WAAP Buying Guide

End-to-End Protection for Apps, APIs, and Infrastructure

What's WAAP?

Organizations that strive to deliver secure digital experiences will achieve competitive advantage by safely unleashing application innovation that delights customers.

However, changing dynamics in the way applications are designed and deployed have expanded the threat surface and have necessitated a paradigm shift in the way security is delivered.

Efforts to stay ahead in a digital-first world by leveraging modern app development, agile methodologies, and automation are derailed by sophisticated attackers that compromise and abuse apps and APIs, resulting in data breach, downtime, account takeover (ATO), and fraud. This is further exacerbated by strict security controls that inadvertently frustrate customers and burden InfoSec teams with alerts that turn out to be false positives.

Security and risk management leaders need to defend the business by protecting apps and APIs while operating at the speed of business. Friction, manual tuning, and time-consuming remediation needs to be minimized and customer experience optimized.

As a result, more organizations are considering cloud-delivered, as-a-Service solutions to help manage the complexity of securing digital experiences. Namely, Web App and API Protection, or WAAP.

Applications are increasingly evolving toward highly distributed multi-cloud architectures. This paradigm shift in the way apps are designed and deployed introduces new architectural risks. Apps and APIs are only as secure as the infrastructure on which they run; end-to-end protection is a must-have for multi-cloud security.

