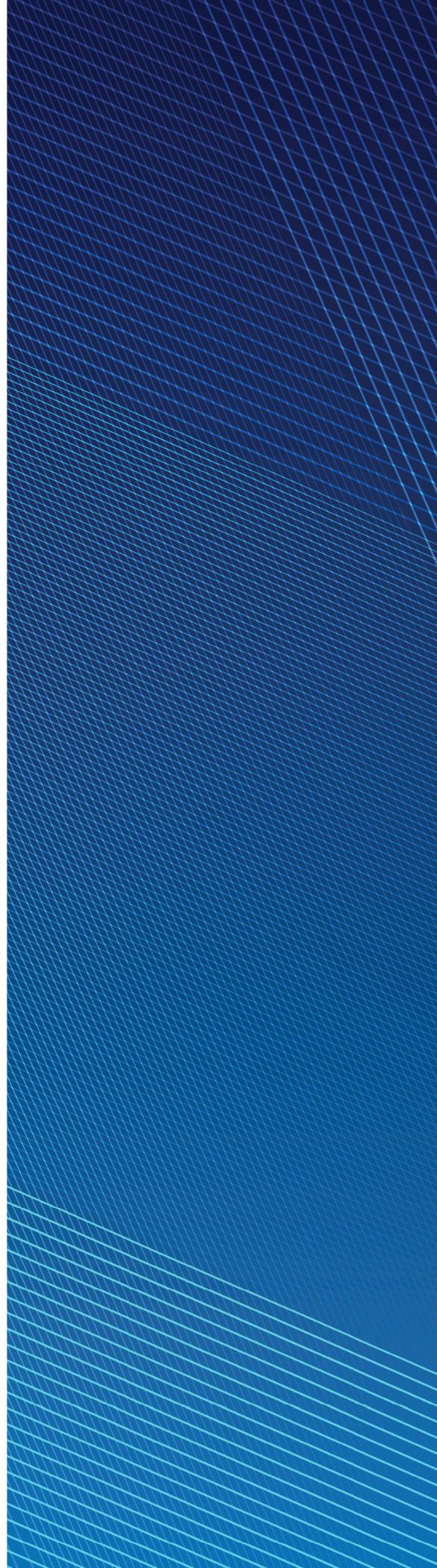


# **PALO ALTO NETWORKS** COMPANY OF THE YEAR AWARD

---

*Identified as best in class in the global cloud-native  
application protection platform (CNAPP) industry*



## Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each Award category before determining the final Award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Palo Alto Networks excels in many of the criteria in the global cloud-native application protection platform (CNAPP) space.

AWARD CRITERIA	
<i>Visionary Innovation &amp; Performance</i>	<i>Customer Impact</i>
Addressing Unmet Needs	Price/Performance Value
Visionary Scenarios Through Mega Trends	Customer Purchase Experience
Implementation of Best Practices	Customer Ownership Experience
Leadership Focus	Customer Service Experience
Financial Performance	Brand Equity

### Addressing Unmet Needs

As part of the digital transformation efforts, companies worldwide increasingly turn to cloud and cloud-native technologies, viewing them as essential tools in their strategies. This adoption significantly changes how organizations build, operate, and manage back-end infrastructure and customer-facing applications. Despite these benefits, Frost & Sullivan analysts monitor how the move toward cloud and cloud-native technologies creates more complex security challenges for organizations. These include weak spots and blind spots resulting from cloud migration efforts, lack of compliance coverage and security breadth, and the challenge of managing multiple tools that do not integrate well. In addition, organizations face a lack of resources for security and security operations (SecOps) - and must balance security risk and business continuity.

To overcome these challenges, organizations report to Frost & Sullivan that they seek cloud security solutions that provide comprehensive security coverage for cloud environments, workloads, and applications across their development lifecycle, from code to runtime in multiple clouds and deployment scenarios. Specifically, customers look for purpose-built security tools for modern cloud compute architectures (such as containers, Kubernetes, and serverless technologies).

