FROST & SULLIVAN

BEST PRACTICES

2026 GLOBAL WAF AND API SECURITY

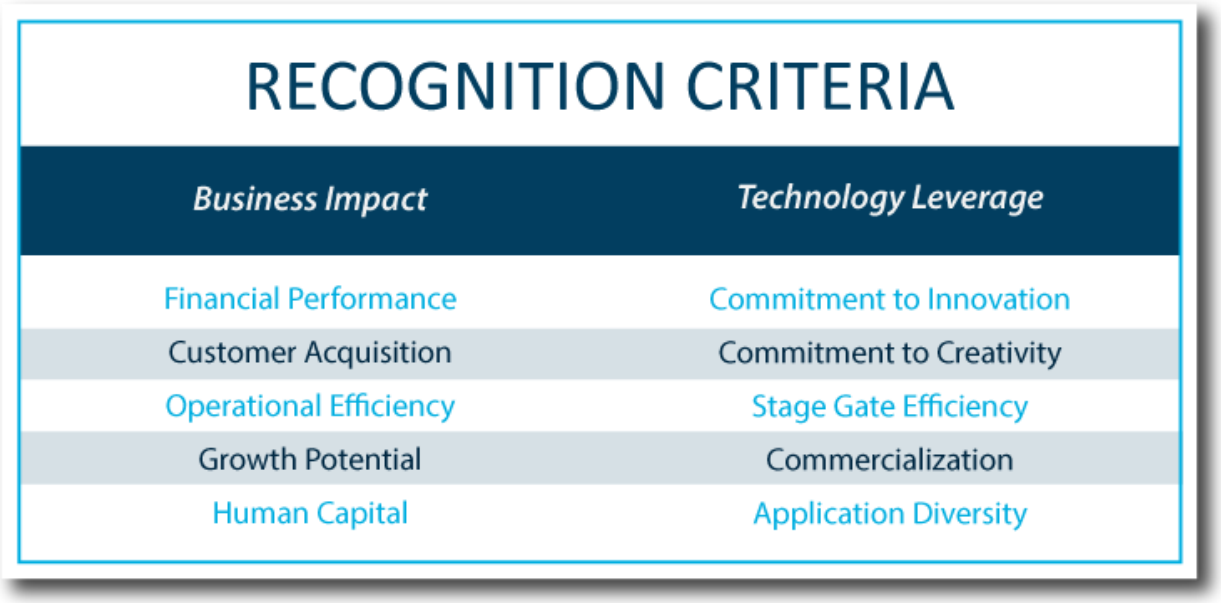
TECHNOLOGY INNOVATION LEADERSHIP

CHECK POINT™

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. Check Point excels in many of the criteria in the WAF and API security space.



The Transformation of the WAF and API Security Industry

Over the past several years, the application security landscape has structurally transformed as architectures shifted from monolithic deployments to highly dynamic, cloud-native ecosystems composed of microservices, application programming interface (API)-first integrations, and AI-driven components. Each release now introduces new containers, APIs, business logic, and third-party dependencies across hybrid, multi-cloud, and edge environments. At the same time, DevSecOps, continuous integration/continuous delivery (CI/CD), and infrastructure-as-code have accelerated deployment, increased complexity and making threat detection and response more difficult.

Architectural decentralization has expanded the attack surface beyond standard open web application security project (OWASP) risks to encompass zero-day exploits, API abuse, GenAI misuse, and advanced evasion techniques. Traditional tools, such as static code scanners and first-generation web application firewall (WAF) and API security solutions, rely on signatures, manual rule tuning, emergency patching, and periodic scans. They struggle in production settings where runtime behavior diverges from static assumptions, resulting in false positives, missed threats, higher total cost of ownership, and security team fatigue.

Zero-day events such as Log4Shell and Spring4Shell highlighted the structural limitations of signature-driven defenses. Enterprise priorities have therefore shifted from vulnerability discovery to active runtime prevention. Organizations now seek context-aware web applications and API protection (WAAP) platforms that use AI, ML, and automation to continuously analyze behavior and block known and novel attacks in real time.

Bridging the Gaps to Match Industry Needs

Founded in 1993 and headquartered in Israel and the United States, Check Point Software Technologies is a global cybersecurity leader with a broad security portfolio encompassing network, cloud, and application protection. To modernize its cloud-native application security stack, Check Point evolved its Cloud portfolio and rebranded CloudGuard WAF as Check Point WAF, a cloud-native web, GenAI apps & APIs security solution. This transition marks a shift from rules-driven WAFs to an AI-first, cloud-native protection model.

Check Point WAF addresses modern web, API, and GenAI security challenges where legacy WAFs fail to address zero-day exploits, evasion techniques, and operational overhead. As part of the Cloud family, it functions as an AI-driven WAAP platform for cloud-native applications. It protects legacy web services, internal APIs, customer-facing cloud-native apps, and GenAI-powered applications, with strong relevance for regulated sectors such as BFSI and retail that face frequent web-based attacks and stringent compliance requirements.

