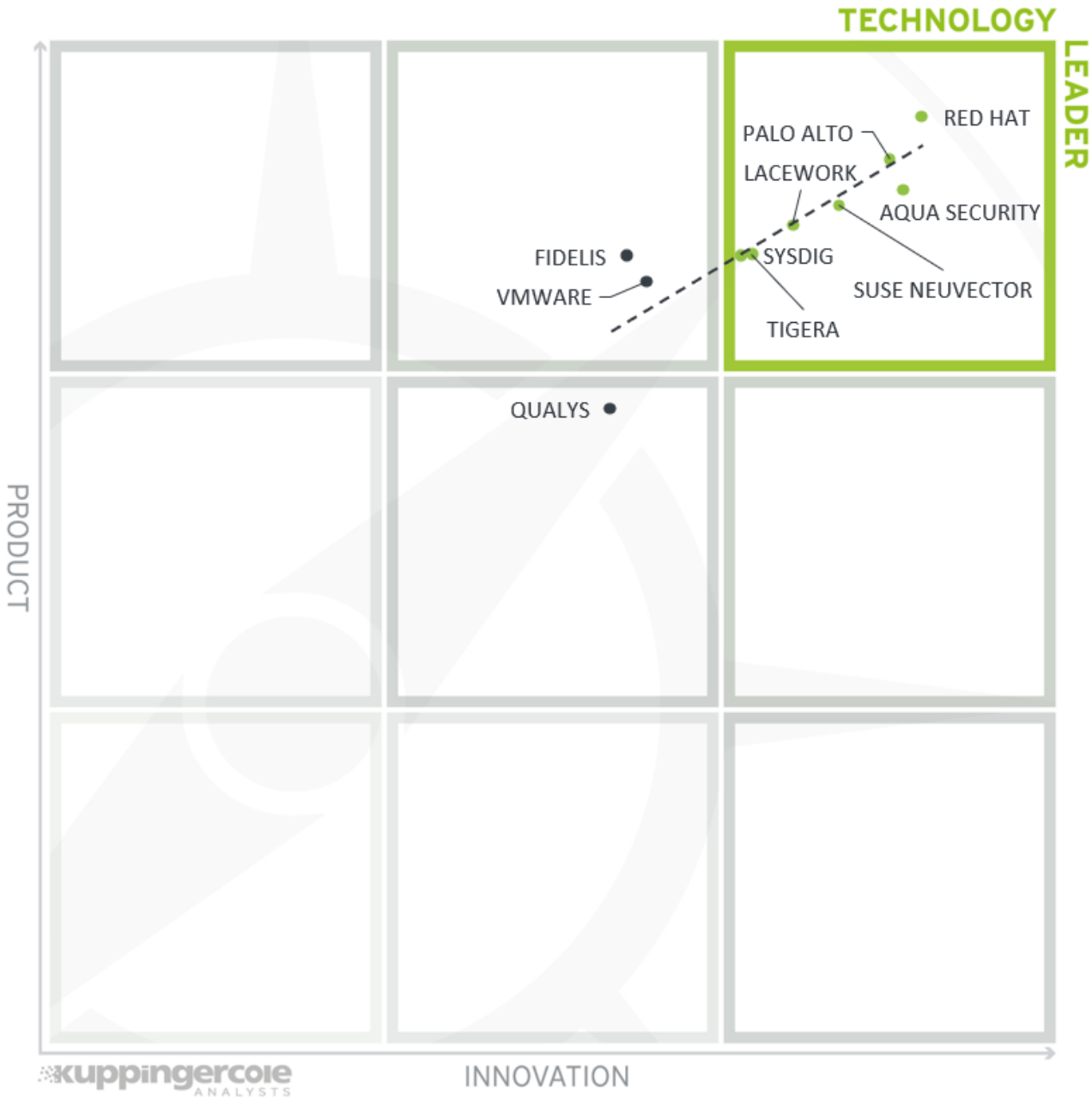


Figure 9: The Product/Innovation Matrix

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position.

On the other hand, highly innovative vendors have a good chance of improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate while having less market share, and thus the biggest potential for improving their market position.

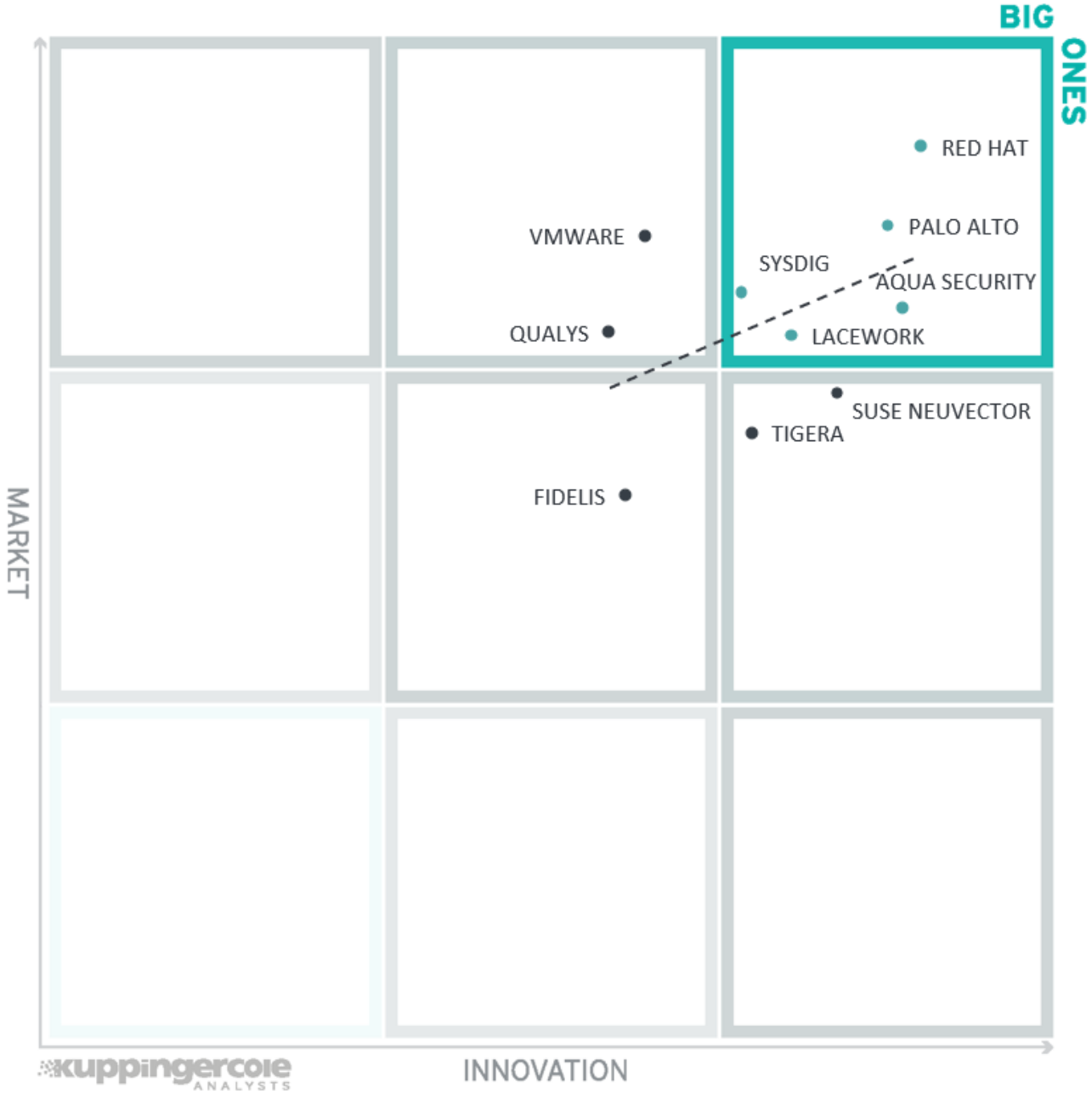


Figure 10: The Innovation/Market Matrix

Unsurprisingly, most of the overall leaders can be found among the Big Ones, indicating both their strong market presence and investments into R&D that ensure staying on top of the market trends in terms of

innovation.

The positioning of VMware and Qualys in the top middle box shows that, perhaps, they do not consider container security their strategic focus and thus do not invest enough in innovation to match their substantial market presence. On the other hand, Tigera and SUSE NeuVector are occupying the right middle box, showing that they need more time to persuade the market with their highly innovative developments.

Fidelis is the only company remaining the middle box, indicating average results that leave some headroom for future improvements.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other.