More importantly, Frost & Sullivan points out that all of these capabilities must be converged and delivered from a single platform to simplify and automate the compliance and security checking process to reduce the reliance on error-prone human intervention and make security outcomes more effective.

An integrated cloud security platform can help organizations deal with the development, security, and operations (DevSecOps) culture, enabling Dev, Ops, and Security to fully see infrastructure requirements, security risks, and business priorities. This enhances their collaboration and allows organizations to operationalize cloud security more effectively.

Palo Alto Networks is a global cybersecurity leader known for its integrated security operating platforms, with flagship products such as the Next-Generation Firewalls (NGFW), SASE and Prisma Cloud, and Cortex, which includes endpoint and security operations solutions.

Palo Alto Networks is one of the first vendors in the market that can provide a full-stack CNAPP, Prisma Cloud, that delivers all security aspects for cloud-native applications throughout the application development lifecycle from code to cloud. These include code security, cloud security posture management (CSPM), cloud workload protection (CWP, agent-based and agentless), infrastructure as code (IaC) security, cloud network security (CNS), and cloud infrastructure entitlement management (CIEM), which enables companies to effectively shift-left their security strategies and maximize security coverage and protection in different environments.

*“Palo Alto Networks is one of the first vendors in the market that can provide a full-stack CNAPP platform, Prisma Cloud, that delivers all security aspects for cloud-native applications throughout the application development lifecycle from code to cloud. These include code security, cloud security posture management (CSPM), cloud workload protection (CWP, agent-based and agentless), infrastructure as code (IaC) security, cloud network security (CNS), and cloud infrastructure entitlements management (CIEM), which enables companies to effectively shift their security strategies and maximize security coverage and protection in different environments.”*

**– Anh Tien Vu,  
Industry Principal, Global Cybersecurity Research**

Prisma Cloud distinguishes itself from other CNAPP solutions by offering a platform that covers five critical cloud security areas, providing organizations with best-in-class security across the entire software development lifecycle (SDLC). By taking a prevention-first approach to cloud security, Frost & Sullivan notes that Prisma Cloud also stands apart from many other CNAPP providers that mainly offer visibility and compliance checks with limited prevention control capability. This means they cannot proactively stop critical attacks and prevent lateral

movement. Prisma Cloud can also deliver continuous, real-time visibility and threat detection with updates in just minutes. This is a more effective option compared to other solutions that scan cloud configurations and workloads every 12 to 24 hours as these solutions create blind spots that miss out on cloud configuration change states, audit trails, and ephemeral workloads.

With the ability to offer the broadest security capabilities (e.g., DevOps, CSPM, CWP, CIEM, CNS) and coverage across cloud service providers (CSPs), workload architectures, DevOps tools, and SecOps integrations, Prisma Cloud has gradually become a platform of choice for many large organizations that need comprehensive security capabilities.

Palo Alto Networks designed Prisma Cloud for cloud-scale security. The company has proven to secure any multi-cloud environment at any scale, securing over 7 billion cloud assets and 2.5 million workloads

and processing over 1 trillion events daily. Palo Alto Networks R&D has engineered Prisma Cloud from the ground up to deliver real-time visibility and protection at scale.

### ***Implementation of Best Practices and Leadership Focus***

According to the Cloud Native Computing Foundation, 96% of organizations worldwide now use or are considering cloud-native application development tools. The growing adoption of cloud-native application development platforms introduces new security challenges, making traditional security solutions obsolete and inadequate. This drives organizations to seek cloud-native platforms that can offer visibility into the cloud environment and workload behavior and provide protection across the lifecycle, from designing and testing to runtime protection.