The solution delivers unified protection for web applications, APIs, microservices, and bots in a single platform. It supports on-premises, multi-cloud, and edge deployments via content delivery networks, enabling consistent protection across environments. Check Point WAF replaces the traditional "detect, tune, and react" model with continuous, contextual runtime enforcement. Using dual-layer ML, it analyzes attacker behavior and application context to block both known and unknown zero-day exploits, including Log4Shell, Spring4Shell, and padding-based evasion techniques exemplified by React2Shell, without emergency signature updates.

> *"Check Point WAF addresses modern web, API, and GenAI security challenges where legacy WAFs fail to address zero-day exploits, evasion techniques, and operational overhead. As part of the Hybrid Mesh Network Security family, it functions as an AI-driven WAAP platform for cloud-native applications."*
>
> ***- Anh Tien Vu***
> ***Industry Principal, Global Cybersecurity Practice***

Operating in-line and in real time, it automatically blocks malicious transactions, including injection attacks, cross-site scripting, bot activity, and API abuse. During the Log4Shell incident, users were protected without product updates because the AI engine recognized aberrant behavior at runtime. This reduces reactive patching and manual rule creation.

Check Point WAF also provides real-time API discovery and schema enforcement to reduce shadow API exposure. Integrated GenAI protection secures AI-powered interfaces and agent-driven workflows. Available as a SaaS service or via lightweight agents integrated with Kubernetes ingress controllers, gateways, and reverse proxies, it embeds security into DevSecOps pipelines and scales with continuous application changes. The solution provides rich visibility into application traffic, automatically discovers APIs, and enforces intended usage patterns to prevent abuse, validating APIs as a primary attack vector.

Ahead of the Curve: Unique Designs to Position Itself as an Innovator

Check Point WAF redefines modern WAF technology for cloud-native and AI-powered environments. Its dual-AI engine architecture replaces signature-based inspection with real-time behavioral intelligence, introducing a more efficient WAAP solution.

Unlike competitors that rely on rules or a single ML model, which often forces trade-offs between coverage and accuracy, Check Point WAF combines supervised and unsupervised AI to provide both breadth and precision. The supervised Attack-Indicator engine identifies known attack patterns and variants, while the unsupervised Context Analysis engine continuously learns each application's behavioral baseline. With full-payload inspection and real-time hyperText transfer protocol secure (HTTP/S) analysis, the 2 engines correlate findings to detect abuse and exploitation with high precision across distributed, API-driven environments. This approach achieves near-perfect detection with exceptionally low false positives, eliminating manual tuning cycles.

WAF Comparison 2026 testing reports balanced accuracy of 99.5% in the Critical profile and 99.3% in the Default configuration, outperforming hyperscaler-native and traditional enterprise WAFs that exhibit either higher false positives or reduced detection coverage. Built cloud-native from inception, Check Point WAF deploys as a lightweight containerized service or a fully managed SaaS. It integrates into CI/CD pipelines and distributes architecture using Helm charts, Terraform, and other infrastructure-as-code tools, enabling security updates alongside application releases.

> *"Unlike competitors that rely on rules or a single ML model, which often forces trade-offs between coverage and accuracy, Check Point WAF combines supervised and unsupervised AI to provide both breadth and precision. The supervised Attack-Indicator engine identifies known attack patterns and variants, while the unsupervised Context Analysis engine continuously learns each application's behavioral baseline."*
>
> ***- Anh Tien Vu***
> ***Industry Principal, Global Cybersecurity Practice***

The solution supports Kubernetes ingress, cloud gateways, and edge deployments via content delivery network (CDN) integration, lowering onboard effort and maintaining protection across multi-cloud environments.

Beyond detection, Check Point WAF unifies WAF enforcement, real-time API security, GenAI protection, bot mitigation, file inspection, intrusion prevention, and distributed denial-of-service mitigation in a single architecture. This consolidation reduces operational complexity and supports security platformization. Combined with Check Point's open-appsec initiative, which promotes transparency and community validation of its AI engine, Check Point WAF demonstrates an innovation trajectory aligned with the long-term evolution of application security.

In summary, Check Point WAF has positioned itself as an innovator through:

- **Dual-Layer AI Engines (Supervised and Unsupervised):** The platform provides near-100% threat detection with extremely low (<1%) false positives by combining pattern recognition with AI-powered behavioral analysis. This dual-engine approach achieves high security efficacy without the tuning trade-offs of other solutions.
- **Comprehensive WAAP Functionality:** Check Point WAF unifies web application firewall with API security (discovery and schema validation), bot management, distributed denial-of-service (DDoS) protection, file upload scanning, and intrusion prevention system (IPS) signatures in a single

platform. This consolidation replaces fragmented point products, reduces blind spots, and lowers administrative overhead.