These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Product	Security	Functionality	Interoperability	Usability	Deployment
Aqua Security	●	●	○	●	●
Fidelis Cybersecurity	●	○	●	○	○
Lacework	○	○	○	●	●
Palo Alto Networks	●	●	●	●	○
Qualys	○	○	○	○	●
Red Hat	○	●	●	○	○
SUSE NeuVector	○	●	●	●	○
Sysdig	○	●	○	●	●
Tigera	○	○	●	●	●
VMware	○	●	●	○	○
Legend		● critical	● weak	● neutral	○ positive	● strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, in Table 2 we provide an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Aqua Security	●	●	●	●
Fidelis Cybersecurity	●	●	●	●
Lacework	●	●	●	●
Palo Alto Networks	●	●	●	●
Qualys	●	●	●	●
Red Hat	●	●	●	●
SUSE NeuVector	●	●	●	●
Sysdig	●	●	●	●
Tigera	●	●	●	●
VMware	●	●	●	●
Legend	● critical	● weak	● neutral	● positive ● strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For intelligent SIEM platforms, we look at the following categories:

- **Image security** - ensure that container images start their life according to the modern design best practices. This includes scanning for known or zero-day vulnerabilities in images, preventing them from being infected by malware, not allowing hardcoded credentials to leak into them, etc. The results of container vulnerability scans should be aligned and ranked according to risk assessment models.
- **Registry security** - continuous visibility, access control, and security for container images stored in registries, ensuring that valid images cannot be compromised, and unauthorized access, modifications of images, or infiltration of rogue containers are prevented.
- **Network security** - tracking and visualization of traffic flows in container deployments, using behavior analytics and machine learning to identify unnecessary exposure and suspicious patterns, and creating and managing network security policies to contain threats and prevent data leaks.
- **Platform security** - across all layers of its underlying infrastructure, from securing host systems to implementing network segmentation, workload isolation, and securing all management interfaces. Both proactive hardening and real-time monitoring must be implemented, along with configuration management and comprehensive access governance, enforcing segregation of duties and least privilege principles.
- **Runtime monitoring** - continuous real-time visibility into activities within running containers, utilizing both signature-based detection and ML-powered behavior analytics to identify runtime threats. Container security platforms should utilize the full range of security controls on the host, network, container, and application levels to block or otherwise mitigate detected threats quickly and automatically.

- **Incident management** - help security analysts react to identified threats quickly, conduct forensic investigations, reach the right decisions and, finally, automate threat remediation using a combination of native orchestration controls and specialized security tools.
- **Audit and compliance -** regulatory compliance is a major challenge and simultaneously a business driver for organizations of any size or industry. Security data retention and comprehensive compliance reporting are the basic capabilities here. Out-of-the-box support for regulatory frameworks like GDPR, HIPAA, or PCI is a major differentiator for many customers.
- **Performance and Scalability** - security solutions must be able to keep up with the cloud scale and ephemeral nature of container orchestration platforms, adapt to complex, distributed deployments, and, of course, provide native support for cloud and hybrid scenarios.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some products may have gaps in certain areas while being strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations - for example, for powering enterprise-grade security operations centers.

5.1 Aqua Security

Aqua Security is a cloud-native security company headquartered in Ramat Gan, Israel. Founded in 2015, it is one of the pioneers among the dedicated cloud workload security solution providers. With a large market presence around the world and partnerships with all major container orchestration platform operators, Aqua Security is the largest pure-play security player in this market. It is also a maintainer of a large open-source ecosystem with projects like Trivy, a container vulnerability scanner.

Aqua is a complete cloud-native security platform that provides security across the application lifecycle (from development to production), for the whole stack (workloads, infrastructure, hosts, orchestration, and cloud layers), and across containers, virtual machines, and serverless functions.

The platform is designed from the ground up to ensure consistent visibility and protection for cloud workloads from the early development stage, beginning with identifying software supply chain risks in application source code. Vulnerability management and dynamic threat analysis help identify, classify, and analyze both known and unknown vulnerabilities.

Cloud security posture management ensures that the infrastructure is configured for optimal security and compliance, prevents drifts and misconfigurations. Flexible policies help determine the risk posture of images, functions, and hosts, along with acceptance gates along the pipeline based on a wealth of vulnerability, configuration, data, and Kubernetes context parameters. With the recent acquisition of Argon, a supply chain security vendor, the platform now includes controls for securing code development and CI/CD toolchain.

All these capabilities, including the ones obtained from earlier acquisitions, are now integrated into a single control plane with unified policy management across different workload types, as well as common UI, access management, reporting, etc. The Aqua platform is designed for SaaS delivery, but can be run in isolated environments as well, both on-prem and in edge deployments.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

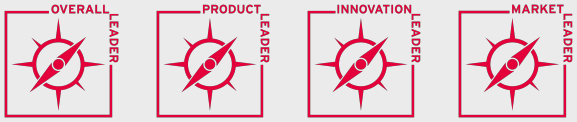
Strengths

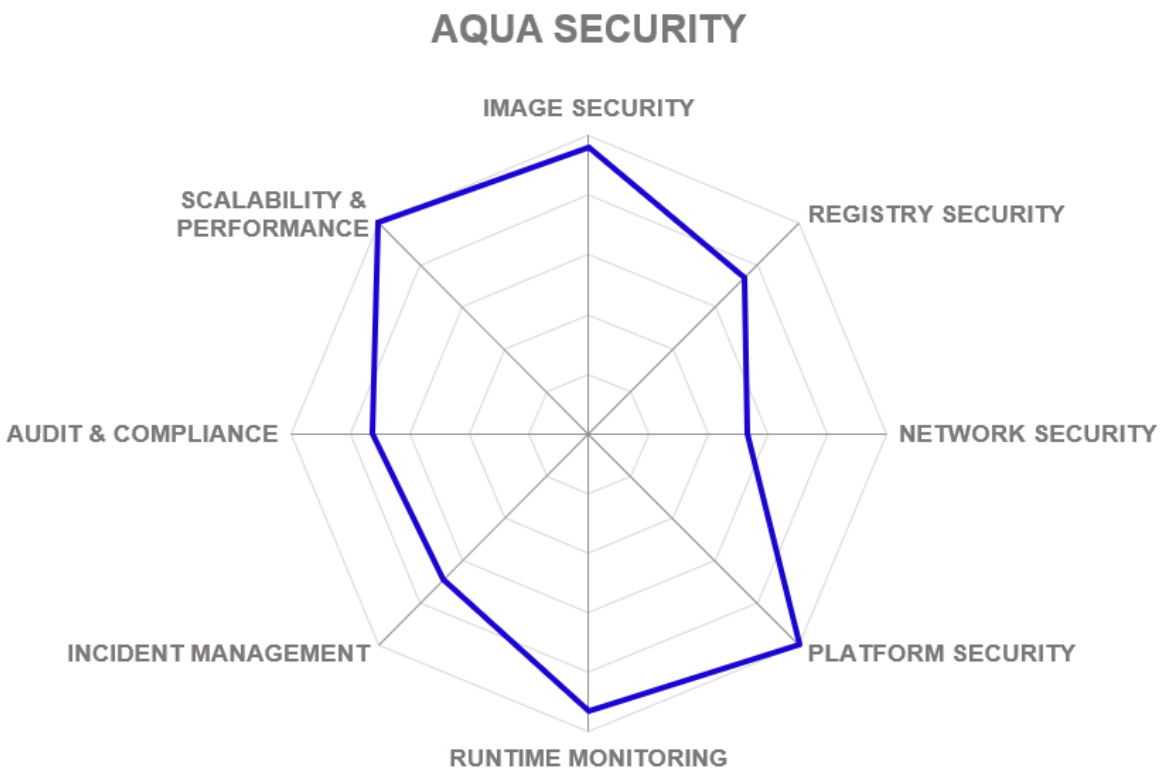
- Fully integrated, unified platform specifically designed for cloud-native workload security (beyond just containers)
- Full coverage for each phase of the workload lifecycle, every layer of infrastructure
- Integrations with major CSPs and orchestration platforms for simplified deployment at scale
- Incorporates “shift left” controls for code, CI/CD, supply chain security
- Single unified management console for all capabilities
- Strong global market presence, large partner network

Challenges

- Network security coverage is limited, no 3rd party integrations
- Does not offer security controls for service meshes
- As a pure-play cloud-native security vendor, additional coverage would require 3rd party integrations

Leader in




AQUA SECURITY
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.2 Fidelis Cybersecurity

Fidelis Cybersecurity is a provider of proactive cyber defense and defense-in-depth solutions to safeguard modern IT environments. Its detection, deception, response, cloud security, and compliance capabilities speed threat detection, hunting, and response across endpoints, networks, and the cloud. The company is based in Bethesda, Maryland, and was founded in 2002. The company's flagship is Fidelis Elevate, an Active XDR platform.

In May 2021, Fidelis Cybersecurity has acquired CloudPassage, a well-known provider of cloud security and compliance solutions, to further enhance its coverage of cloud security. With the CloudPassage Halo® platform, Fidelis now offers a unified, automated security and compliance solution for all kinds of cloud workloads, including containers.

The Fidelis CloudPassage Halo platform unifies security and compliance for servers, containers, and IaaS and PaaS resources across public, private, hybrid, and multi-cloud environments, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. Fidelis Halo's extensive automation capabilities help accelerate workflows between security and DevOps teams.

Out of the box, Fidelis Halo offers over 200 customizable security policies with over 20,000 rules that provide asset inventory and monitoring, vulnerability management, threat management, network security, and compliance management (based on CIS benchmarks). It is offered as a single platform with three services, Fidelis Halo Container Secure, Fidelis Halo Server Secure (CWPP), and Fidelis Halo Cloud Secure (CSPM), running in that platform and sharing data. Each of the Fidelis Halo services can be used on its own or in combination to enable unified visibility and management.