Palo Alto Networks is a CNAPP pioneer and has solidified its position as a market leader in cloud-native security market through a combination of acquisition and technology innovation. It has acquired several companies, including Evident.io, Redlock, PureSec, Twistlock, and Bridgecrew, and has integrated them into a single platform. This acquisition strategy has enabled the company to broaden its security offerings, providing protection for containers, public cloud applications, and serverless environments. In addition to acquisition, Palo Alto Networks has also focused on technology innovation to develop in-house capabilities such as Web application firewall (WAF), API security, threat detection, CIEM, data security, software composition analysis, and secrets security. This balance of acquire and build has resulted in the

*“Prisma Cloud distinguishes itself from other CNAPP solutions by offering a platform that covers five critical cloud security areas, providing organizations with best-in-class security across the entire software development lifecycle (SDLC). By taking a prevention-first approach to cloud security, Palo Alto Networks also stands apart from many other CNAPP providers that mainly offer visibility and compliance checks with limited prevention control capability. This means they cannot proactively stop critical attacks and prevent lateral movement.”*

***– Anh Tien Vu,  
Industry Principal, Global Cybersecurity Research***

most comprehensive security solution to protect critical workloads, applications, and data in the cloud, positioning Palo Alto Networks as the market leader for holistic cloud-native security.

For example, in 2021, Palo Alto Networks’ Prisma Cloud became the first CNAPP solution to integrate code security by integrating Bridgecrew. It also released IaC security and launched Web Application and API Security that integrates Web App Firewall (WAF), API Security, Runtime Protection, and Bot Defense together. The company quickly expanded with the code

security offering in 2022 with the organic development of software composition analysis (SCA) with software bill of materials (SBOM) and secret scanning into its platform. Its in-house innovation continued with the addition of agentless CWP in 2022, making it one of the few vendors in the market that offers integrated CNAPP solutions with both agent-based and agentless security options for multi-cloud environments.

The company also introduced alert prioritization via MITRE ATT&CK for cloud framework and expanded CSPM threat detection and granular role-based access control (RBAC) for CNAPP. In addition, it completed its acquisition of Cider Security (Cider), a pioneer in application security (AppSec) and software supply chain security. This strengthens Prisma Cloud’s ability to bring security further to the left of the

development lifecycle to help organizations better manage cyber risks in the continuous integration (CI)/continuous delivery or deployment (CD) pipeline and recommend remediation solutions. Looking ahead, Palo Alto Networks aims to bring security closer to DevOps and developer teams to minimize friction. The company has a thriving partner ecosystem, including 8K+ NextWave partners, system integrators (SIs), service providers, and CSPs.

From the go-to-market strategy perspective, Palo Alto Networks creates deeper and more strategic partnerships to bring its entire portfolio to more customers. The company has established strategic alliances with leading CSPs (e.g., AWS, Azure, and Google Cloud), ecosystem leaders (e.g., Hashicorp and Red Hat), and global SIs, channel partners, and distributors. As the partner-engaged strategy drives most of its business, expanding its partnership with international partners and CSPs will enable the company to expand its market leadership position.

### ***Financial Performance***

Palo Alto Networks has registered a significant adoption and consumption rate across its security modules and capabilities, particularly CSPM, cloud workload protection platform (CWPP), API protection, CIEM, and secret scanning. The company recorded a 48% year-on-year (YoY) increase in the credit consumption of Prisma Cloud in 2022, driven by new customer additions and customers increasing their cloud footprints and consuming additional modules. Despite discussions of moderation and cloud consumption in the market, Palo Alto Networks believes the early stage of cloud security adoption will shelter them from these headwinds.

Based on Frost & Sullivan's latest estimate, Palo Alto Networks recorded a 38.5% YoY growth in 2022, making it the world's largest CNAPP vendor in revenue. The company experienced strong business growth in all regions, particularly in North America, where it maintained the largest CNAPP market share and continued to grow tremendously, driven by federal government agencies, technology, healthcare, and banking. It also saw remarkable revenue growth in Europe, the Middle East, and Africa (EMEA) during the year while recording robust CNAPP platform adoption in APAC by companies operating in financial technology (FinTech); banking, financial services, and insurance (BFSI); and healthcare.

Palo Alto Networks gains traction for its Prisma Cloud in critical verticals such as BFSI, technology, government, telecommunications, and healthcare. Since many of these are large businesses with cloud deployment at scale and are existing customers, Frost & Sullivan points out that it is easier for Palo Alto Networks to cross-sell or upsell Prisma Cloud solutions on top of their current security deployment.

