Market Share

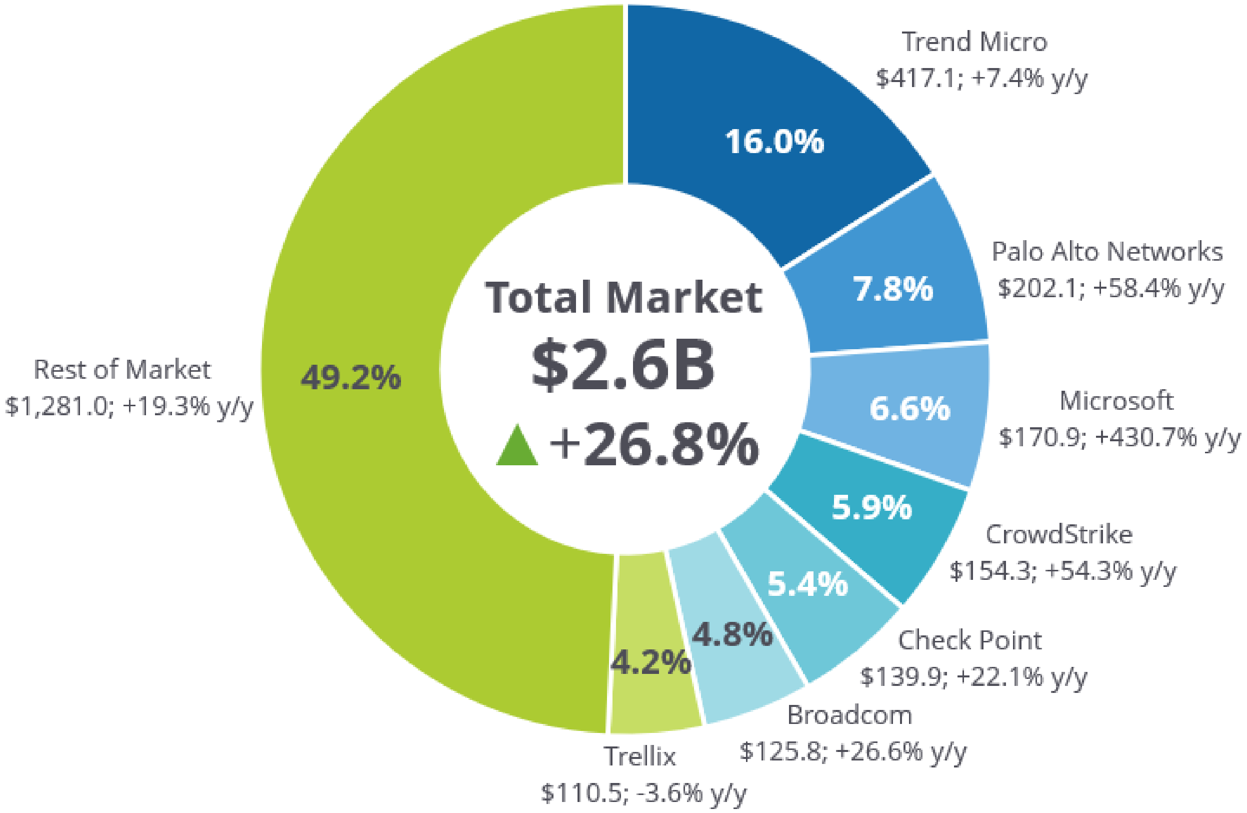
Worldwide Cloud Workload Security Market Shares, 2022: A Shifting Landscape

Ed Lee Philip Bues Frank Dickson

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Cloud Workload Security 2022 Share Snapshot



Note: 2022 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2023

IN THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Cloud Workload Security Market Shares, 2022: A Shifting Landscape (Doc #US50197823). All or parts of the following sections are included in this excerpt: Executive Summary, Advice for Technology Suppliers, Market Share, and Market Context sections that relate specifically to Trend Micro, and any figures and or tables relevant to Trend Micro.