Fidelis Halo Container Secure provides security and compliance automation for containerized applications running on-prem or in any cloud. It validates security for the entire infrastructure stack for containers including registries, pre-production images, run-time environments, rogue containers, and DevOps toolchains.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

Fidelis® Cybersecurity

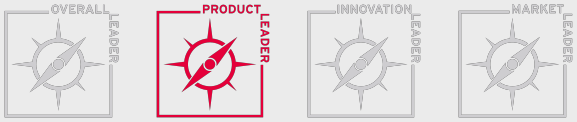
Strengths

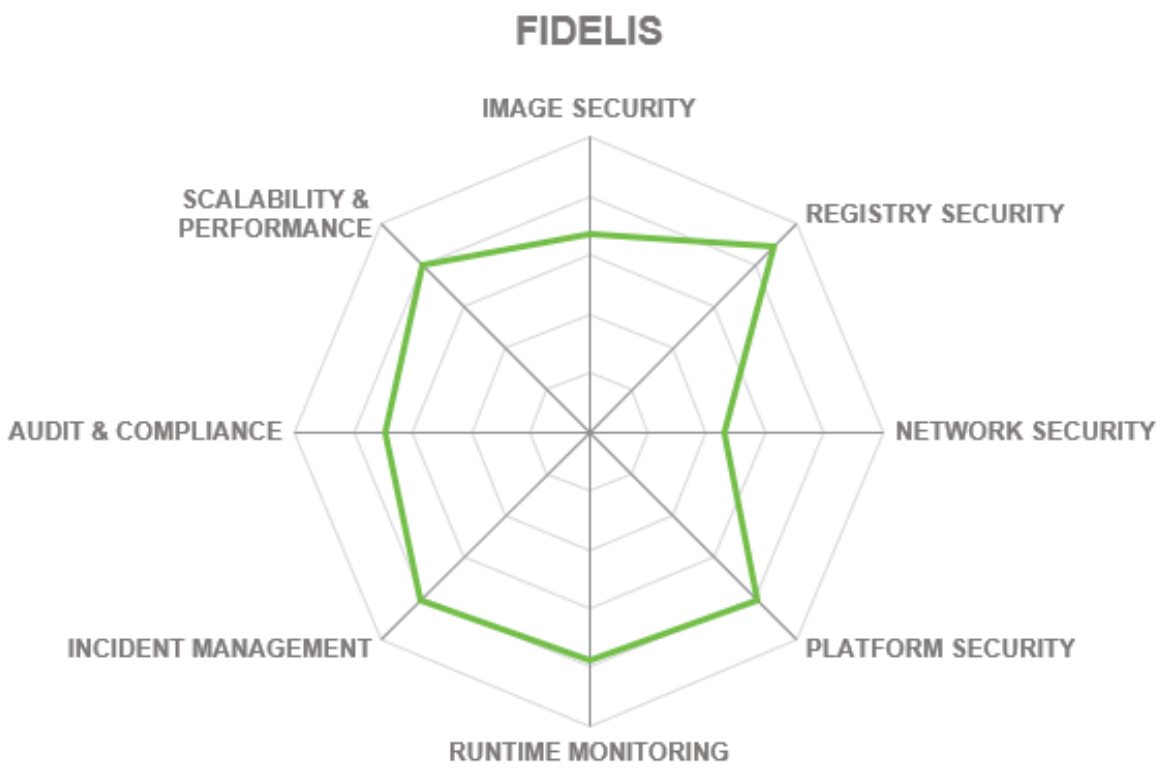
- Single integrated platform combining container security, CWPP, and CSPM services
- Security coverage for each layer of containerized architectures
- Single microagent with minimal resource footprint
- Broad range of integrations with 3rd party security solutions
- Easy portability across hybrid and multi-cloud environments
- Native integrations with all major clouds, deploys in minutes
- Rich out-of-the-box content library simplifies setup and operations

Challenges

- Very small market presence outside of North America
- Control plane cannot be deployed on-premises
- Weak focus on privacy, and data sovereignty - could be a deal-breaker for European customers
- Integration of two security platforms is still work in progress

Leader in




FIDELIS
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.3 Lacework

Lacework is a cloud security solution provider based in San Jose, California. Since 2015, the company developed and brought to market the Lacework Polygraph Data Security Platform, a data-driven cloud security architecture designed to ingest massive amounts of cloud telemetry across public cloud and container environments, uncover anomalies, vulnerabilities, and misconfigurations by applying patented machine learning and behavioral analytics.

The Polygraph Data Platform provides Cloud Workload Protection, Cloud Security Posture Management, Kubernetes Security, Container Security, Compliance, Host intrusion Detection, and Behavioral Analytics Visibility across multicloud environments.

For containerized workloads, the platform provides full visibility and tracking from container image to container instances across a wide variety of infrastructures. This includes build-time Software Vulnerability risks, continuous Runtime Vulnerability risks, infrastructure and network visibility, and runtime behavior tracking.

The Lacework Polygraph machine learning engine automatically learns the activities and behaviors that are unique to container and cloud environments and surfaces unexpected changes, along with full context to make investigations quick and easy. Through the consolidation of multiple tools into a single platform and a 95% reduction in false positives, the platform promises to achieve up to 80% reduction in root cause and investigation times for security analysts.

Dynamically calculated risk scores for each event and artifact related to it provide a consistent method of quantifying container risks and then defining thresholds that would prevent vulnerable or compromised images from deployment to production.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

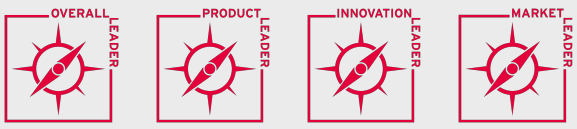
Strengths

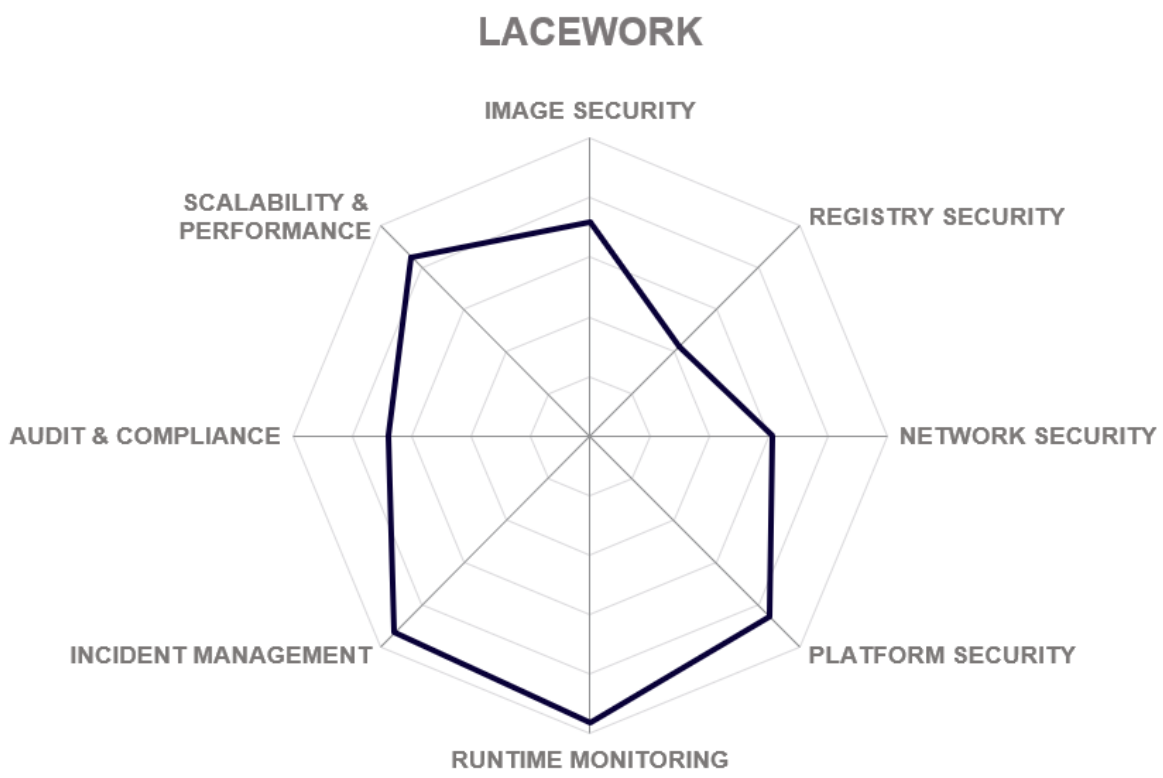
- Fully cloud-native SaaS platform designed for massive scalability and data ingestion
- Multiple deployment scenarios supported, with or without local agents
- Sophisticated automation and machine learning technologies minimize false positives, enrich investigation with context
- Identification of unknown threats without the need to write detection rules
- Very comprehensive incident management capabilities, both internally and through integrations
- Modern, easy-to-use user interface that unifies all capabilities of the solution in a single management console

Challenges

- Focuses more on prevention and detection of threats, remediation capabilities are limited
- By design, only available as a SaaS offering
- Small but growing market presence outside of North America

Leader in




LACEWORK
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.4 Palo Alto Networks

Palo Alto Networks is a multi-national cybersecurity company, a leading provider of both traditional network security tools and modern cloud-native security solutions. Founded in 2005, the company is headquartered in Santa Clara, California. In 2019, the company acquired Twistlock, a well-known provider of container security solutions. Its technology has been integrated into Palo Alto Networks' own Prisma Cloud portfolio.

