FROST & SULLIVAN

BEST PRACTICES

2026 GLOBAL CLOUD WORKLOAD SECURITY

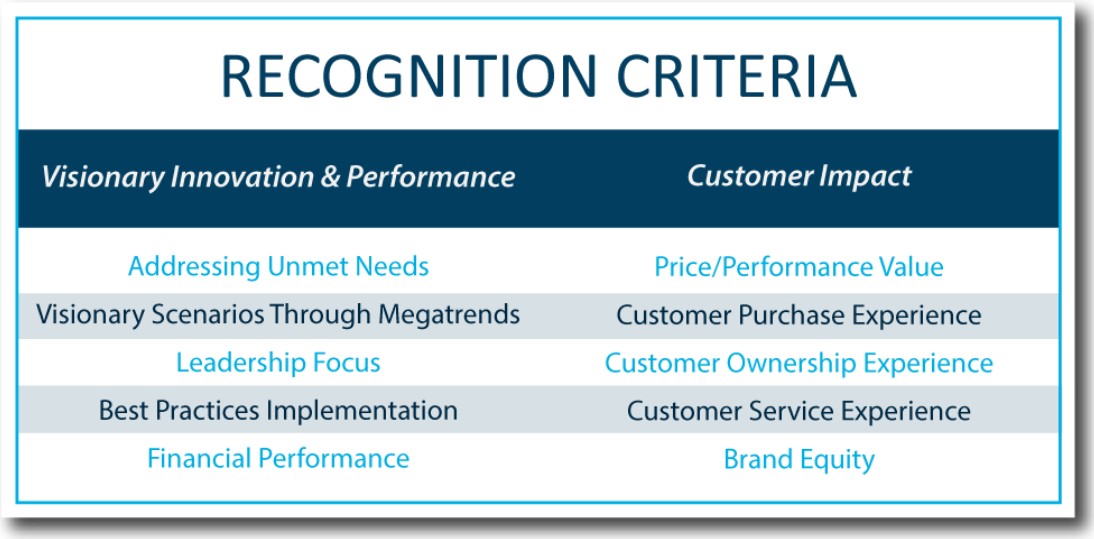
COMPANY OF THE YEAR

CROWDSTRIKE

Table of Contents

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. CrowdStrike excels in many of the criteria in the cloud workload security space.



The Transformation of the Cloud Workload Security Industry

Cloud migration continues to introduce a host of new attack vectors and cyber risks, exponentially expanding the attack surface through pervasive use of open-source components and cloud-native development tools. The highly dynamic nature of cloud environments creates a pronounced gap between the speed at which cloud workloads scale and the ability of security programs, tools, and teams to keep pace. As a result, SecOps and security operations center (SOC) analysts are flooded with routine alerts and telemetry, leaving limited capacity to investigate high-risk events, contain active threats, and support innovation, which ultimately slows digital transformation and strains relationships between security and development teams.

Hybrid and multi-cloud strategies force organizations to manage workloads across AWS, Azure, Google Cloud, private clouds, and on-premises data centers. This heterogeneity fragments visibility and control, mainly when legacy tools rely on separate consoles, policies, and monitoring workflows for each environment. The resulting operational complexity makes it difficult for SOC teams to maintain consistent policies, detect lateral movement, and rapidly understand the scope of an incident, increasing both dwell time and breach impact.

Chief information security officers (CISOs) face the difficult task of balancing budget constraints with the reality of tool proliferation across their organizations.

© Frost & Sullivan 2026

The need for efficient security operations has prompted a fundamental shift toward consolidation, with organizations increasingly seeking unified platforms rather than managing disjointed point solutions. Navigating these challenges within multi-cloud architectures further compounds the complexity. To succeed in this environment, CISOs require solutions that bridge the skills gap between teams, facilitate continuous compliance, and offer comprehensive, automated security coverage across the entire cloud infrastructure stack.

Cloud workload security (CWS) is evolving to address this complexity by extending runtime security across virtual machines (VMs), containers, and serverless workloads, providing a single layer of visibility, security control, and threat detection and response (TDR). CWS solutions that enforce consistent runtime policies across multi-cloud and hybrid deployments not only help organizations reduce risk, but also simplify compliance reporting and governance. This unified approach allows organizations to apply consistent policies whether a workload runs in the public cloud, a private Kubernetes cluster, or a regulated on-premises system.