EXECUTIVE SUMMARY

Trend Micro remains the largest player in cloud workload security by far. It saw solid growth in overall revenue, breaking the $400 million mark. While Trend Micro saw a small decrease in market share, its revenue is still more than the second and third larger players combined. Palo Alto Networks, Microsoft, CrowdStrike, and Check Point round out the top 5.

Overall, the market for cloud workload security grew 26.8%. There are numerous drivers fueling this growth:

- The market for cloud continues to grow.
- Containers remain on a fast growth track, with the enterprise container instances installed base growing each year.
- The complexity of protecting cloud workloads increased as applications move from monolithic to microservice and container based, linking hundreds or even thousands of loosely coupled services that are dynamic, ephemeral, and highly distributed.
- Security vendors offered new and innovative approaches to protecting cloud workloads such as leveraging extended Berkeley Packet Filter (eBPF) and block storage for agentless solutions, attack path analysis, and risk prioritization.

This IDC study presents the worldwide cloud workload security market shares for 2022.

"The competitive landscape of cloud workload security is changing as IT titans like Microsoft and Cisco and security innovators like CrowdStrike and Check Point make massive market inroads and impressive share gains. That being said, Trend Micro's position at the top of the market goes unthreatened, exceeding the share of the second and third largest vendors combined. Addressing both security professionals' need for efficacy and resiliency while simultaneously addressing the ease of use and code velocity needs of application developers will determine future market winners." — Ed Lee, research director, Security and Trust at IDC

ADVICE FOR TECHNOLOGY SUPPLIERS

Moving applications from on premises to the cloud changes the requirements for security as applications are always available to the internet. In addition, the rules of the software code protections game are simultaneously changing as applications move from monolithic to microservices based, linking hundreds or even thousands of loosely coupled services that are dynamic, ephemeral, and highly distributed. Many more potential intrusion points now need to be tracked and secured, producing a classic paradox in which security becomes acutely critical and increasingly complex. And so, the classic approach of relying on server agents detecting and responding (e.g., alerting, blocking, removing, isolating, and reverting the endpoint to last known good state) to cyberthreats based on file signatures or analyzing process behaviors is essentially neutered by complexity.

More complexity though is accompanied by richer metadata context, providing different opportunities for anomalous behavior detection. For example, you can identify what kind of network communication or system calls that the application container image can perform, and everything else can be flagged as anomalous and so forth. Taking advantage of the richer metadata context is the trick though, demanding much from cloud security providers as doing it poorly generates noise and a sea of false flags. To reduce the noise of alerts, security vendors should focus on extracting additional value from the richer context and aggregate vulnerability data from multiple sources and focus on prioritized risk assessments and actionable remediations.

Modern application development requires the ability to build security into applications. Rather than the detection and blocking approaches of the past, the focus of security must be executed as an integrated component of the application, addressing a vulnerability or configuration issue natively as part of the application development process while NOT slowing code velocity.

The application registry plays an important role as it creates visibility into what is deployed. Better registries and build tools automate container regeneration, updating base images and layers within images. Further, continuous integration/continuous deployment (CI/CD) software/service release processes ensure that code vulnerabilities and bug fixes are expeditiously deployed. Patching is replaced with container destruction and recreation from a new golden image whenever updates are needed. The frequency of updates can change from twice a year to almost a limitless number of code drops — daily or even hourly.

Ideally, the immutable infrastructure concept would be extended to include operating system (OS) images and Terraform templates. This way developers can guarantee that no extraneous system-level processes are running at the host/virtual machine (VM) level, unnecessarily broadening an app's attack surface. And the criticality of tools integration and automation needs to be noted. Simply stating that our applications are to be managed as immutable infrastructure is far different than the realities required to do so. The difference between the principle and the reality may be the choice of tools and processes.

MARKET SHARE

Trend Micro remains the largest player in cloud workload security by far, breaking the $400 million mark. Although Trend Micro saw a small decrease in its market share, it is still greater than the second and third larger players combined. Palo Alto Networks, Microsoft, CrowdStrike, and Check Point round out the top 5 (see Table 1).