- **Cloud-Native, DevOps-Friendly Design:** The solution supports containerized deployment, configuration-as-code policies, and integration with CI/CD and cloud services (e.g., AWS CloudFront and API Gateway). This architecture enables flexible and agile security implementation across modern environments.
- **Minimal Maintenance Through Automation:** The platform eliminates manual rule creation and signature updates via self-learning AI. It continuously adapts to application changes, significantly reducing false positives, emergency patches, and operational burden compared with legacy WAFs.
- **Open-Source Community Engagement (Open-appsec):** The initiative advances transparency and innovation through a community-driven model, enabling collective hardening of the engine and faster updates for new threats and techniques.

Gaining Trust and Popularity Through Proven Outcomes and Excellent Ownership Experience

Check Point WAF's architectural differentiation translates into measurable improvements in operational efficiency, application resilience, and enterprise risk posture. Organizations report substantial reductions in WAF-related overheads such as rule creation, fine-tuning, and life cycle management—enabling them to focus on new business and customer satisfaction instead of tool maintenance.

WAF Comparison 2026 testing also shows Check Point WAF delivers approximately a 99.5% threat detection rate with near-zero false positives, achieving balanced accuracy of 99.45%. This performance effectively reduces the traditional trade-off between security efficacy and application availability. With near-zero false positives, enterprises can operate confidently in full prevention mode, minimize alert fatigue, and significantly reduce manual rule refinement while maintaining business continuity.

Because malicious requests are automatically blocked at runtime, Check Point WAF reduces 'time-to-mitigation' gap that signature-based WAFs often have (waiting for a new rule or update, then tuning exceptions). This strengthens defenses against fast-moving campaigns and reduces exposure windows during zero-day exploitation.

By consolidating multiple WAAP functions into a unified AI-native platform and reducing manual maintenance, Check Point WAF lowers total cost of ownership (TCO) across the application security life cycle. Enterprises gain stronger protection, improved operational efficiency, and better utilization of security resources.

The near elimination of false positives also improves collaborations between security and development teams. Developers gain confidence to release faster without compromising security insurance by the solution. This outcome has driven adoption across large enterprises, including roughly half of the top 50 Fortune 500 companies, where low TCO and high efficacy are key decision factors.

Frost & Sullivan research indicates that organizations consistently achieve the following outcomes with Check Point WAF:

- **Dramatically Lower False Positives:** False positive alerts and unnecessary blocks drop by ~90–95%, essentially eliminating the alert fatigue.
- **Proactive Zero-Day Protection:** Organizations automatically stop zero-day attack attempts (including critical CVEs) with no emergency updates needed.
- **Faster Incident Response and Investigations:** Detailed request logging and contextual understanding enable teams to identify root causes and attack vectors within hours, reducing overall incident impact.
- **Operational Efficiency Gains:** Reduced rule management significantly lowers the administrative burden on SecOps and AppSec teams.
- **Enhanced User Experience and Uptime:** High detection accuracy improves application availability and end-user experience.

Check Point WAF extends innovation beyond detection performance by redefining the ownership model. Outcome-driven support emphasizes guided investigation, contextual remediation, and automation-enabled response workflows, accelerating time-to-protection while reducing the need for continuous manual involvement.

Flexible procurement models across partner ecosystems and cloud marketplaces further reinforce differentiation. Availability as both SaaS and lightweight agent-based deployment enables alignment with architectural and compliance requirements. Transaction-based pricing models designed for API-driven workloads enhance cost transparency compared to bandwidth-centric pricing prevalent among traditional WAF and content delivery network (CDN) vendors.

Strong technological innovation, comprehensive security features, and excellent service have resulted in significant adoption momentum and retention. The platform achieved triple-digit customer growth in 2025, expanding average deal sizes and accelerating SaaS uptake globally. High retention rates reflect sustained market confidence and validate its ability to deliver superior efficacy, reduced operational friction, and simplified life cycle management.

Conclusion

As traditional WAFs and application security tools struggle against modern threats, Check Point WAF is transforming web application security with a prevention-first, AI-driven approach. By integrating dual AI engines, comprehensive WAAP features, and cloud-native simplicity into a unified platform, it provides high-performance, automated, and context-rich security for web applications, APIs and GenAI applications. By converting continuous learning and runtime observability into instant, customized threat prevention with limited human intervention, Check Point WAF sets a new benchmark for what organizations should expect from a web application firewall in securing modern web applications and APIs in the cloud-native and AI era.

With its strong overall performance, Check Point earns Frost & Sullivan's 2026 Global Technology Innovation Leadership Recognition in the WAAP industry.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Recognition identifies the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Recognition Analysis

For the Technology Innovation Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

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

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Leveraging innovative technology characterizes the company culture, which enhances employee morale and retention

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 fueled 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)