EXECUTIVE SUMMARY

Adaptive Security Engine: A Smarter Foundation for Web and API Protection

Modern web applications and APIs are increasingly complex, built on microservices, serverless architectures, and hybrid cloud environments. This complexity widens the attack surface, which has 292,000 known vulnerabilities and counting. Threat actors exploit these vulnerabilities through automated bots, zero-day exploits, DDoS, and API abuse campaigns.

Akamai Adaptive Security Engine is the intelligence behind our leading web application and API protection (WAAP) solution, powering real-time, always-current defenses against application-layer attacks. This breakthrough technology has positioned Akamai's WAAP solution as a consistent leader across analyst reports, efficacy benchmarks, and real-world customer results. Designed for both performance and precision, Adaptive Security Engine uses smart and robust attack detection logic to identify and mitigate attacks with velocity and precision, without adding operational overhead to maintain up-to-date protections as the attack landscape evolves. With an AI-powered automated false-positive detection system, protections can be tuned further to your environment and traffic patterns.

Critically, Adaptive Security Engine is also built for trust. Its core algorithms are proven and compliant with strict regulatory frameworks, making it ideal for security-conscious organizations that require transparency and control. With the rapid innovation of AI, Adaptive Security Engine continues to advance, providing AI-powered event investigation, enhanced actionable insights, and swift attack detection.

With Adaptive Security Engine, security evolves automatically, freeing your team to focus on what matters most. It's not just smarter protection. It's a smarter way to run security.

Always learning, always protecting: Intelligent defense for modern apps

Adaptive Security Engine stands out for its ability to fuse advanced analytics and automation into a cohesive system built on four core pillars that drive smarter, faster protection:

- **AI-powered system** that augments accurate and customized defenses
- **Advanced automation** that implements protections without manual effort
- **Live edge analysis** of every request to speed protection and minimize latency
- **Global and local intelligence**, informed by 400+ Akamai security professionals and threat researchers

Together, these technological pillars enable near-zero-touch security by automatically recommending and implementing optimized protections for each customer environment.

Beyond the stats: Adaptive in every layer

Adaptive Security Engine incorporates additional context from global traffic patterns, application behaviors, and end-client information for efficient outcomes across varied applications and APIs. It adapts to:

- **Identify** anomalous behavior
- **Tune** protections to each customer's traffic
- **Anticipate** new and evolving attack types

This means Adaptive Security Engine intelligently customizes protections for your application's unique context, making it a smarter way to secure modern applications. It replaces manual tuning with automation, broad generalizations with contextual specificity, and static detections with fluid protections — all delivered at the edge.

At launch, Adaptive Security Engine doubled detection rates and reduced false positives fivefold compared to legacy rulesets. Recent machine learning model improvements have cut false positives by an additional 4x.

In third-party testing by SecureIQ, Adaptive Security Engine achieved a 100% false-positive avoidance score and was recognized as a leader among cloud WAAP providers.

Real-time risk scoring at the edge

Every day, Akamai sees more than 1.3 billion client interactions across its global platform. This unmatched visibility powers Adaptive Security Engine, which ingests and analyzes traffic data to detect anomalies, refine protections, and inform decision-making.

Instead of relying on binary allow/block rules, Adaptive Security Engine uses a multidimensional threat scoring model that evaluates:

- Global threat intelligence
- Application-specific traffic behavior
- Per-request data (headers, paths, payloads, parameters)

This enables a high-resolution, real-time understanding of risk that's tailored for each request

Detecting what others miss

Adaptive detections are especially effective against evasive, targeted, and stealthy attacks. These attacks often bypass traditional WAF rulesets by mimicking normal traffic or probing for edge-case vulnerabilities. Adaptive Security Engine is designed to recognize the subtle patterns and anomalies that characterize these threats, even as adversaries iterate using GenAI-enhanced tools and techniques.

Because the threat landscape is evolving fast, and the tools to generate attacks are more accessible than ever, Adaptive Security Engine evolves too. Since the detections are built to identify different forms of common and sophisticated attacks in flight versus exploitation of each vulnerability of specific technologies, the protections are comprehensive and frequently effective against zero-day vulnerabilities.

Inside Adaptive Security Engine: Adaptive Intelligence

These detection capabilities come together in what Akamai calls Adaptive Intelligence, the decision-making layer within Adaptive Security Engine that analyzes each request and adjusts protections dynamically.

By combining flexible threat scoring, behavioral signals, and anomaly detection, Adaptive Intelligence evaluates traffic in context and fine-tunes security responses in real time, all while minimizing false positives.