Prisma Cloud, the company's flagship platform for securing infrastructure, applications, and data in multi-cloud environments provides comprehensive security capabilities for hybrid and multi-cloud environments, including but not limited to containers, virtual machines, serverless functions, web applications, and APIs.

Prisma Cloud is a comprehensive Cloud-Native Security Platform with broad security and compliance coverage - for applications, data, and the entire cloud-native technology stack - throughout the development lifecycle and across multi- and hybrid-cloud environments. From a single dashboard, users can be protecting cloud resources and applications and integrating with CI/CD tooling across all the leading cloud providers and most popular application stacks.

A fully integrated solution, it helps security operations and DevOps teams to stay agile, collaborate effectively, and accelerate cloud-native application development. However, it can be split out into individual products which can be standalone or consumed as a single platform - a flexible, credits-based licensing model allows customers to choose how to consume the capabilities and reallocate the credits between different workloads as the requirements change.

A separate on-premises offering, Prisma Cloud Compute Edition, is available for highly regulated or otherwise sensitive deployments, where there should be no possibility of remote access to the customer's infrastructure or data.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

paloalto® NETWORKS

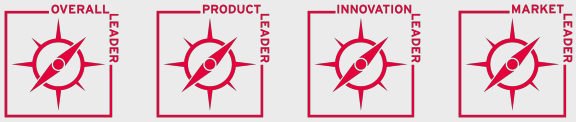
Strengths

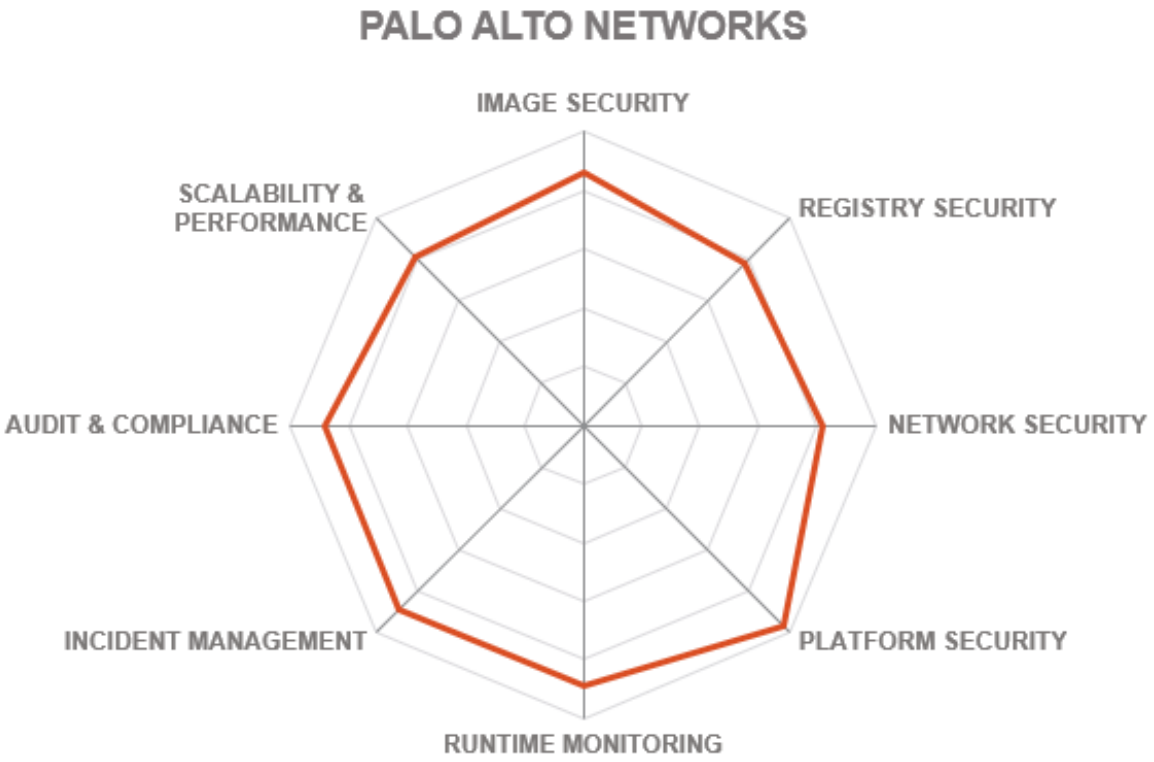
- Single agent, policy engine, console – across multi-cloud, hybrid environments
- Unified cloud security platform helps developers, operations, and security teams collaborate
- Comprehensive support for all types of cloud workloads: VMs, containers, serverless, PaaS
- Extends CWPP by integrating web app and API security capabilities
- Flexible composition and licensing model helps customers choose their priorities and address changing requirements
- Strong market presence and global brand recognition

Challenges

- Solution primarily targeted towards enterprise customers, less suitable for small companies
- No 100% feature parity between SaaS and self-hosted editions of the platform
- Onboarding developers to participate in investigation and response needs more flexibility

Leader in




PALO ALTO NETWORKS
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.5 Qualys

Qualys, Inc. is a vendor of cloud security and compliance solutions founded in 1999 and headquartered in Foster City, California. One of the veteran players in the vulnerability management market, the company was also the first one to offer vulnerability detection using a "software as a service" model. Currently, the company operates the Qualys Cloud Platform, a fully managed universal data management, analytics, and messaging platform that collects security telemetry from sensors across on-premises, endpoints, cloud, containers, and mobile environments around the world.

With this information processed in real-time, Qualys offers their customers continuous, always-on assessment of their IT, security, and compliance posture, with 2-second visibility across all IT assets - with automated, built-in threat prioritization, patching, and other response capabilities. On this shared foundation, the company offers over 20 specialized security solutions, including Qualys Container Security.

Qualys Container Security (CS) extends the Qualys Security Platform to provide visibility, vulnerability, and compliance assessment of customers\' containers and images. It utilizes container sensors to provide comprehensive integrated security across the container lifecycle.

The assessment workflow is performed in real-time when a container launches and covers both source images and running instances. Registry scanning provides complete visibility to the inventory and vulnerability posture of all the images and helps enforce registry hygiene. The platform integrates into customers\' CI/CD pipelines to turn vulnerability assessments into a self-service capability that prevents non-compliant containers from reaching production environments.

By leveraging the Qualys Cloud Platform customers can use the variety of Qualys sensors to gain unique perspectives on their vulnerability and compliance postures to help provide a clearer picture of their attack surface and associated risks beyond just containers.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●

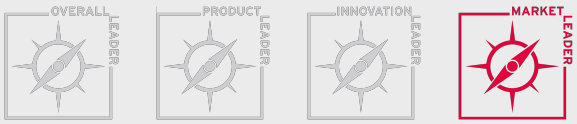
Strengths

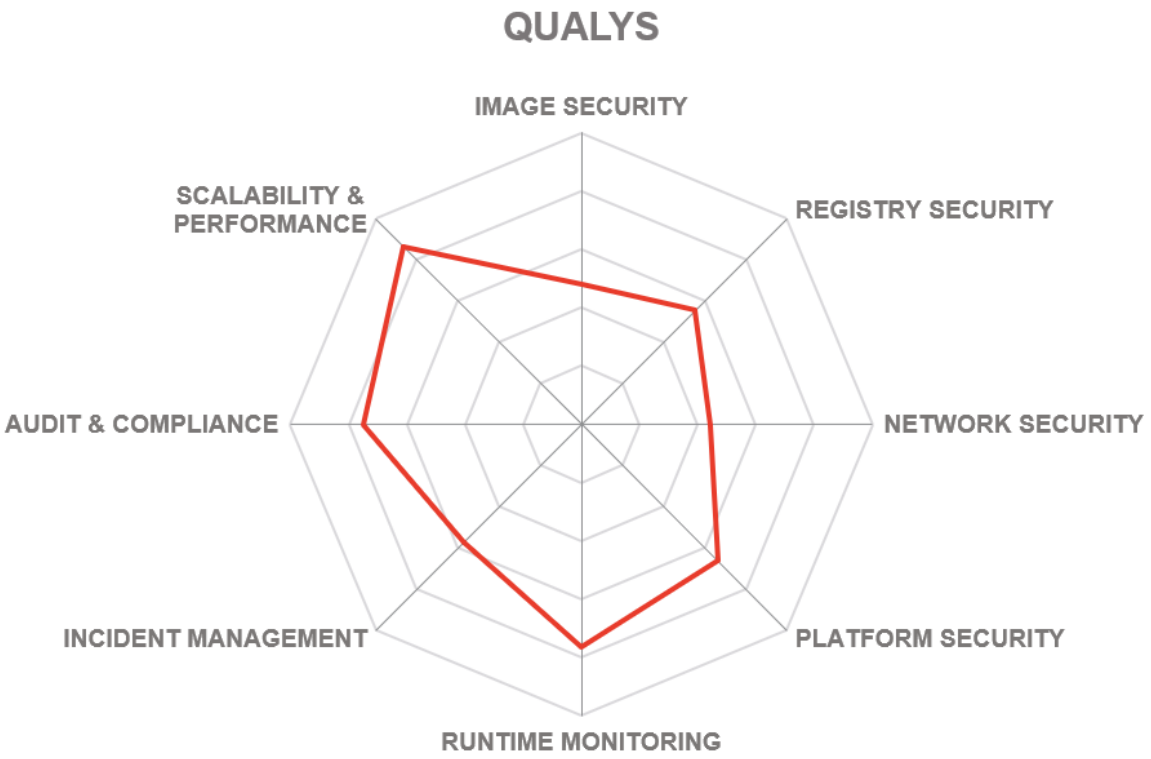
- A global-scale unified cloud-native analytics platform with over 20 security tools tightly integrated
- Coverage for every phase of the DevOps pipeline
- A broad range of sensors suitable for different deployment scenarios and use cases
- Integrations with all notable container management and orchestration platforms
- Private cloud deployment option
- Massive global market presence and brand recognition

Challenges

- Container security controls are less sophisticated compared to other, more specialized vendors
- By design, different cloud workloads are supported in separate modules without shared reporting
- No built-in risk scores for containers, customers must create their own dashboards

Leader in




QUALYS
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.6 Red Hat

Red Hat is a multinational software company that develops enterprise open-source solutions, including cloud, infrastructure, application development, and integration technologies. Founded in 1993, the company is known for its enterprise Linux operating system, as well as for hybrid cloud management, virtualization, and other solutions. In 2019, Red Hat was acquired by IBM and now operates as an independent subsidiary.