2022 saw a shuffling of the leader board. Moving up in the rankings were Microsoft and CrowdStrike and moving down were Check Point and Trellix. Microsoft saw the largest jump in rankings as the company made a heavy move into the cloud workload security market.

TABLE 1

Worldwide Cloud Workload Security Revenue by Vendor, 2021 and 2022

	2021		2022		
Vendor	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2021–2022 Growth (%)
Trend Micro	388.5	18.9	417.1	16.0	7.4
Palo Alto Networks	127.6	6.2	202.1	7.8	58.4
Microsoft	32.2	1.6	170.9	6.6	430.7
CrowdStrike	100.0	4.9	154.3	5.9	54.3
Check Point	114.6	5.6	139.9	5.4	22.1
Other	1288.2	62.8	1517.3	58.3	17.8
Total	2,051.1	100.0	2,601.6	100.0	26.8

Source: IDC, 2023

WHO SHAPED THE YEAR

Trend Micro

Trend Micro's Cloud One platform secures workloads and applications built in software-defined compute environments across source code repositories, container images, serverless functions, file storage, and workloads.

In November 2022, Trend Micro announced Cloud Sentry, a new offering under the Cloud One platform. Cloud Sentry deploys as a serverless application in a customer's cloud account to scan resources for threats. Only findings are returned to Cloud One Central. Data never leaves a customer's local environment, which upholds data sovereignty and compliance requirements.

Trend Micro continues to perform well each year. For its FY22, the company reported a year-over-year net sales growth of 18% in actual currency. Enterprise subscription-based annual recurring revenue (ARR) increased by 29% year over year along with subscription-based customers, now exceeding 424,000 organizations, which is an increase of 12% YoY. According to the company, leading drivers of the accelerated growth included organizations' need to consolidate tools into a single security platform, data sovereignty driving geographic expansion, and increased dependence on cloud.

MARKET CONTEXT

The shift-left approach to security continues to be adopted by industry. DevSecOps teams play a vital role in bridging the gap between development, security, and operation teams. Part of the benefit of a shift-left approach is to reduce friction by bringing together previously siloed teams and injecting security earlier into the software development life cycle (SDLC). In IDC's 2022 *U.S. Cloud Security Survey,* organizations noted that ease of use, unified hybrid cloud security administration across on premises and multicloud, and supporting vulnerability check at build, deploy, and runtime were the top reasons for choosing a cloud workload security solution.

Kubernetes remains complex, offering a lot of scalability and flexibility, but with an ongoing struggle to find the right expertise to properly configure and manage it. Kubernetes totally changes the rules of the software code protections game as applications move from monolithic to microservices based, linking hundreds or even thousands of loosely coupled services that are dynamic, ephemeral, and highly distributed, often with the support of third-party applications that have their own vulnerabilities and maintenance challenges.

Kubernetes manages critical resources such as containers, network configuration, and secrets, which makes it a high-value target for attackers. Kubernetes security is important due to the variety of threats facing clusters, containers, and code, including malicious actors, malware running inside containers, broken container images, and compromised or rogue users. Without proper controls, a malicious actor who breaches an application could take control of the host or the entire cluster, exfiltrate customer or company data, consume resources through cyrptojacking, or run botnets. In addition, a security breach can result in service and operation disruptions, reputational and financial damages, and other serious consequences. Kubernetes security exists to identify and address security and compliance issues to protect against current and future threats. The identification of Kubernetes as a need fueled the growth of early Kubernetes specialists to gain not only traction in securing Kubernetes but also broader cloud security use cases.

Helping fuel the company's growth in 2022, Aqua Security, for example, expanded its global presence with the launch of its Cloud Native Application Protection Platform SaaS service in Singapore, Europe, and Korea. The company boasts success in the public sector; manufacturing industries, such as manufacturing and automotive; and financial services, where it says it represents 2 of the top 3 largest asset management companies in the world, 2 of the top 5 U.S. banks, and 4 of the top 5 banks in Canada.