Adaptive Intelligence analyzes factors such as:

- Anomaly scores and threat intelligence ratings
- Selector name inference
- Popular coding characteristics

By evaluating each request through this multi-signal lens, Adaptive Security Engine can confidently differentiate between true threats and legitimate user activity, even as attackers evolve their tactics.

Why false positives matter

False positives aren't just an operational nuisance, they're a business risk. Overblocking legitimate users can disrupt services, impact revenue, and erode trust.

Traditional WAFs often rely on rule-level exceptions to reduce false positives, but these static workarounds must be reviewed, retuned, and retired as traffic and attack techniques evolve. Adaptive Security Engine removes this burden by making adaptive, context-aware decisions per request. In fact, internal analysis shows that exception abuse occurs in 23% of customer-generated static rule exceptions, compared with just .02% for Adaptive Security Engine's smarter, context-aware exceptions embedded in Adaptive Intelligence — about a 1,000x improvement in precision.

Exception type	Total requests	Attacks ASE missed (exception abuse)	Missed attack %
Customer	18,994,618	4,402,872	23%
Adaptive Intelligence	3,027,090	687	.02%

Akamai uses Balanced Accuracy, or the average of true positive and true negative rates, as a benchmark. It reflects how well Adaptive Security Engine maintains high security without overblocking. In internal and third-party testing, Adaptive Security Engine consistently scores among the highest for this metric, delivering confident protection without collateral damage.

Staying ahead of the attack

Today's attackers don't just throw one payload and leave. Opportunistic threat actors may run large automated scans, such as hundreds of SQL injection attempts in minutes, and move on if blocked. But more determined attackers follow a stepwise methodology similar to the Cyber Kill Chain, adapting their payloads based on response feedback. These actors will manually test, tweak, and obfuscate attacks until they succeed or are shut down.

That's where Adaptive Security Engine delivers a key advantage. Rather than relying on static rules, Adaptive Security Engine modifies protections on the fly, based on the characteristics of each request. It analyzes signals such as anomaly scores, threat intelligence ratings, parameter names, path structures, and common attackers, as well as coding practices and more, as they happen.

This makes Adaptive Security Engine especially effective at catching stealthy, evasive attacks, even when adversaries modify their tactics midstream. By combining global insight, request-specific analysis, and live scoring, Adaptive Security Engine helps security teams disrupt attackers mid-strategy without manual intervention — even when adversaries shift tactics.

Penalty Box: Stopping active attack sessions faster

While adaptive scoring prevents many threats from escalating, some attackers persist. To contain these active attack sessions, Adaptive Security Engine uses another powerful tool: the Penalty Box.

Once Adaptive Security Engine detects a request that triggers a "Deny" action (for example, part of a SQL injection campaign), the client is placed in the Penalty Box for a temporary period of time. During that time, any further requests from the same IP are automatically blocked, regardless of individual detection logic. This forces attackers to either give up or shift to different IPs, significantly increasing attacker cost and reducing their ability to probe and evade.

Combined with Adaptive Security Engine's adaptive scoring, the Penalty Box helps deliver a two-pronged defense:

1. **Precision blocking:** Real-time decisioning based on multiple risk factors
2. **Active attack session disruption:** Automated escalation against persistent threats

All of this happens at the edge, automatically, and with highly reduced manual tuning requirements. The result: Security teams gain smarter protection with less operational overhead, and attackers encounter a defense that adapts and strikes back in real time.

Adaptive protection that works for the business

Adaptive Security Engine represents the latest evolution of Akamai's WAF detection strategy, built on more than a decade of experience with the Core Rule Set (CRS) and Kona Rule Set (KRS). This evolution reflects a deeper shift in how modern security must operate dynamically by design.

By combining real-time behavioral intelligence, automation, and global visibility, Adaptive Security Engine helps organizations:

- **Reduce** false positives and alert fatigue
- **Simplify** operations with automatic updates
- **Deliver** consistent, secure user experiences
- **Scale** securely without scaling security headcount

That's why more than 96% of the 700,000+ hostnames currently using Adaptive Security Engine run in Automatic mode. In a threat landscape that changes by the minute, Adaptive Security Engine offers resilient, adaptive protection that meets the needs of both your security team and your business.

For clients seeking a more technical white paper with hands-on guidance covering implementation details, configuration best practices, and integration scenarios, please contact your Akamai account representative.

Looking for more technical depth? Explore our product page for implementation details and best practices, and take advantage of our free migration and protection offer.