With runtime monitoring and protection capabilities, CWS enables continuous inspection of workloads, alerting teams to suspicious processes, anomalous behavior, or privilege escalations as they happen. This ability to react in real time makes CWPP a great complement to pre-deployment security checks, detecting anomalous behavior, privilege escalation, and lateral movement.

> *"Falcon Cloud Security is widely recognized for innovation and growth, delivering deep cloud visibility, advanced runtime defenses, and strong cloud detection and response (CDR). While other posture-centric or compliance-driven tools tend to detect risk only pre-deployment or at the control plane, CrowdStrike's CWPP uses artificial intelligence (AI)/machine learning (ML)-driven behavioral analytics, Indicators of Attack, and rich adversary intelligence to detect fileless attacks, lateral movement, and privilege abuse at runtime that traditional scanners consistently miss. This runtime-first model provides materially stronger breach prevention than solutions that rely solely on periodic assessments."*
>
> ***– Anh Tien Vu,***
> ***Industry Principal, Global Cybersecurity Practice***

Advanced CWSs can offer automated response actions, such as isolating a VM, terminating a malicious container, or blocking lateral movement, to prevent major breaches caused by the lateral movement of risks or threats in the cloud environment. This real-time response complements shift-left practices by catching issues that slip past pre-deployment controls and closing blind spots created by ephemeral workloads. When CWS integrates with XDR and SOC workflows, it provides unified, contextualized intelligence across endpoints, identities, networks, and cloud workloads, helping organizations reduce tool sprawl, lower mean time to detect (MTTD) and mean time to respond (MTTR), and significantly improve overall SOC efficiency and effectiveness.

Addressing Unmet Needs with Integrated Code to Cloud to SOC Cloud Security Vision

Established in 2011, CrowdStrike is a leader in cybersecurity by delivering a unified, runtime-powered cloud security platform that protects endpoints, cloud workloads, identities, and data through a single

lightweight agent. This architecture significantly reduces operational overheads while enabling deep visibility, real-time threat prevention, and seamless scalability across multi-cloud and hybrid environments. Unlike many competitors that rely on fragmented toolsets that combine separate agents, scanners, and cloud-only monitors, CrowdStrike integrates runtime protection, cloud security posture management (CSPM), identity security (cloud infrastructure entitlement management [CIEM]), XDR, and managed detection and response (MDR)into a single cohesive platform, reducing both complexity and security gaps.

To meet the industry-wide push for platform consolidation, CrowdStrike offers Falcon Cloud Security, a complete cloud-native application protection platform (CNAPP) that unifies CWPP, container and Kubernetes security, CSPM, Kubernetes Security Posture Management (KSPM), CIEM, and IaC security. Vendors that focus solely on posture management or agentless scanning often struggle to deliver the runtime depth and workload-level prevention needed to stop active breaches. CrowdStrike's strategic acquisitions of Bionic, Flow Security, and Adaptive Shield extend the platform into Application Security Posture Management (ASPM), Data Security Posture Management (DSPM), and SaaS Security Posture Management (SSPM), enabling full code-to-cloud-to-application risk management that few rivals can match.

Falcon Cloud Security is widely recognized for innovation and growth, delivering deep cloud visibility, advanced runtime defenses, and strong cloud detection and response (CDR). While other posture-centric or compliance-driven tools tend to detect risk only pre-deployment or at the control plane, CrowdStrike's CWPP uses artificial intelligence (AI)/machine learning (ML)-driven behavioral analytics, Indicators of Attack, and rich adversary intelligence to detect fileless attacks, lateral movement, and privilege abuse at runtime that traditional scanners consistently miss. This runtime-first model provides materially stronger breach prevention than solutions that rely solely on periodic assessments.

The platform continues to push the frontier of runtime and Kubernetes protection. Falcon deploys as a Kubernetes DaemonSet, uses Admission Controllers to block risky workloads before they run, and leverages extended Berkeley Package Filter (eBPF) for high-fidelity, low-overhead telemetry across containers and cloud data flows. Unlike competitors that rely solely on agentless snapshots or metadata analysis, CrowdStrike can detect in-memory attacks and real-time behavioral anomalies, including in serverless environments such as AWS Fargate, and integrates with numerous image registries for comprehensive pre-deployment scanning.