### ***Customer Purchase and Service Experience***

Palo Alto Networks offers a comprehensive and integrated cloud platform that delivers many customer benefits, such as unified management, simplified security operations, and improved return on investment. The Prisma Cloud platform provides end-to-end protection for the entire application development lifecycle, utilizing agent-based and agentless approaches to increase visibility, protection, and remediation efficacy while reducing risks and increasing productivity. For example, Palo Alto Networks reported that the solution enables organizations to reduce DevOps time to reduce vulnerability by 60%, time spent configuring policies by 80%, and renewable identification number (RIN) compliance reporting by 90%.

Notably, the company provides extensive training for customers to operate its technology. This reduces customers' time-to-value to under 60 days. Palo Alto Networks also offers a single stock-keeping unit (SKU) with a flexible credit system that customers can use for any of its offerings. This makes it simple for customers to purchase and consume security products as they need across the platform.

In addition, Palo Alto Networks has created a robust partner ecosystem, including CSPs, global SIs, and channel partners, to help customers scale securely in the cloud. The company provides strong support from its teams and channel ecosystem, leveraging partners' capabilities to deliver support and professional and educational services to organizations. With access to over 100 customer success experts, customers can accelerate time-to-value and ensure operational best practices when implementing solutions.

Overall, Palo Alto Networks' strong technological capabilities, innovation, and support enhance customer satisfaction and experience, driving engagement and loyalty among existing customers and attracting new ones globally. It understands an organization's cloud maturity, DevOps maturity, and cloud security pain points before recommending the appropriate solution, such as a workload protection solution for cloud workloads and applications. Since the services are modular, customers can gradually expand their capabilities over time without additional fragmented tools.

## Conclusion

---

Prisma Cloud from Palo Alto Networks offers comprehensive security for cloud-native applications regardless of their technology stack and cloud environment. This solution covers all aspects of cyber threat management, including virtual machines, serverless applications, containers, containers-as-a-service, and containers-on-demand, all from a single, unified platform.

By delivering comprehensive capabilities from code to cloud with a unique prevention-first approach, Prisma Cloud has gained significant popularity among global organizations. Its excellent customer purchase and service experience also increase customer confidence and satisfaction, leading to consistent revenue growth over the past few years.

With its strong overall performance, Palo Alto Networks earns the 2023 Frost & Sullivan Global Company of the Year Award in the cloud-native application protection platform (cnapp) industry.

## What You Need to Know about the Company of the Year Recognition

---

Frost & Sullivan's Company of the Year Award is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

### Best Practices Award Analysis

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

#### *Visionary Innovation & Performance*

**Addressing Unmet Needs:** Customers' unmet or under-served needs are unearthed and addressed by a robust solution development process

**Visionary Scenarios Through Mega Trends:**

Long-range, macro-level scenarios are incorporated into the innovation strategy through the use of Mega Trends, thereby enabling first-to-market solutions and new growth opportunities

**Leadership Focus:** Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

**Best Practices Implementation:** Best-in-class implementation is characterized by processes, tools, or activities that generate a consistent and repeatable level of success

**Financial Performance:** Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics.

#### *Customer Impact*

**Price/Performance Value:** Products or services provide the best value for the price compared to similar market offerings

**Customer Purchase Experience:** Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

**Customer Ownership Experience:** Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

**Customer Service Experience:** Customer service is accessible, fast, stress-free, and high quality

**Brand Equity:** Customers perceive the brand positively and exhibit high brand loyalty

## About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at <http://www.frost.com>.

## The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

[Learn more.](#)

### Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** Implementation Excellence
- **Transformational Growth:** Industry Leadership



## The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

### Analytical Perspectives:

- **Mega Trend (MT)**
- **Business Model (BM)**
- **Technology (TE)**
- **Industries (IN)**
- **Customer (CU)**
- **Geographies (GE)**