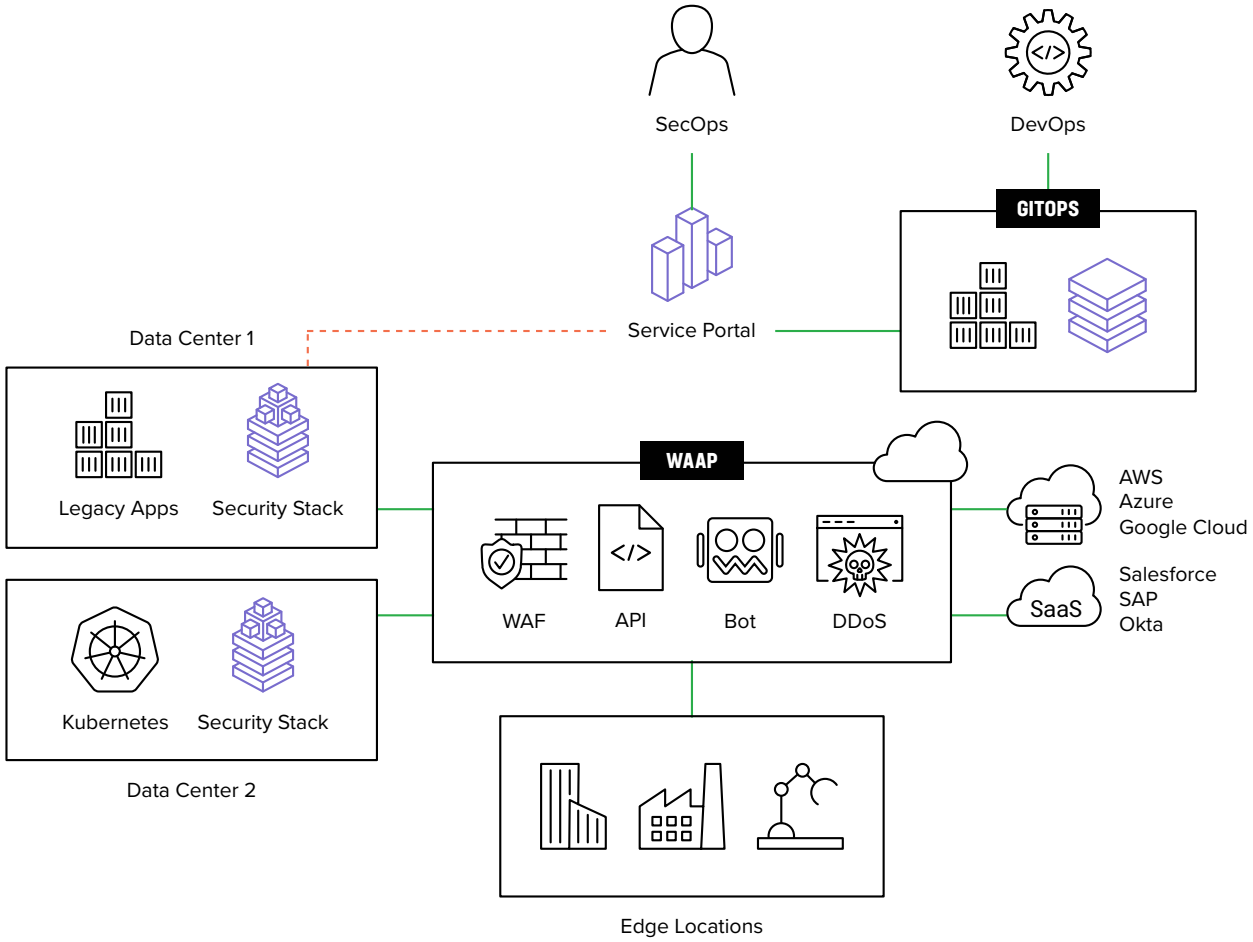


Figure 1: Web App and API Protection

Why Do Organizations Need WAAP?

Business leaders are grappling with unprecedented change and uncertainty as the pace of digital transformation continues to accelerate, serving as a forcing function to better align and strengthen alliances across security and application teams. The complexity of managing both legacy and modern apps has led to friction between security and apps teams, customer frustration, and an opportunity for attackers

Complexity

The biggest challenge is complexity, brought on by a proliferation of architectures resulting from a constant need to deliver capabilities and features to gain competitive advantage.

For example, the pressure to innovate quickly has resulted in large-scale adoption of third-party integrations via APIs, which can introduce unknown risks to the business.

The number of APIs worldwide, public or private, is already approaching 200 million.[1]

Legacy and Modern Apps

Architectural decentralization and modern software development has led to an array of assets that must be secured, significantly increasing the risk of compromise as organizations maintain legacy applications as well as new digital catalogs.

While three-tier custom web stacks in the data center still have a place, cloud, microservices, and container technologies—like APIs—have facilitated an explosion of innovation that application teams leverage to improve their digital capabilities.

Friction and Frustration

Security teams can struggle to keep up with rapid feature and code releases that leverage open source and third-party components, leading to missed opportunities and internal friction.

With so many ways to buy in the digital economy, customers have become intolerant of friction from excessive authentication that inhibits their ability to transact.

Customer expectations are also driving digital touchpoints to be deployed closer to the edge, as any performance hiccup may result in transaction, revenue, and even brand abandonment.

Businesses that remove last mile digital friction will see customer and revenue growth.[2]

Attacker Economic

The complexity of managing legacy and decentralized modern apps has made the economics of cybercrime more attractive. A constant cadence of vulnerabilities, weaponized exploits, and compromised credentials continues to expand the threat surface, and sophisticated automated tools and readily-available botnet infrastructure provide attackers with an attractive ROI for their efforts. The most sophisticated criminals and state actors are not easily deterred and constantly retool to evade detection.

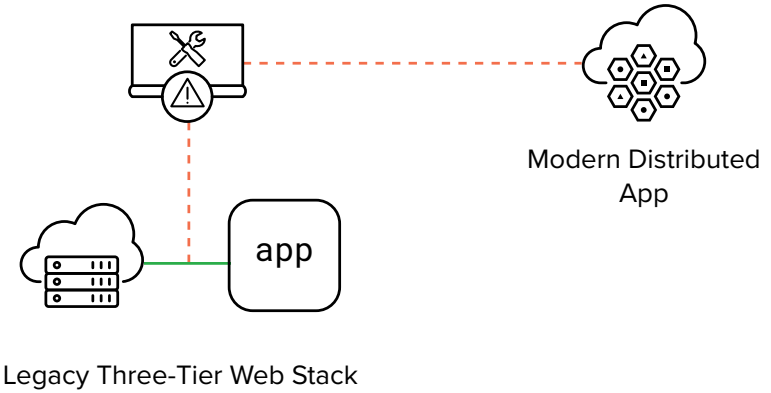


Figure 2: Complexity driven by architecture decentralization dramatically expands the threat surface

Analysis of 100 largest events of the past 5 years show web app attack fallout at $10 billion.[3]

What Makes WAAP Effective?