Red Hat is a veteran vendor of enterprise open-source solutions, including Red Hat OpenShift, a leading enterprise-grade container orchestration platform. With a massive market presence and proven expertise in container management, enhanced by the recent acquisition and integration of StackRox, a leading container security company, Red Hat is one of the broadly recognized leaders in container orchestration and security markets.

Red Hat OpenShift is a leading enterprise Kubernetes platform with broad adoption around the globe. It provides a comprehensive set of built-in security capabilities for every Kubernetes cluster, so it's secure by default across the entire application lifecycle. For applications that require more complex security, Red Hat OpenShift Platform Plus extends security and compliance across every cluster with even more controls, functions, and policies, including:

- **Red Hat Advanced Cluster Security for Kubernetes** provides native security to enhance infrastructure and workload security through the entire application lifecycle.
- **Red Hat Advanced Cluster Management for Kubernetes** for extended visibility of your entire Kubernetes domain with built-in governance and application life-cycle management capabilities.
- **Red Hat Quay** is a scalable central registry providing a single source of truth of available software with the ability to distribute it efficiently to multiple clusters.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

Red Hat

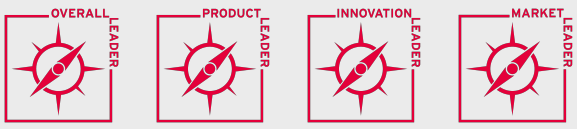
Strengths

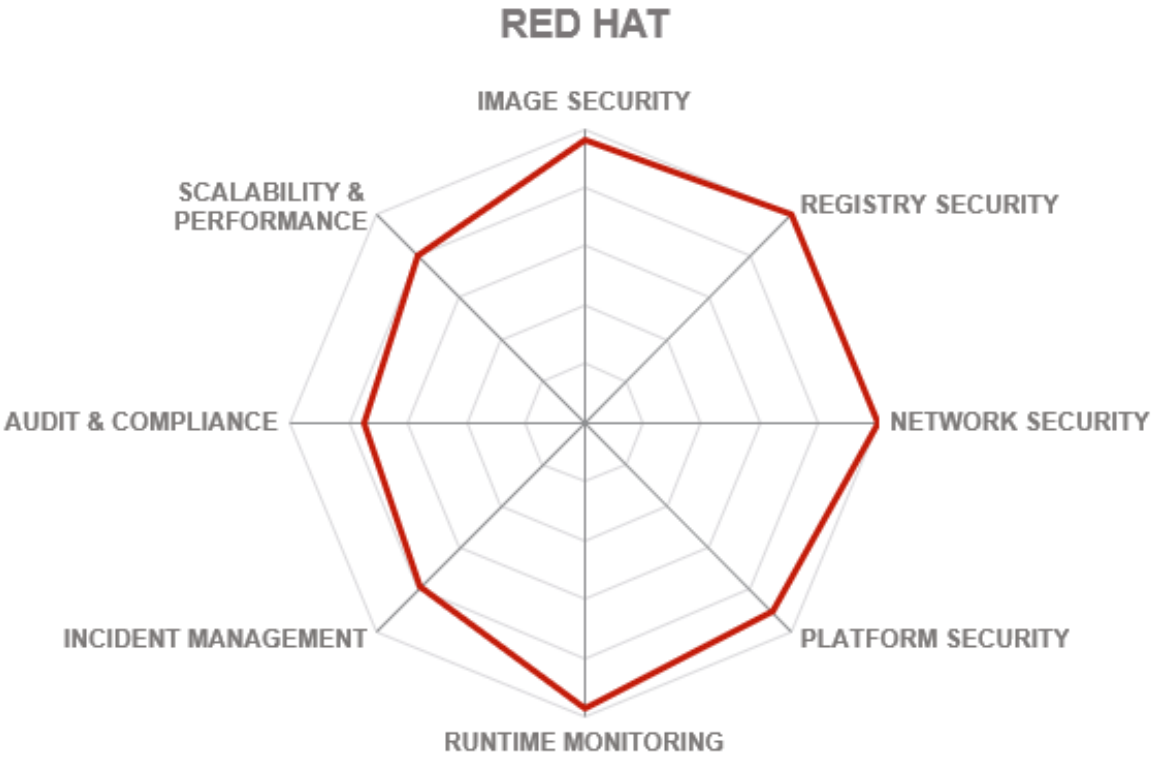
- Full-stack solution for container management and orchestration, from base images to multi-cluster management to advanced security and compliance
- Managed offerings available on each major public cloud
- Multiple secure-by-design features that are enabled by default
- Advanced hybrid and multi-cluster management, security, and image management capabilities
- Massive market presence and brand recognition
- Global partner network and open-source ecosystem

Challenges

- Platform primarily targeted towards enterprise customers, smaller companies might opt for a managed offering
- Full incident management lifecycle depends on integrations with external SIEM/SOAR tools
- Some security capabilities not yet fully integrated, might overlap partially (e.g., registry scanning)

Leader in




RED HAT
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.7 SUSE NeuVector

SUSE is a multinational open-source software company headquartered in Nuremberg, Germany. Founded in 1992, it was the first company to market Linux for enterprise. Its primarily known for SUSE Linux Enterprise and its community counterpart openSUSE Linux distribution. In 2020, the company has acquired Rancher Labs, provider of the Rancher container management platform. In 2021, it has also acquired NeuVector, a container security vendor from San Jose, California. Currently, NeuVector operates as an independent unit within SUSE, but the company has plans to fully integrate it into Rancher.

NeuVector was previously a pureplay security vendor, focusing on combining network security and virtualization infrastructure protection to deliver a highly automated security platform for DevOps teams. It is now part of the broader SUSE Rancher product line, providing a complete cloud-native orchestration stack with security being built-in to multiple layers. The company's continuous container security and compliance platform simplifies data protection, enforces compliance, and provides unparalleled visibility and automated controls to combat known and unknown threats.

NeuVector offers a cloud-native Kubernetes security platform with end-to-end vulnerability management, automated CI/CD pipeline security, and complete run-time security, including a container firewall to block zero-days and other threats. This Layer7 container firewall with DPI and DLP for all container traffic does not rely on eBPF, network CNI/network policy, or IP tables for inspection and enforcement.

The solution can be easily deployed as a container onto virtual machines or bare metal OS environments, native integrations with all notable Kubernetes and container management platforms, and cloud services are supported as well. In fact, the platform's architecture mimics the architecture of container platforms themselves: a single Enforcer container is deployed on each node to protect containers running on it, and a Controller container manages the cluster of Enforcers. The whole platform can be managed through the Console, REST API, or CLI.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

