IDC MarketScape

IDC MarketScape: Worldwide Cloud-Native Application Protection Platform 2025 Vendor Assessment

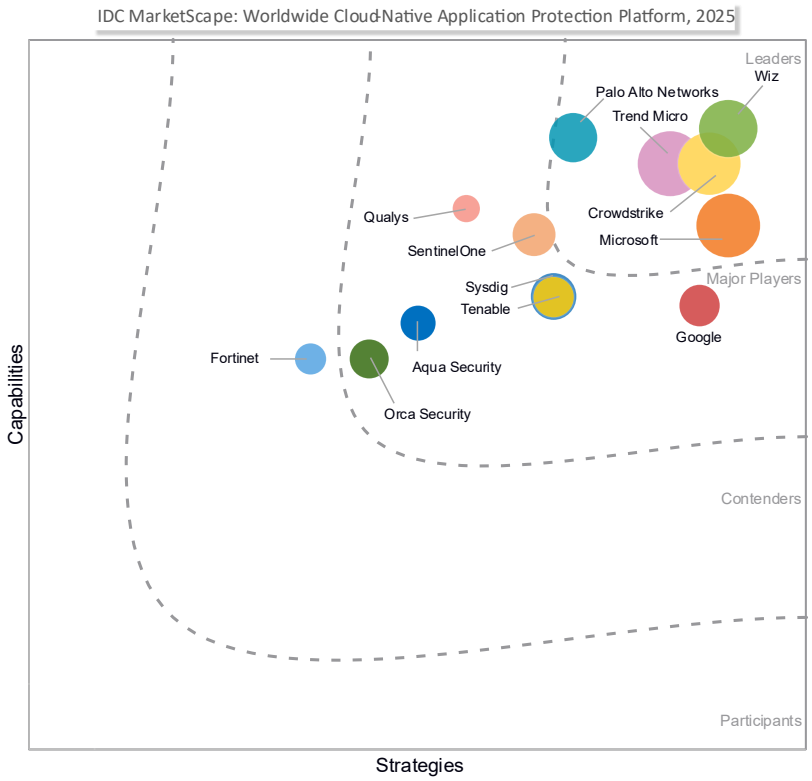
Philip Bues Frank Dickson

THIS EXCERPT FEATURES MICROSOFT AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cloud-Native Application Protection Platform Vendor Assessment



Source: IDC, 2025

June 2025, IDC #US53549925

See the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

This IDC study represents the vendor assessment model called IDC MarketScape. This study is a quantitative and qualitative assessment of the characteristics that explain a vendor's success in the marketplace and help anticipate the vendor's ascendancy.

This vendor evaluation assesses the capability and strategic vision of many of the worldwide cloud-native application protection platform (CNAPP) vendors software market. The evaluation is based on a comprehensive criterion expected to be most conducive to success in providing a unified, holistic cloud-native application protection platform capable of integration across the major cloud environments and on premises and promotes compliance as part of its main product offering.

IDC expects critical success factors for CNAPP to include but not limited to:

- Certifications: ISO 27017 for cloud security, ISO 27018 for privacy, ISO 27001:2022 SOC 2 type II, FedRamp High, European Cloud, Gov Cloud, Gov Cloud 2 IL5, 27032 (cybersecurity), VPAT/SEC 508: Accessibility, StateRamp High, HIPAA, GDPR, and so forth
- Risk scoring that can dynamically adjust to recent information such as exploitability, automatically classify risk tolerance/assign a risk score to each asset, and conduct attack path analysis to determine which assets may be a vulnerability
- Correlation of detections/alerts with threat intelligence, mapped to MITRE ATT&CK
- Asset graph showing how various assets are connected
- Integration with identity systems to show the user/owner associated with the asset without requiring additional analyst work, configuration management database (CMDB) to show the user/owner associated with the asset
- Remediation guidance for all the vulnerabilities captured in the platform
- Automated responses/playbooks
- Native integrations with collaboration platforms
- Holistic organizational risk score
- Monthly uptime guarantee of 99.9%
- Performance metrics or security outcomes and maturity model/assessment offered to customers to benchmark success and demonstrate effectiveness
- Insights on how customers compare against peers
- Partnerships/alliances with MSSP, technology partners, and channel partners (e.g., systems integrator [SI] and value-added reseller [VAR])

- Solution available in major cloud marketplaces

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

The process for this IDC MarketScape on CNAPP began in July 2024. IDC sent prequalification surveys to vendors that offered CNAPP. The preliminary list was quite substantial, and it became clear that specific conditions were required to make adequate comparisons between solutions.