In February 2022, Aqua added new features to its Cloud Native Application Protection Platform, which included automated continuous asset discovery and inventory that includes related key security information about vulnerabilities, misconfigurations, sensitive data, and malware; cloud workload scanning; and cloud security insights.

In November 2022, Aqua announced its Lightning Enforcer to stop zero-day attacks and shield critical vulnerabilities in production until a patch can be applied. Using extended Berkeley Packet Filter technology, Lightning Enforcer provides total visibility into running workloads and allows security professionals to identify and stop attacks in real time quickly and easily.

Sysdig also demonstrated success by starting with Kubernetes and broadening the approach. Sysdig offers cloud and container security throughout the software development life cycle. The company started out offering cloud-native runtime threat detection and response and later added source security, which involves embedding security into the software development and deployment life cycle. Over the past three years, the company has added vulnerability management, cloud security posture management, IaC security, and cloud infrastructure entitlement management capabilities to its platform.

In February 2022, Sysdig and Synk announced the integration of Sysdig Secure with Snyk Container to cover security from development to operations. Sysdig Secure brings broader DevSecOps agility and flexibility to prioritize vulnerability alerts, while Snyk Container tests and fixes these environments answering customers' demands for more comprehensive solutions.

In June 2022, Sysdig announced Drift Control to detect, prevent, and speed incident response for containers that were modified in production, also known as container drift. Drift Control automatically flags and denies deviations from the trusted original container.

In April 2022, Sysdig introduced Risk Spotlight, which prioritizes and highlights the vulnerabilities in packages in containers that are actually used in runtime — thus greatly reducing the noise created by vulnerabilities, which exist in containers but are not exploitable.

Significant Market Developments

The Growth of Cloud as a Service

Cloud dominates tech spending across infrastructure, platforms, and applications. Globally, the consumption of cloud-based as-a-service (aaS) spending on cloud-related managed and professional services and the investments in hardware and software needed to build cloud environments represented 39% of worldwide IT spending (including infrastructure hardware, software, and IT services but excluding devices and telecom services) in 2022. By 2026, this will expand to 53%. An even more telling point is that a majority of all spending on the submarket of software was via "as a service" in 2022 and will rise to almost two-thirds by 2026.

Organizations struggled with the growing set of economic and geopolitical disruptions in 2022. The results are enterprises are turning their focus to tactical actions that ensure they are achieving the maximum return on past, current, and future cloud investments. In addition, concerns regarding overspending on cloud services are growing, resulting in enterprises beginning to scrutinize and review the cloud security products and services that they are currently purchasing. While more scrutiny will be placed on all expenditures, IDC research shows that cybersecurity is the area most resilient to budget cuts in 2023.

Agent, Agentless, and Infrastructure as Code

Agentless security is a wonderful innovation to address imperfective approaches to application security within organizations. Numerous vendors including Aqua Security, CrowdStrike, Lacework, Microsoft, Orca Security, Palo Alto Networks, Sysdig, Tenable, and Wiz now offer an agentless solution. In IaaS, agentless security leverages block storage to take snapshots of the environment and then analyze the environment based on the snapshot. This approach is often referred to as side scanning. The advantage of the solution is that it does not leverage an agent, so there is a very limited possibility of interference to or impact on the production environment. As a result, cloud operations professionals can get the security telemetry that they need for compliance or other security without raising objections from application developers. Essentially, agentless security mitigates cross-organization conflict resulting from developer objections as cloud operations is essentially examining the environment behind a virtual sealed pane of glass.

The drawback to agentless security is that is agentless; the strength is the weakness. The "snapshot" approach of agentless limits visibility to the frequency of the snapshot. If snapshots are taken every eight hours for example, ephemeral workloads that spin up for minutes or seconds are invisible. In addition, agentless solutions cannot extract activity telemetry like process information, L3/L4 connections activity, memory analysis, or other real-time information. Essentially, you cannot "hear" what is happening behind the virtual pane of glass. Finally, you are very limited in taking action without an agent, so response and remediation actions are limited. A security professional will be limited in the ability to isolate a workload or redeploy a golden image without an agent.