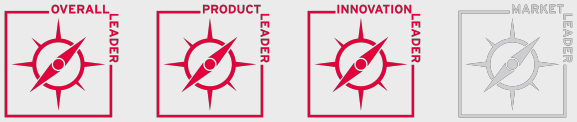
Strengths

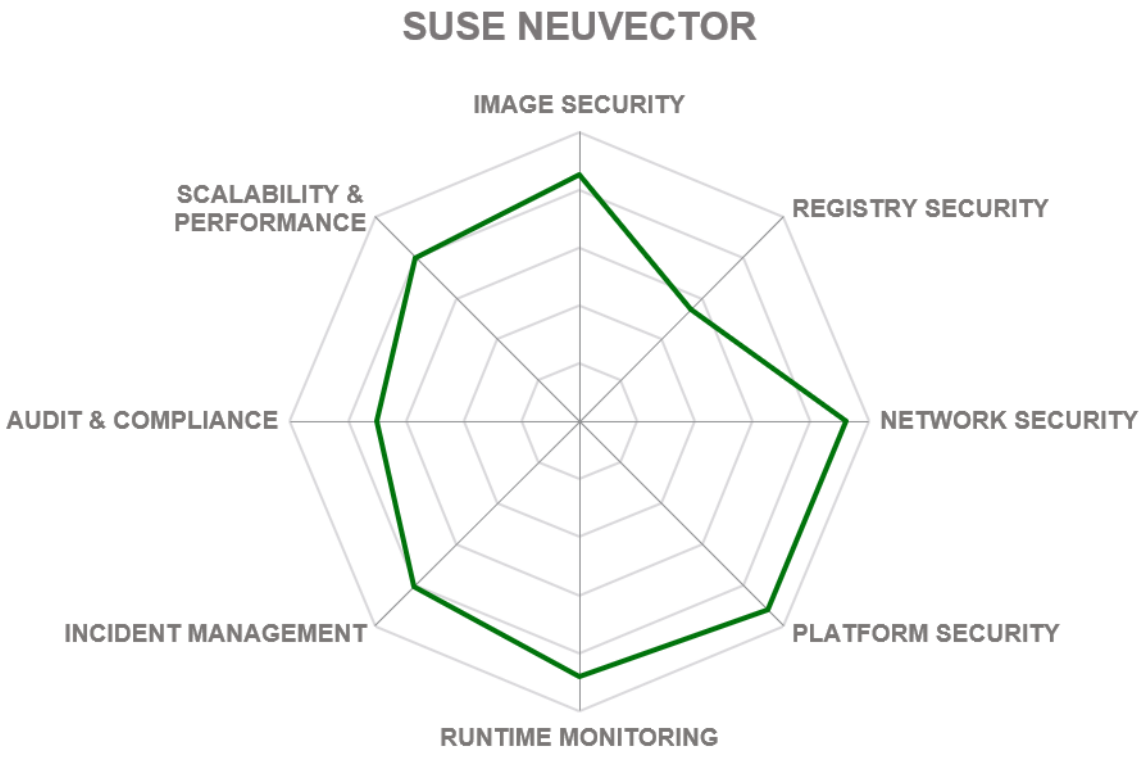
- Unique cloud-native containerized architecture simplifies deployment, improves scalability, does not require agents
- End-to-end container vulnerability management with a broad range of integrations and APIs
- Native integrations with all notable on-prem and cloud orchestration and management platforms
- Built-in firewall for application layer traffic inspection, threat detection, and blocking
- Built-in DLP engine to protect sensitive data from leaks
- Compliance templates for major frameworks like PCI, GDPR, HIPAA, etc.

Challenges

- Not available as a SaaS offering
- Designed only for container security: no support for VMs or serverless
- Registry security controls are somewhat lacking compared to other coverage areas

Leader in




SUSE NEUVECTOR
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.8 Sysdig

Sysdig is a Kubernetes and cloud security vendor based in San Francisco, California. Founded in 2013 by the co-creator of the popular open-source project Wireshark, the company has deep roots within the OSS community and designs its products on an open-source security stack including Prometheus, Falco, Sysdig Inspect, OPA, etc.

The company's flagship product is the Sysdig Platform that combines container, Kubernetes, and cloud observability and security functions in a single universal foundation that turns cloud posture management, vulnerability management, and container visibility into actionable insights for DevOps and security teams. Sysdig Monitor and Sysdig Secure can be licensed separately or together.

Sysdig Secure is a SaaS offering (also available on-prem), built on an open-source stack that includes Falco and Sysdig OSS, popular open-source projects created by Sysdig for runtime threat detection and response. With this platform, teams can find and prioritize vulnerabilities, detect and respond to threats, and manage cloud configurations, permissions and compliance. It covers the full lifecycle of cloud-native apps, from the registry and CI/CD security to runtime monitoring and detection to incident response.

Although the platform is built upon popular OSS tools than can be deployed independently, the enterprise SaaS offering is a popular replacement for such home-grown deployments, offering multiple advantages like quick deployment in every public cloud, unified, convenient UI across cloud infrastructure and containers, policy management at scale, compliance reporting, etc.

Sysdig also partners with large cloud and security vendors like AWS (to provide security for the serverless container service Fargate), Google, Azure, Red Hat, VMware and Oracle, as well as and IBM (which includes Sysdig Secure's technology as a part of its Cloud Pak for Security and also integrated into the IBM Cloud offering).

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

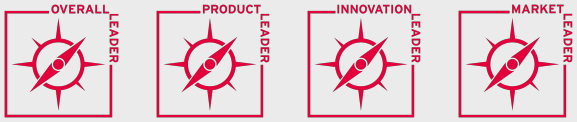
Strengths

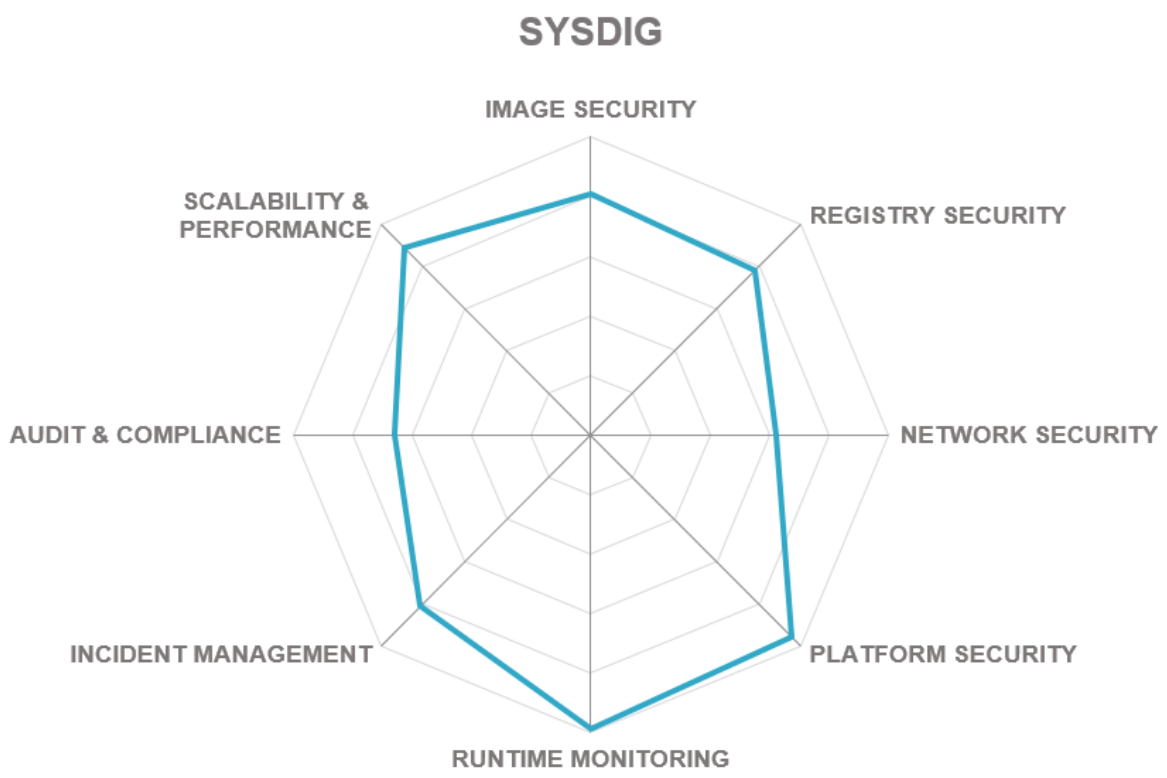
- Unified cloud-native platform that combines monitoring and security capabilities
- Native integrations with all notable container orchestration platforms, in the cloud and on-premises
- Quick and simple deployment into all major public clouds
- Coverage for all phases of container lifecycle
- Single composite UI for the full visibility and analysis of an attack chain
- Strong partner network and open-source ecosystem

Challenges

- Relatively small but growing market presence outside of North America
- Does not offer built-in incident management capabilities
- Network security functions focus on monitoring; enforcement limited to native Kubernetes controls

Leader in




SYSDIG
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.9 Tigera

Tigera is a cloud-native application security vendor headquartered in San Francisco, California. Founded in 2016, the company is the creator and maintainer of Calico Open Source, a widely used container networking and security solution that secures over 2 million Kubernetes nodes across over 160 countries.

Building on this open-source foundation, Tigera offers an enterprise-grade commercial Cloud-Native Application Protection Platform that prevents, detects, troubleshoots, and automatically mitigates risks of security issues for containers and Kubernetes during build, deploy, and runtime. The platform is available both as Calico Enterprise for on-prem and hybrid deployments and as Calico Cloud, a managed SaaS solution.

Regardless of the deployment choice, the Calico platform offers the same level of unified control across multiple clusters, multi-cloud and hybrid deployment for any Kubernetes distribution. The platform provides runtime threat defense by monitoring workloads in real-time and identifying both known malicious attacks and suspicious anomalies in behavior profiles. With deep packet inspection, a built-in web application firewall, and Envoy-based application edge protection, Calico provides intrusion detection and prevention of network attacks.

Policy management and automation capabilities allow developers, DevOps, and security teams to define their own security policies and ensure that they work properly in accord. Every policy change is audited and tested before going into production.