There are a number of CNAPP solutions available from organizations that are not included in this evaluation, including but not limited to vendors that serve specific geographies and newer solutions with limited revenue and time on the market.

The following conditions need to be met for inclusion in this evaluation:

- The offering should be commercially available for use as a CNAPP that can be managed by the customer.
- The product must be available as an individual product (e.g., has its own SKU).
- The CNAPP product must be offered and available on a worldwide basis with sales in a minimum of two global regions.
- CNAPP revenue for CY24 reached a threshold determined by IDC through research or existing data.
- The CNAPP must contain three of the following components, in addition to cloud security posture management (CSPM), which is mandatory: CWPP, cloud infrastructure entitlement management (CIEM), KSPM, IaC, software composition analysis (SCA), AISPM, cloud detection and response (CDR), data security posture management (DSPM), API security, and vulnerability management.

ADVICE FOR TECHNOLOGY BUYERS

When selecting a cloud-native application protection platform vendor, it is essential to consider several factors beyond just vendor and tool consolidation. While reducing the number of vendors and tools can streamline operations, the primary drivers should include the platform's ability to integrate seamlessly with your existing security infrastructure and enhance your overall security posture.

Key Considerations

- **Integration and enrichment of existing security data:** Choose a CNAPP vendor that can easily integrate with your current deployments. The value lies in how the solution enriches your existing security data, providing deeper insights and more comprehensive protection.

- **Comprehensive capabilities:** Look for a solution that offers robust monitoring and reporting on cloud security posture, runtime, and application security. The goal is to select a platform based on its aggregate capabilities rather than merely reducing the vendor footprint.
- **Ease of setup and support:** Note that many vendors provide extensive support and make the initial setup straightforward with minimal technical effort required. However, the real value comes from planning and strategizing with stakeholders to ensure that the implementation aligns with your organizational goals. Remember, "measure twice and cut once," especially when dealing with heavily regulated data.
- **Vendor partnership:** Opt for a vendor that is committed to your success. This means having strong support from the customer success team, product team, and executives. Treat this relationship as a partnership where your team can raise issues, bugs, or feature enhancement requests, ensuring continuous improvement and alignment with your needs.
- **Compliance and security requirements:** Consider the best of both agent and agentless approaches. In particular, agentless solutions like "side scanning" may not meet stricter compliance requirements on their own. Therefore, it's crucial to consider dedicated vulnerability management solutions that can integrate with other security tools. This integration may provide a stronger business case, particularly during budgeting and compliance audits.
- **Phased implementation of AI policies:** Implement AI policies in phases to help control the use of AI tools. Careful planning and monitoring are necessary to ensure compliance without overly restricting user capabilities. This phased approach allows for adjustments and improvements based on real-world usage and feedback.

By focusing on these key areas, technology buyers can make informed decisions that not only enhance their security posture but also ensure seamless integration and long-term success.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Microsoft

Microsoft is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide CNAPP.

Microsoft Defender for Cloud, a cloud-native application protection platform, leverages advanced AI, comprehensive risk management, and unified security operations to enhance the security posture of cloud environments. Microsoft security offers unique capabilities such as autonomous attack disruption and deep integration across Microsoft's security ecosystem. Specifically, Defender for Cloud factors in over nine different elements, including critical assets, attack paths, and code reachability, to minimize false positives and expedite remediation efforts. The platform integrates near–real-time detections across all cloud and AI workloads, databases, storage, and APIs into a unified security operations platform.

Defender for Cloud is an integral part of Microsoft's comprehensive security platform. This unified platform combines the full capabilities of cloud-native SIEM (Sentinel), XDR (Defender XDR), unified exposure management (Microsoft Security Exposure Management), and cloud security (Defender for Cloud). By taking a platform approach, Microsoft can bring core security operations capabilities, data, and workflows together — in a single data lake — where they can be enriched with threat intelligence and enhanced and accelerated with GenAI copilots and agentic AI.