The debate between agent and agentless is ongoing. But the decision to use one or the other or even both will depend on the individual situation/application and should be evaluated on a case-by-case basis. In IDC's 2022 *U.S. Cloud Security Survey* of 400 enterprises, the use of an agent scored highest. The survey found that when organizations were asked about their preference for a cloud workload security solution that utilizes either agent or agentless solution, 45% chose agent, 40% chose the combination of agent and agentless, and only 15% chose agentless.

Infrastructure-as-code scanning was the rage in 2022 for good reason. It strengthens cloud resource configurations in code. IaC tools minimize cloud misconfigurations reaching production environments, discovering infrastructure-as-code misconfigurations, and identifying security issues.

A key driver of the adoption of IaC continues to be the growth of cloud computing in enterprises, the adoption of a DevOps approach, and the automation of infrastructure workflow. Another driving factor is the increasing complexity of modern applications and infrastructure. With the rise of microservices and containers, IT teams struggle to manage sprawling and complex infrastructure environments. IaC tools help automate the deployment and management of these environments. Key benefits include consistent, repeatable infrastructure, agility in spinning up and changing environments, and reductions in the risk of errors and downtime.

Open Cybersecurity Schema Framework

In August 2022, the Open Cybersecurity Schema Framework (OCSF) was launched by AWS and leading partners in the cybersecurity industry. The 18 founding members of the OCSF are AWS, Broadcom, Cloudflare, CrowdStrike, DTEX, IBM Security, IronNet, JupiterOne, Okta, Palo Alto Networks, Rapid7, Salesforce, Securonix, Splunk, Sumo Logic, Tanium, Trend Micro, and Zscaler.

OCSF is a collaborative, open source effort that provides a standard schema for common security events, defines versioning criteria to facilitate schema evolution, and includes a self-governance process for security log producers and consumers.

Increasingly, security threats are driven by sophisticated cybercriminal organizations and nation-states, and the mounting pressure on chief information officers and chief information security officers to report on their digital resiliency is unprecedented. There are related issues such as inflationary pressures and the importance of measured and reported outcomes. This can lead to consolidation and integration and promote deeper visibility of security products and functionality accessible from a single pane of glass. However, in security, nothing's free; these same benefits can pose new challenges as multiple, disparate sources of telemetry are brought together with differing identifiers and data fields.

Normalization of hybrid multicloud security telemetry is needed before any converged data is useful. Institutional learning suggests that if all cloud security protections speak OCSF, there would be no need to normalize or translate data for each connector, which would enable faster threat detection and response. IDC is bullish on OCSF because it is being driven by a growing list of vendors, is an open source project, entails lightweight governance, and is extensible beyond cybersecurity events.

The Russia-Ukraine War

The Russia-Ukraine War has entered its second year and shows no signs of ending anytime in the immediate future. Cyberwarfare has been an integral tactic employed by Russian government-backed attackers against Ukraine. These attackers have engaged in destructive attacks on Ukrainian government, military, and civilian infrastructure. Attack tactics, techniques, and procedures (TTPs) have included multiple wiper malwares, including HermeticWiper, CaddyWiper, and IsaacWiper, which target Windows devices and make a system inoperable by destroying data and hard drive partition information, as well as ICS malware, Industroyer 2, and Pipedream, which are designed to disrupt industrial control systems in critical infrastructure industries.

The war has raised the profile and specter of nation-state attackers, and their targets are likely to spread beyond Ukraine. Security vendors, globally, continue to gather threat intelligence on the latest TTPs so that they can provide the necessary patches, signatures, and fixes.

METHODOLOGY

The purpose of this section is to provide an overview of the methodology employed by IDC's software analysts for collecting, analyzing, and reporting revenue data for the categories defined by the software taxonomy.