CrowdStrike further differentiates itself through a dual agent-based and agentless model, drift detection, exploit prevention, and broad operating system support. For DevSecOps teams, advanced shift-left capabilities, such as continuous integration/ continuous development (CI/CD) scanning, Software Bills of Materials (SBOM) generation, image attestation, and Software Component Analysis (SCA) with reachability, go well beyond the limited static scanning offered by many alternatives.

CrowdStrike also excels at aligning cloud protection with SecOps and SOC operations. While some platforms generate high alert volumes with limited cross-domain context, Falcon correlates endpoint, identity, and cloud telemetry to produce prioritized, actionable alerts that reduce noise and speed investigations. Automated remediation and guided response streamline triage and help lower MTTD and

MTTR. When combined with Falcon XDR and Falcon Complete Cloud Security MDR, organizations gain 24/7 cross-domain threat hunting and incident response across endpoints and cloud workloads.

> *"CrowdStrike is one of the fastest-growing players in the CNAPP market, maintaining stellar momentum into 2025 precisely because its business model aligns perfectly with how organizations actually procure and deploy security solutions. The company's rapid growth is primarily fueled by the explosive adoption of its cloud workload security module, which has become a critical add-on for its massive installed base of endpoint security customers. This 'land-and-expand' strategy proves highly effective because it leverages existing customer relationships and trust, allowing CrowdStrike to monetize its installed base while simultaneously capturing net-new cloud-first customers seeking unified security platforms."*
>
> ***– Anh Tien Vu,***
> ***Industry Principal, Global Cybersecurity Practice***

Ultimately, CrowdStrike's unified, cloud-native architecture delivers unmatched consistency across workloads and environments. By combining runtime defense, code-to-cloud visibility, and SOC-grade detection and response, CrowdStrike provides a level of protection and operational efficiency that clearly outperforms fragmented or posture-only cloud security offerings, making it an excellent candidate for cloud workload protection and runtime defense, which many competitors cannot deliver.

Leadership Focus via Explosive Growth and Platform Expansion

CrowdStrike is one of the fastest-growing players in the CNAPP market, maintaining stellar momentum into 2025 precisely because its business model aligns perfectly with how organizations actually procure and deploy security solutions. The company's rapid growth is primarily fueled by the explosive adoption of its cloud workload security module, which has become a critical add-on for its massive installed base of endpoint security customers. This "land-and-expand" strategy proves highly effective because it leverages existing customer relationships and trust, allowing CrowdStrike to monetize its installed base while simultaneously capturing net-new cloud-first customers seeking unified security platforms.

A key driver of this exceptional expansion is CrowdStrike's sophisticated partner-first ecosystem strategy. The company has successfully operationalized a Cloud Security Sales Play that engages over 1,900 global solution providers, 500+ managed security service providers, and major global systems integrators. This extensive channel network ensures that CrowdStrike solutions are embedded into large-scale digital transformation projects across critical verticals, including banking and financial services, technology, healthcare, media and entertainment, and retail. By enabling partners to succeed with CrowdStrike technology, the company is amplifying its reach far beyond what direct sales alone could achieve.

CrowdStrike's ability to transact in the cloud era has established new market benchmarks. The company became the first cybersecurity independent software vendor (ISV) to surpass $1 billion in cumulative sales through the AWS Marketplace, which reflects not just the platform's market adoption but also the efficiency with which it enables cloud-native purchasing and deployment. Furthermore, the company is experiencing significant growth on the Google Cloud Marketplace and has forged strategic alliances with technology titans, including NVIDIA and Microsoft. These partnerships elevate CrowdStrike's platform

relevance by integrating it into the technology stacks of organizations that already rely on these partners for critical infrastructure.

In addition, the company's strategic acquisition strategy demonstrates a commitment to comprehensive innovation rather than incremental feature development. The acquisitions of Bionic and Flow Security expanded the platform's capabilities in ASPM and DSPM, respectively, filling critical gaps that would have taken years to develop organically. These moves differentiate CrowdStrike from competitors that rely primarily on reactive compliance tools rather than on proactive breach prevention frameworks. By combining technology and acquisition-driven innovation with its world-class MDR and threat-hunting expertise, CrowdStrike creates a virtuous cycle of customer value that competitors struggle to match.

The company's brand perception stands unrivaled in the market. CrowdStrike is viewed not merely as a tool vendor, but as a strategic partner capable of securing the entire enterprise estate, from the endpoint to the cloud to identity and data, through a single, integrated security lens. This positioning enables the company to command premium pricing, maintain exceptional customer retention rates, and operate at significantly higher margins than point-solution competitors.