Strengths

Customers highlighted the strong partnership with Microsoft, which includes dedicated support and consulting, ensuring quick resolution of issues and access to experts for optimal product use. Microsoft Defender for Cloud was also recognized for providing detailed threat analytics, combining information from various sources to create comprehensive attack paths, helping understand the severity of alerts in context, and making it easier to prioritize and respond to threats. Additional commentary addressed Security Explorer and automatic detection of sensitive data without additional configuration, enhancing the security posture by providing valuable insights and automating critical security tasks.

Defender for Cloud provides visibility into cloud attacks across the entire environment, from enterprise endpoints and exposed identities to on-premises secrets. This holistic approach examines attack vectors inside and outside the cloud. Prebreach posture graphs are integrated with live incidents, offering exposure risk assessment through blast radius analysis.

Defender for Cloud has built-in capabilities in foundational CSPM that enable customers to perform assessments in their environment using security best practices

derived from Microsoft Cloud Security Benchmark, and using the secure score, customers can benchmark their progress over time.

In addition, Microsoft also offers a number of comprehensive training and workforce development campaigns, which range from student engagement to public training at low cost and some for free.

Challenges

While optimizing cloud security spend can always be a challenge, costs associated with various Microsoft products, including licenses, are at the higher end for some organizations. Customers noted this challenge may be exacerbated as enabling or disabling various components of Defender for Cloud at the subscription level can be cumbersome, leaving some to just leave things "as is." Overall, this speaks to the powerful features available in Defender for Cloud and being able to effectively use them may require creating additional processes and training.

Consider Microsoft When

Customers can measure the effectiveness of the Microsoft Defender for Cloud CNAPP solution with Secure Score. This allows customers to get insights into their overall cloud security posture and how they can improve it with security recommendations and remediation guidance in Defender for Cloud. With multicloud support, customers can manage and secure their cloud environments more effectively, ensuring robust protection across multiple cloud platforms. Cloud security is one of the workload security initiatives where customers can assess, manage, and measure the risk associated with specific workload domains. Each security initiative provides an all-up score that provides a fast measure of how strong security posture is for the chief information security officers (CISOs), and security teams can use security insights and context to understand and manage exposure risk across the entire organization and to prioritize security efforts and investment.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under

this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Cloud-native application protection platform (CNAPP) solutions are designed to maintain the integrity of software-defined compute (SDC) servers, providing protection features that traditionally include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. The definition of CNAPP has expanded to include security solutions such as vulnerability management, configuration management, and application developer tools. Since the genesis of the market, products and features have been added and continue to evolve, unifying security and compliance capabilities across cloud environments.

As CNAPP has expanded its field of action, on-premises virtualized datacenters have become part of CNAPP's coverage. In light of this expansion and due to the importance of virtualization, hybrid ecosystems, and silicon-level security, some CNAPP solutions may also include physical server security products as part of their security offering. CNAPP offerings accomplish their goals by ensuring that the system does not run malicious software that can compromise business applications and data on the servers and/or prevent malicious actors from accomplishing nefarious tasks.

LEARN MORE

Related Research

- *IDC's Worldwide Security Products Taxonomy, 2025* (IDC #US53164625, February 2025)
- *CIEM and Zero Trust — Lower Risk Appetite Improves Posture* (IDC #US53164625, February 2025)
- *Who's Winning the Hearts of AI-Enabled Outcomes* (IDC #US53188625, February 2025)
- *Emerging Security Technologies and Trends for 2025: What Happens AFTER GenAI… Outcomes Get Real Again* (IDC #US52697424, November 2024)
- *Kubernetes Security Best Practices, 2024* (IDC #US52677524, October 2024)

Synopsis

This IDC study evaluates the capabilities and strategic vision of 13 global vendors in the cloud-native application protection platform (CNAPP) market. It provides a comprehensive assessment of each vendor's ability to deliver integrated security solutions across major cloud environments and on premises, promoting compliance. The study includes detailed vendor profiles, strengths, challenges, and advice for technology buyers, helping organizations make informed decisions to enhance their security posture and enable seamless integration.

"Discover the future of cloud-native security with IDC MarketScape 2025 Vendor Assessment, evaluating top CNAPP solutions for comprehensive protection and strategic vision." — Philip Bues, senior research manager, Cloud Security and Confidential Computing, IDC

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

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