Fine-grained access controls and identity-aware microsegmentation help implement Zero Trust workload security and protect containers and microservices from data exfiltration and other advanced threats.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

TIGERA

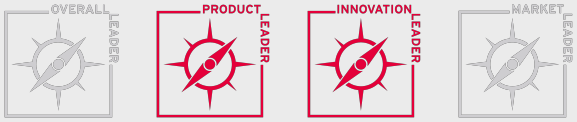
Strengths

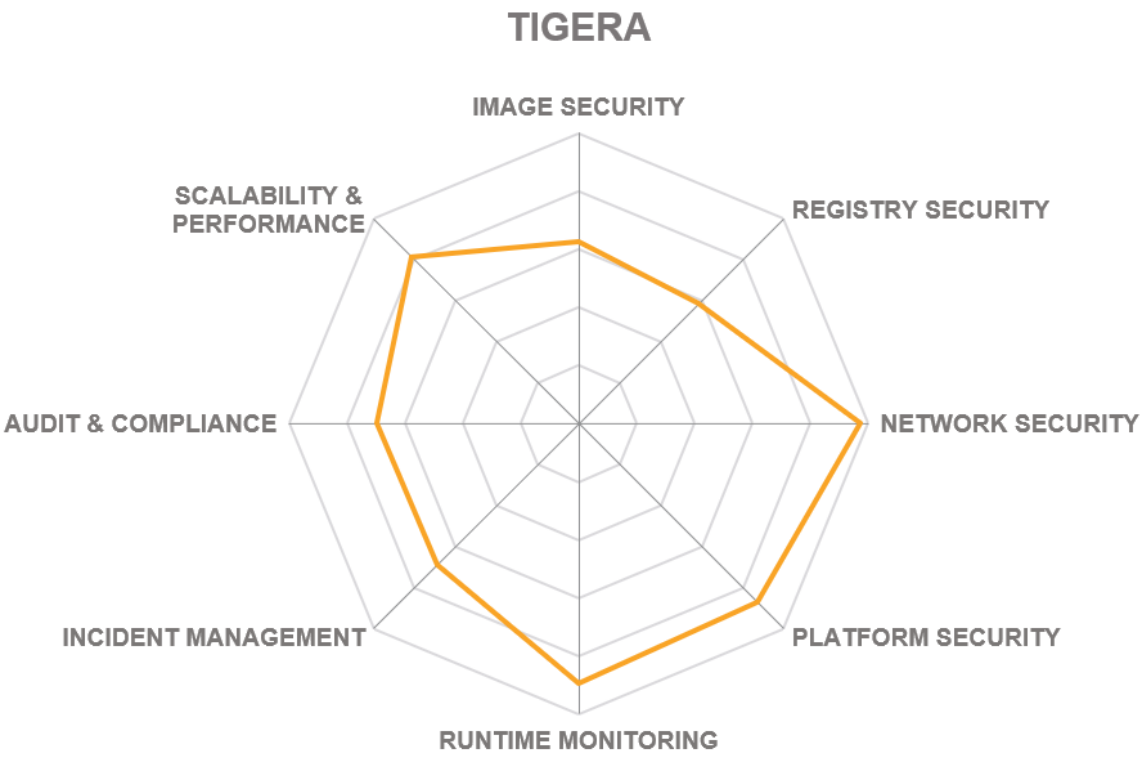
- Full-stack observability and security platform for Kubernetes and cloud-native applications
- Support for any Kubernetes distribution or environment
- Strong focus on application-level microsegmentation and internal traffic flow monitoring
- Comprehensive policy management, staging and auto-recommendations
- Quick and easy deployment: initial setup in minutes, guided tutorials for beginners
- Large global open-source community

Challenges

- Unified visibility across different clusters is not yet complete
- Yet to reach a substantial market presence for the commercial offering despite having massive open-source adoption
- Advanced, more actionable alerting capabilities are still on the roadmap

Leader in




TIGERA
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

5.10 VMware

VMware is an international cloud computing, virtualization, development tool, container application lifecycle, container operational management, container and endpoint security and software defined network, load balancer and API ingress vendor headquartered in Palo Alto, California. Founded in 1998, the company was an early pioneer in hardware virtualization technology. VMware offers a broad portfolio of security tools, including products for both running and securing cloud workloads.

After the acquisition of Pivotal Software in 2019, VMware has added an application development and container lifecycle management and operations platform to its portfolio, expanding its virtualization strategy to containers. With the VMware Tanzu product suite, the company now offers a multi-cloud Kubernetes management and observability platform with a broad set of security capabilities. With Carbon Black Cloud Container (acquired in the same year) along with the acquisition of Octarine, it has added a visibility, security, and compliance solution for the full container lifecycle.

VMware Tanzu enables customers to build, run and manage modern apps on any cloud - and continuously deliver value. It helps simplify multi-cloud operations and free developers to move faster with easy access to the right resources. It enables developers and operations teams to work together in new ways that deliver transformative business results. By combining popular tools and standardized best practices, VMware Tanzu facilitates rapid development of applications that meet pre-approved security controls requirements.

Tanzu Build Service and the Tanzu Application Platform provide a pluggable container vulnerability scanning, secure software build of materials database that is accessible to CI/CD as well as customers, application dependency scanning and signing. Cloud-native buildpacks support building containers directly from source code. With Tanzu Service Mesh, combined with Avi Networks' ingress technology, the security of the running applications can be monitored directly in the API calls. It also provides tracking of PHI/PII and customer-defined protected data and security attack detection and prevention.

Tanzu Observability is a platform for enterprises to deliver observability as a service across all their engineering teams. It is purpose-built for modern apps running on the enterprise multi-cloud at scale. It delivers full-stack observability with advanced analytics on metrics, traces, histograms, and logs gathered on distributed applications, application services, container services, and a multi-cloud based on public, private, and hybrid cloud infrastructures.

VMware Carbon Black Container offers a full range of runtime risk assessment and threat detection for containerized applications, providing image and cluster scanning, network visibility and ingress/egress security, runtime anomaly and configuration drift detection, and actionable alerts for most notable Kubernetes platforms, both on-prem and in the cloud.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

vmware®

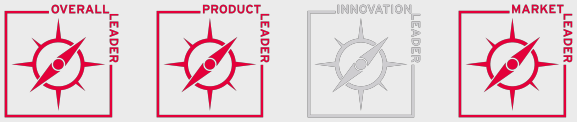
Strengths

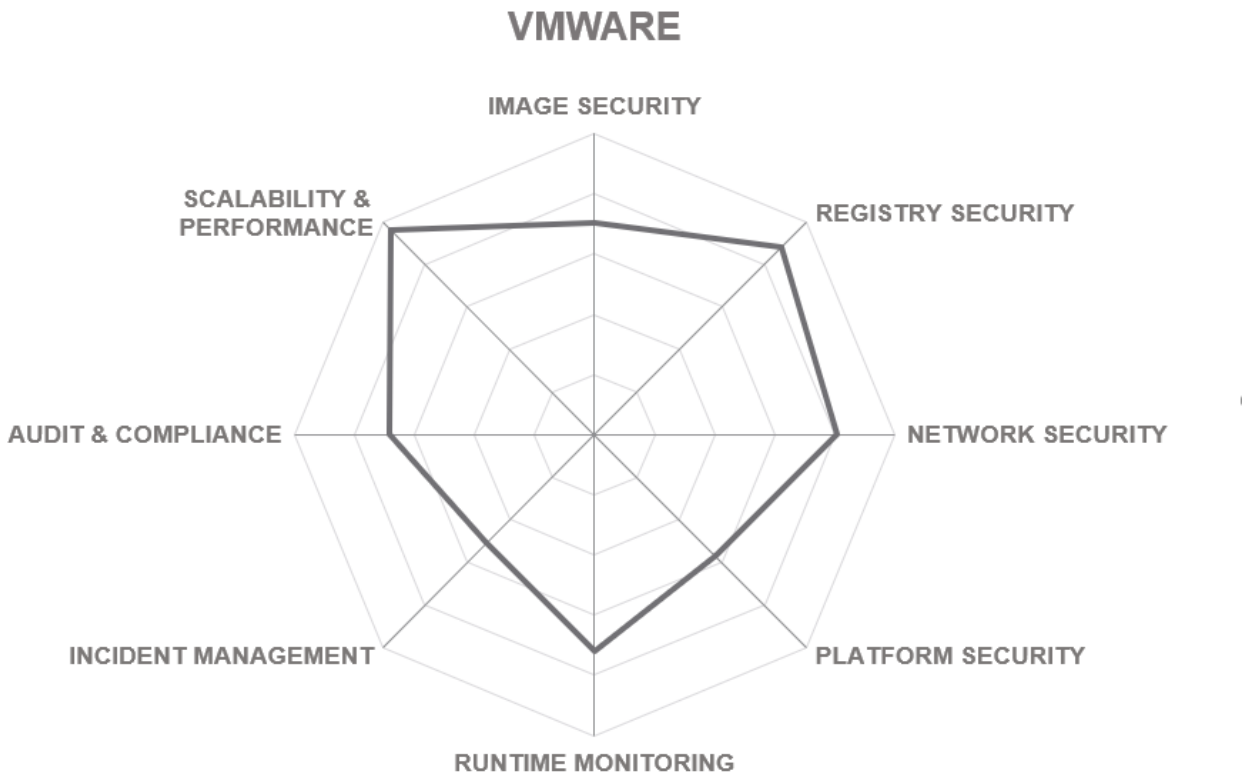
- Strategically unified virtualization platform for VMs and containers to solve the enterprise app modernization challenge
- Common Kubernetes foundation across multiple clouds with centralized policies
- Enterprise-grade scalability for most demanding customers
- Powerful CI/CD automation functions for container developers
- Full visibility into container security posture throughout its lifecycle
- Continuous risk assessment and misconfiguration detection for all notable Kubernetes platforms

Challenges

- Platform primarily targeted towards enterprise customers, small companies might opt for open-source or free tools
- Multiple individual products must be combined for a full-featured solution
- No unified UI across proactive and real-time security capabilities yet (Tanzu vs Carbon Black) due to the strong focus on the API-first approach

Leader in




VMWARE
IMAGE SECURITY
REGISTRY SECURITY
NETWORK SECURITY
PLATFORM SECURITY
RUNTIME MONITORING
INCIDENT MANAGEMENT
AUDIT & COMPLIANCE
SCALABILITY & PERFORMANCE

6 Vendors to Watch

Aside from the vendors covered in detail in our rating, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors that do not fully fit into our definition of the market segment or are not yet mature enough to be considered in this evaluation. We provide short descriptions of these vendors and their respective products below.