Accelerating Popularity through a Customer-First Service Approach

Beyond its technological prowess, CrowdStrike's success is deeply rooted in a customer-first service model that bridges the often-frustrating gap between complex cloud security technology and meaningful operational outcomes. This commitment to customer success extends far beyond traditional vendor support, positioning CrowdStrike as a strategic security partner rather than a transactional software provider.

The flagship Falcon Complete Cloud Security managed service represents a major differentiator in how CrowdStrike approaches customer engagement. This fully managed detection and response offering addresses the chronic cybersecurity skills shortage that plagues organizations globally by providing 24/7 expert management and threat hunting. For most organizations, building a mature cloud security program internally is cost-prohibitive, time-consuming, and difficult.

Falcon Complete solves this problem by delivering instant operational maturity and breakthrough protection outcomes from the very first day of deployment. This service dramatically lowers adoption barriers by making enterprise-grade security accessible to organizations of all sizes and maturity levels, enabling even those with limited security expertise to confidently migrate to the cloud with robust protection from day one.

CrowdStrike's commitment to customer success extends into its support architecture, which reflects a fundamentally different philosophy from many competitors. The company offers a transparent, tiered support structure with Express, Essential, and Elite tiers that cater to various business needs and organizational sizes. Critically, CrowdStrike maintains direct engagement options rather than offloading support entirely to third-party channels, enabling customers to receive consistent, high-quality assistance aligned with CrowdStrike's product vision and best practices. The company also provides global assistance through local phone support, automated case routing, and clear response time commitments, streamlining access to assistance based on incident urgency.

The platform itself is architected to reduce operational burden through intelligent design choices that reflect a deep understanding of real-world SOC operations. CrowdStrike integrates with existing SecOps and SOC workflows by providing prioritized, contextual alerts that dramatically reduce alert fatigue and false positives, thereby increasing productivity and team collaboration. Features such as one-click sensor deployment, agentless snapshot scanning, and automated remediation recommendations streamline daily operations and free security teams to focus on strategic initiatives rather than routine tasks. By emphasizing observable outcomes over alert volume, CrowdStrike helps organizations achieve more security value per dollar invested and per security professional employed.

The platform's approach to bridging security and development teams represents another dimension of customer-first design, enhancing collaboration across DevSecOps initiatives while maintaining operational efficiency in fast-paced, cloud-native environments. By providing developers with actionable shift-left capabilities and giving security teams automated visibility into development pipeline security posture, CrowdStrike enables these teams to work toward shared objectives rather than at cross-purposes.

The ability to combine excellent technology with world-class service helps maximize customer value, further fostering deep loyalty, encouraging the expansion of platform adoption across additional use cases and departments, and creating a powerful customer purchase lifecycle that drives organic growth through referrals and case studies. This customer-centric philosophy directly translates into higher retention rates, lower churn, and accelerated revenue growth.

Conclusion

CrowdStrike’s rise to this market inflection point demonstrates its delivery of a unified cloud-native platform that protects endpoints, cloud workloads, identities, and data with an equal level of protection. By focusing on breach prevention-first principles and proactive threat detection and response, CrowdStrike enables organizations to confidently embrace cloud technologies without compromising security. The Falcon Cloud Security platform delivers superior breach prevention through proactive attack path visualization and automated response orchestration, seamless customer experiences through direct support and managed services, and rapid time-to-value through intelligent platform design and extensive integration capabilities.

With its exceptional financial performance, industry-leading technology capabilities, and unwavering commitment to customer success, CrowdStrike earns Frost & Sullivan's 2026 Global Company of the Year Recognition in the cloud workload protection and runtime security industry.

© Frost & Sullivan 2026

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

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

Best Practices Recognition Analysis

For the Company of the Year Recognition, 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 to create growth opportunities across the entire value chain

Visionary Scenarios Through Megatrends: Long-range scenarios are incorporated into the innovation strategy by leveraging megatrends and cutting-edge technologies, thereby accelerating the transformational growth journey

Leadership Focus: The company focuses on building a leadership position in core markets to create stiff barriers to entry for new competitors and enhance its future growth potential

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

Financial Performance: Strong overall business performance is achieved by striking the optimal balance between investing in revenue growth and maximizing operating margin

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

© Frost & Sullivan 2026

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

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 Generator™

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:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)