IDC's industry analysts have been measuring and forecasting IT markets for more than 40 years, and IDC's software industry analysts have been delivering analysis and prognostications for commercial software markets for more than 25 years.

The market forecast and analysis methodology incorporates information from five different but interrelated sources:

- **Reported and observed trends and financial activity.** This includes reported revenue data for public companies.
- **IDC's software vendor interviews and surveys.** IDC interviews and/or surveys significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area model on more than 1,000 worldwide vendors.

- **IDC's demand-side research.** This includes annual interviews with business users of software solutions and provides a fifth perspective for assessing competitive performance and market dynamics. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in IDC's software studies and pivot tables represents our best estimates based on the previously mentioned data sources as well as reported and observed activity by vendors and the further modeling of data that we believe to be true to fill in any information gaps.

Note: All numbers in this document may not be exact due to rounding.

MARKET DEFINITION

Cloud workload security products protect software-defined compute solutions, which encompass a number of compute abstraction technologies that are implemented at various layers of the system software stack. SDC workload security solutions are not intended to protect the integrity of the SDC infrastructure (hypervisors, control plane/management, and orchestration) but to protect what runs on top of the SDC infrastructure (VMs and containers). SDC technologies are often used in the context of public or private clouds but can also be implemented in noncloud environments, particularly virtualized and/or containerized environments. Workload security solutions are designed to maintain the integrity of SDC servers, providing protection features that include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. These products accomplish their goals by ensuring that the system does not run malicious software that can compromise business applications and data on the servers. Like the other endpoint security submarkets, SDC workload security solutions are a mutually exclusive category with no overlap with other categories such as physical server or antimalware and suites. Workload security solutions provide protection to three categories of software-defined compute environments:

- **Virtual machine software,** also known today as hypervisor software, uses low-level capabilities offered by certain hardware environments or installs a complete hardware emulation layer using software to support multiple operating environments and the related stacks of applications, application development and deployment software, and system infrastructure software. This segmentation is often referred to as server virtualization or partitioning.
- **Containers** are an operating system segmentation technology. They are similar in concept to hypervisors, except they abstract an OS instead of server hardware. Containers rely on segmenting away parts of the operating system. Each application is presented with a pristine virtual copy of the OS, and the application is made to believe that it is the only application installed and running on that OS. An application and its immediate dependencies are packaged into a container file. Optionally, various OS user space tools and libraries may also be included.
- **Cloud system software** represents a tightly bundled combination of server abstraction, orchestration software, and node-level controller software often sold as part of a larger cloud infrastructure platform solution. The compute resource layer represents a combination of virtual machine, container engine, and/or operating system and orchestration software running on a physical server, which is designated as a cloud compute node. The controller software virtualizes groups of compute nodes into a single logical compute resource. Cloud system software also exposes APIs that simplify the scheduling and control of VMs, containers, and bare metal servers running on the node and maintains a database of resource state and policies.

RELATED RESEARCH

- *Which Features/Services Do Companies Look for When Choosing a Primary Cloud Workload Security Supplier?* (IDC #US50523423, March 2023)
- *How Many Cloud Workload Security Providers and Which Independent Software Vendors/Specialized CWS Vendors Do Organizations Rely On?* (IDC #US50523923, March 2023)
- *Shaping the Narrative - Cloud Security Market Assessment, Part 1* (IDC #US50506423, March 2023)
- *Kubernetes Security: K8s Is Both the Problem and the Solution* (IDC #US50223323, February 2023)
- *Worldwide Whole Cloud Forecast, 2022-2026: The Next Stage of the Shift to a Cloud-Centric Technology Industry* (IDC #US49857122, December 2022)
- *Market Analysis Perspective: Worldwide Cloud Workload Security, 2022* (IDC #US49669822, September 2022)
- *IDC TechScape: Worldwide Cloud Security Enabling Technologies, 2022* (IDC #US48849622, February 2022)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com