There is a clear opportunity for organizations that leverage security as a competitive advantage to protect the business and satisfy customers. By integrating security into development frameworks, deploying it consistently across architectures, and continuously adapting, the business can focus on earning and engaging customers.

Visibility

Deployment

Effective and easy-to-operate security deploys consistently across clouds and architectures, integrates into CI/CD pipelines, and updates with continuous threat intelligence.

Policy Tuning

Adaptive security that reacts as apps and attackers evolve continuously mitigates risk from compromise and abuse.

Enforcement

Discovery

Dynamic API discovery with anomaly detection and behavioral analysis protects against unintended risk in the new digital economy.

Authentication

Accurate and durable telemetry with highly-trained AI removes the need for strict security challenges that frustrate the customer experience.

Remediation

Automatic false positive suppressionand insight correlation across threat vectors minimizes operational burdens and allows InfoSec to focus on risk and incident response.


Visibility
Deployment
API and CI/CD Driven
Discovery
Automatic identification and enforcement
Policy Tuning
Self-learning adaptive security
Authentication
ML-based frictionless authentication
Remediation
Insight correlation across threat vectors
Enforcement

What Makes the Best WAAP?

Effective Security

The best WAAP maintains resilience with minimal friction and false positives through real-time mitigation, retrospective analysis, and adaptive security.

- Robust security, threat intelligence, and anomaly detection protects all apps and APIs from exploits, bots, and abuse to prevent compromise, ATO, and fraud in real-time.
- Correlated insights across multiple vectors and ML-based evaluation of security events, login failures, policy triggers, and behavioral analysis enables continuous self-learning and retrospective analysis.
- Autonomous security countermeasures that react as attackers retool deceives and convicts bad actors without relying on mitigations that disrupt the customer experience.

Easy-to-Operate

The best WAAP provides self-service deployment with low operational complexity through simple onboarding, automated protection, and interactive reporting.

- Self-learning and self-tuning security integrates into event management and CI/CD ecosystems to reduce the burden on InfoSec, DevOps, and AppDev teams.
- Dynamic discovery and policy baselines enable auto mitigation, tuning, and false positive remediation throughout the development/deployment lifecycle and beyond.
- A suite of security dashboards with contextual drill-down maximizes the power of insight correlation for incident response and forensics.

Distributed Platform

The best WAAP provides universal visibility and consistent policy enforcement across all clouds and architectures.

- Insertion points for data center, cloud, container, and CDN facilitate a comprehensive view of the entire application portfolio.
- Declarative policy abstracts underlying infrastructure to prevent misconfiguration.
- Security deploys on-demand where needed for consistent protection from app to edge.