6.1 AWS

Amazon Web Services, Inc. (AWS) is a multinational cloud service provider headquartered in Seattle, USA. Launched in 2006 as a subsidiary of the American retail giant Amazon.com, AWS is the first and to this day the largest public cloud service provider in the world. The company offers an ever-growing range of container management and orchestration services, running an estimated 80% of all containerized cloud applications.

Why worth watching: AWS offers a large selection of different container solutions, from a fully managed serverless Fargate service that completely hides the administration (and many security aspects) of container infrastructure from customers to a full-scale Kubernetes service. AWS also provides a number of security controls for the underlying infrastructure, identity and access management, and runtime monitoring. To secure container workloads, customers can choose and deploy third-party solutions directly from the AWS Marketplace.

6.2 Dynatrace

Dynatrace is a software vendor based in Waltham, Massachusetts. Founded in 2005, the company develops a unified software intelligence platform that combines observability, automation, and security for multi-cloud and hybrid applications. With a massive catalog of integrations with major public clouds, development and operations platforms, and open-source frameworks, Dynatrace lets business, DevOps, and security teams collaborate effortlessly on various use cases.

Why worth watching: although Dynatrace does not aim to replace existing security solutions like CSPM, CWPP, or RASP, it complements them all and helps fill the visibility gaps between various components of modern applications, including, but not limited to, all layers of container orchestration platforms.

6.3 Google Cloud

Google LLC is a multinational company specializing in internet-related products and services, known primarily for its search engine, online advertising technologies, and cloud computing services. Launched in 2008, Google Cloud is the company's suite of cloud computing infrastructure services, which also powers Google's own SaaS offerings. It is recognized as one of the leading public cloud service providers.

Why worth watching: Google Cloud is one of the earliest adopters of containerized workloads and the original developer of Kubernetes, released as open-source in 2014. Google Kubernetes Engine (GKE) implements a layered approach to securing Kubernetes clusters and individual workloads, combining authentication and role-based access control, fully managed control plane security, management and patching of cluster nodes, monitoring and limiting unsafe network communications, etc. For workload protection, Google Cloud partners with multiple third-party security vendors.

6.4 IBM Cloud

IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York, USA. With over 100 years of history, IBM has evolved from a computing hardware manufacturer towards offering a broad range of software and services in markets such as business intelligence, data analytics, cloud computing, virtualization, and information security. Since 2014, the company also operates its own public cloud service IBM Cloud. In 2019, IBM has acquired Red Hat, a leading supplier of container orchestration solutions.

Why worth watching: IBM Cloud offers several options for running containerized workloads, including Red Hat OpenShift on IBM Cloud, a fully automated OpenShift deployment, which can transparently extend to on-prem and edge locations. Alternatively, customers might opt for the IBM Cloud Kubernetes Service, a fully managed native orchestration service with built-in AI capabilities from IBM Watson. Both options offer comprehensive security and compliance controls, internally and through native 3rd party integrations. A third option is IBM Cloud Code Engine, which runs on the Kubernetes Service but completely abstracts cluster management from the user, so they focus solely on deploying applications. IBM Cloud Paks, the company\'s intelligent hybrid cloud solutions for various use cases, are also powered by IBM\'s containerized OpenShift infrastructure.

6.5 Illumio

Illumio is a cybersecurity vendor headquartered in Sunnyvale, California. Founded in 2013, it develops solutions for Zero Trust segmentation which help reduce risks of ransomware and other cyberattacks on

endpoints, in data centers, and across multi-cloud and hybrid environments. The Illumio Core platform provides real-time analysis and visualization of application dependencies, identifies vulnerable network paths, and automatically creates microsegmentation policies to prevent attacks exploiting those vulnerabilities.

Why worth watching: Although Illumio's coverage extends way beyond just containers, it provides a full range of segmentation solutions for containerized infrastructures. The Illumio Core platform enables centralized visibility and uniform policy management for various types of cloud workloads not just from the perimeter perspective but from within, and also helps achieve industry-specific compliance requirements quickly.

6.6 Microsoft

Microsoft is a multinational technology company headquartered in Redmond, Washington, USA. Founded in 1975, it has risen to dominate the OS market with MS-DOS and Microsoft Windows. Since then, the company has expanded into desktop and server software, consumer electronics and computer hardware, digital services, and, of course, the cloud. Microsoft is the world\'s largest software company and one of the top corporations by market capitalization.

Why worth watching: Like every other cloud service provider, Microsoft has its own portfolio of managed container and Kubernetes services, as well as a specialized tool for security posture management and threat protection in the cloud - the Microsoft Defender for Cloud. However, Microsoft is the only vendor that can currently offer complete and unified visibility and protection across the big three cloud platforms: Azure, AWS, and GCP.

6.7 Oracle

Oracle Corporation is an American multinational information technology company headquartered in Redwood City, California. Founded back in 1977, the company has a long history of developing database software and technologies. Nowadays, its portfolio incorporates products and services ranging from operating systems and development tools to cloud services and business application suites. Oracle has grown into one of the largest companies in the software industry, as well as a prominent cloud service provider.

Why worth watching: like its competitors, Oracle Cloud offers a managed container orchestration service, Oracle Container Engine for Kubernetes. Unlike them, however, Oracle's is offered as a free solution, which nevertheless comes with a broad range of native security controls taking advantage of the OCI's secure cloud infrastructure and other capabilities like continuous assessment, always-on encryption, and role-based access control.

6.8 Styra

Styra is a cloud-native security vendor based in Redwood City, California. Founded in 2016, the company combines an open-source Open Policy Agent and commercial Declarative Authorization Service solutions to deliver a turn-key solution for mixed teams of developers, operations, and security analysts to protect cloud-native applications from threats, human error, and other risks.

Why worth watching: the popular Open Policy Agent (OPA) project allows numerous users to utilize the policy-as-code approach to define context-based entitlements for modern applications. The same approach can be operationalized to provide decoupled, declarative and centralized management and enforcement of security policies for containers, microservices, API gateways, and any other components of cloud-native apps.

6.9 Tenable

Tenable, Inc is a cybersecurity company based in Columbia, Maryland since 2002. A veteran vendor of vulnerability management solutions, Tenable is known as the creator of the popular vulnerability scanning software Nessus. Nowadays, the company's Cyber Exposure Platform is a universal solution to uncover, research and mitigate weaknesses across the entire attack surface.

Why worth watching: Tenable.io, the company's cloud-based vulnerability management platform, provides full visibility and risk assessment for all kinds of cloud assets and workloads. Tenable.io Container Security is integrated directly into existing DevOps pipelines and delivers full visibility into container images, providing vulnerability assessment, malware detection, and policy enforcement both before and after deployment.

6.10 Weaveworks

Weaveworks Ltd is a cloud technology company based in London, United Kingdom. Founded in 2014, the company is a founding member of the Cloud Native Computing Foundation and the driving force behind GitOps, a set of modern best practices for deploying and managing cloud-native infrastructure and applications. Weaveworks' portfolio helps DevOps teams design, deploy and run Kubernetes clusters at scale.

Why worth watching: although GitOps is technically not a security solution per se, its principles help organizations design and run their Kubernetes infrastructure according to the modern security and

compliance best practices, using entirely declarative definitions and continuous detection of configuration drift and other anomalies to ensure scalable, reliable and secure container operations.

7 Related Research

Leadership Compass: API Management and Security - 80477
Leadership Compass: Network Detection & Response (NDR) - 80489
Leadership Compass: Intelligent SIEM Platforms - 80473
Leadership Compass: Privileged Access Management for DevOps - 80355
Market Compass: Cloud-delivered Security - 80208
Market Compass: Global IaaS Providers Tenant Security Controls - 80337
Whitepaper: Securing your IaaS Cloud - 80933
Advisory Note: Protect Your Cloud Against Hacks and Industrial Espionage - 72570
Advisory Note: Security Organization Governance and the Cloud - 72564
Advisory Note: Cloud Services and Security - 72561
Leadership Brief: Responding to Cyber Incidents - 80209
Leadership Brief: Incident Response Management - 80344
Master Class: Incident Response Management
Analyst Chat: How the Cybersecurity Market Is Evolving

Methodology

About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- **Security
- Functionality
- Deployment
- Interoperability
- Usability**

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive
Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.