Infrastructure Protection

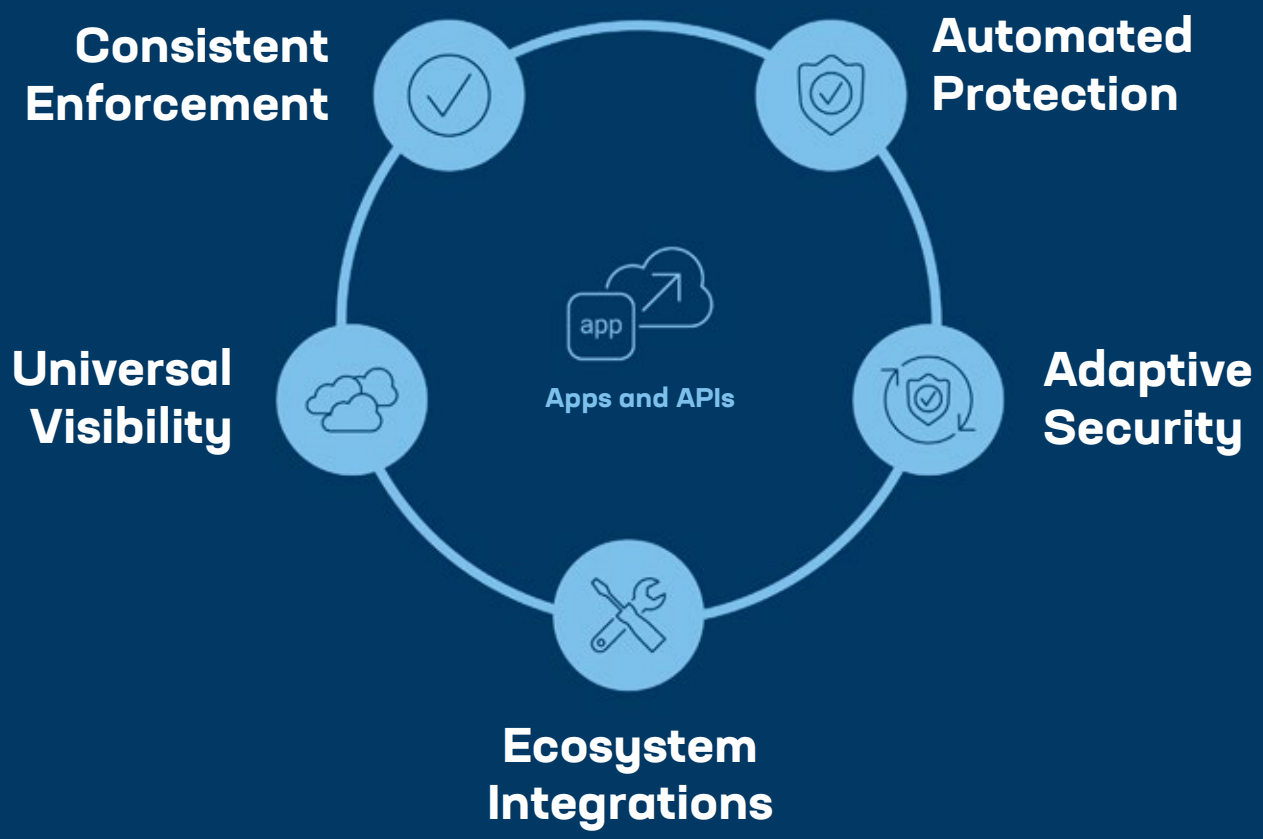
The best WAAP includes comprehensive defense of the architectural components your apps and APIs depend on.

- Visibility across cloud-native infrastructure and the full application stack.
- Infrastructure hardening at scale with resilient network and session protocol security, policy-based decryption, and intelligent traffic steering.
- Detection of vulnerability indicators and mitigation through behavioral analysis, ML-generated context, and actionable insights.


Easy-to-operate
Distributed Platform
Effective Security
Infrastructure Protection

Key Elements of an Effective WAAP

The best WAAP solution provides universal visibility and consistent policy enforcement across hybrid, multi-cloud infrastructure and the full application stack, using automated protections and adaptive security to maximize efficacy and efficiency of existing security investments.



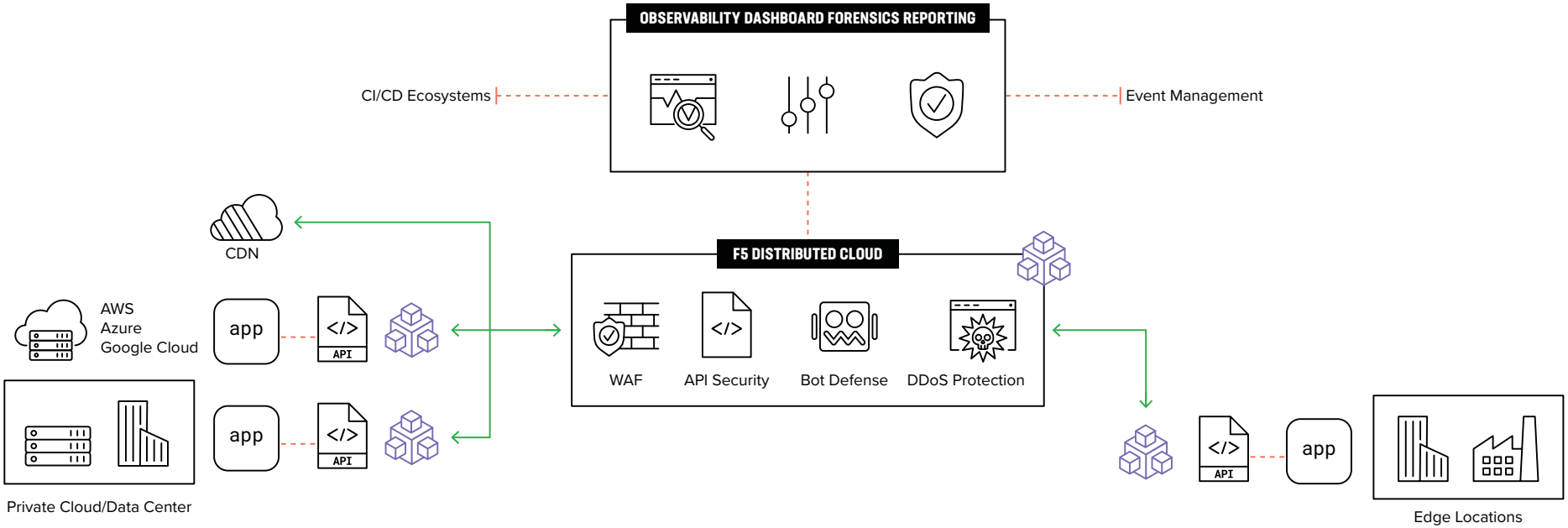


Figure 3: F5 Distributed Cloud WAAP

Conclusion

Inevitably, new vulnerabilities will surface and attackers will develop exploits to capitalize on weaknesses in distributed application architectures. Complex software supply chains, open-source software proliferation, and automation via CI/CD pipelines increase the risk of devastating vulnerabilities. Early detection and remediation are critical to mitigate weaknesses in software, critical protocols, and underlying infrastructure.

A platform with adaptive security can protect applications and APIs across clouds and architectures, and continuously react as apps change and attackers retool, freeing InfoSec from custom authentication rule management and false positive remediation. This allows security and risk management leaders to defend the business while supporting digital innovation.

F5 Distributed Cloud Services provide universal visibility, consistent enforcement, automated protection, adaptive security, and ecosystem integration across the entire application portfolio—protecting apps and APIs while preserving business agility and customer experience.

Shift the perspective of security from a cost center to a digital differentiator by effectively balancing protection and usability to deliver compelling digital experiences while reducing costs and complexity.

Appendix

[1] Rajesh Narayanan and Mike Wiley, "Continuous API Sprawl: Challenges and Opportunities in an API-Driven Economy," F5 Office of the CTO Report (2021) https://www.f5.com/pdf/reports/f5-office-of-the-cto-report-continuous-api-sprawl.pdf

[2] "The New Business Imperative: Adopting Cross-Functional, Cost-Out and Revenue-In Capabilities," F5 White Paper (2021) https://www.f5.com/pdf/shape-security/shape_the_new_business_imperative_2020.pdf

[3] Cyentia Institute, "State of the State of Application Exploits in Security Incidents," F5 Labs (July 20, 2021) https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security-incidents

[4] "State of Application Strategy Report 2021," F5 Report (2021) https://www.f5.com/state-of-application-strategy-report

ABOUT F5

F5's portfolio of automation, security, performance, and insight capabilities empowers our customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users.

Find more banking and financial service resources at **f5.com/solutions**