

Akamai Workforce Protector (Formerly LayerX)

Secure human and AI agent interactions in the browser

Our workspace has changed

Work has moved to the interaction layer, fundamentally breaking traditional security models. As organizations rapidly adopt AI tools, copilots, and web-based workflows, the enterprise threat surface is expanding faster than ever before. Per Forrester, more than 70% of corporate work occurs within a browser,¹ as employees frequently execute business-critical tasks inside encrypted browser sessions, accessing SaaS apps, pasting sensitive data into public AI chatbots, and installing third-party extensions. Because this activity happens at the point of interaction, long before data touches the network, traditional proxies and legacy data loss prevention (DLP) tools cannot see it. This widening gap leaves organizations with no visibility into their most critical vulnerabilities, forcing them to navigate the risks of shadow AI (or even to block AI interactions altogether), and face compliance violations and data leakage without a reliable control point where work actually happens.

The Problem: Why secure access is harder than it seems

The in-session blind spot

Work has moved into AI tools, SaaS applications, and web environments where users and AI agents interact with sensitive data in real time. Legacy security architectures were not designed for this shift. Network controls, existing secure access service edge (SASE) tools, and security service edge (SSE) tools cannot inspect encrypted, dynamic application traffic effectively, and endpoint tools lack granular visibility into user behavior. This creates a massive in-session blind spot. Traditional DLP and proxies cannot see critical interactions — like copy-and-paste activity, screenshots, file transfers, and text input, because they occur inside the browser, long before the data ever touches the network.

The accelerating risk of shadow AI

AI adoption is accelerating faster than governance capabilities. Employees increasingly turn to unapproved generative AI tools, browser-based LLMs, and embedded AI assistants inside SaaS apps. Because this “shadow AI” activity is invisible to traditional security controls, employees frequently paste proprietary source code, customer records, and internal documents directly into unmanaged AI systems, creating silent compliance and intellectual property risks.

Key features

AI usage control

Secure every interaction of humans and AI agents. Apply real-time guardrails to control prompts, responses, and data copy/paste exactly at the point of intent.

AI usage governance

Discover shadow AI, embedded widgets, and unmanaged agentic workflows. Map your complete AI attack surface to enforce consistent enterprise compliance.

Zero Trust browser security

Securely transform any browser into a managed workspace. Instantly verify identity and device posture to govern access to SaaS and private apps without forcing a browser swap.

Extension governance

Automatically analyze risk scores, permissions, and behaviors to instantly block malicious third-party plug-ins using native ExtensionPedia intelligence.

Data loss prevention

Enforce session-level protection against unauthorized data movement across SaaS, web, and private apps, eliminating the visibility gaps of network perimeters.



¹ Forrester Research Inc., Digital Workplace And Employee Technology Survey, 2025, May 2025

The third-party and BYOD challenge

Modern work happens outside tightly controlled corporate environments, but most security tools still depend on managed devices. Organizations struggle to enforce consistent security policies and secure third-party access for contractors, business process outsourcers, and bring-your-own-device (BYOD) users. Securing these unmanaged devices has traditionally required expensive deployments, which introduce friction and operational overhead.

The hidden threat of browser extensions

As the browser becomes the primary work interface, it also becomes the primary attack vector. Third-party browser extensions pose a significant and growing risk due to their elevated permissions and access to corporate identities, session cookies, and user input. A compromised or overprivileged extension can read keystrokes, access enterprise apps, or seamlessly exfiltrate data.

The lose-lose compromise of current tools

Enterprises have historically been forced into a lose-lose compromise: Legacy network security platforms offer low friction but suffer from critical blind spots, relying on blunt “allow” or “block” decisions that miss data leakage at the point of interaction. Conversely, full-stack enterprise browsers provide deeper visibility but demand a highly disruptive trade-off: forcing organizations to completely “rip and replace” the tools their employees already use. This introduces massive change management hurdles, privacy concerns, and fierce end-user resistance.

The Solution: Enterprise browser control. On any browser.

Akamai Workforce Protector (formerly LayerX) is pioneering true interaction security by delivering a frictionless browser extension that securely transforms any browser into a fully managed workspace. You gain the deep, end-to-end security of a dedicated workspace platform without ever forcing a browser swap or disrupting the user experience.

AI usage control

Built on this secure workspace foundation, Akamai Workforce Protector extends its real-time visibility to govern how employees, AI agents, and vendors interact with AI. To safely accelerate AI adoption, organizations need end-to-end governance for AI usage. Workforce Protector performs comprehensive shadow AI discovery across the web and captures full AI conversations. It applies real-time AI data security to text inputs, file attachments, and copy/paste operations directly at the browser. By inspecting and controlling data at the exact moment it is entered into AI tools, Workforce Protector prevents intellectual property loss and regulatory violations right at the source.

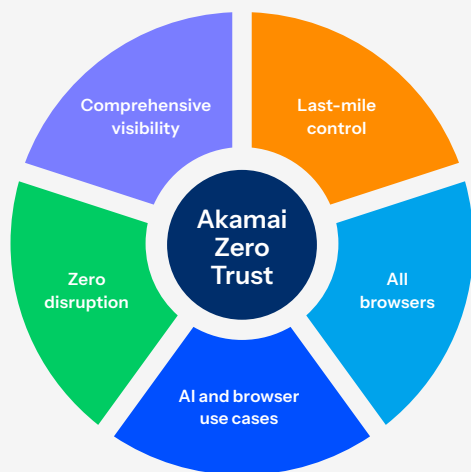
Securing the entire workspace surface

Workforce Protector establishes the browser as a secure, enterprise-controlled workspace for all daily tasks. It secures the entire interaction layer by delivering:

- **Browser-native DLP:** This monitors data in motion natively in the browser without relying on complex network decryption, such as utilizing file sandboxing to isolate and inspect sensitive uploads and downloads.

- **Automated compliance:** Workforce Protector features one-click automated enforcement of CIS Benchmarks across major browsers, ensuring continuous configuration compliance.
- **Unmanaged device support:** For BYOD and third-party contractors, the extension seamlessly enforces read-only sessions and watermarking without requiring heavy device management deployments.
- **Extension risk elimination:** A native extensions risk database automatically analyzes risk scores, behaviors, and permissions to instantly block malicious or overprivileged third-party browser plug-ins.

Take control of your interaction layer



Happy users. Happy security. Happy IT.

Workforce Protector delivers measurable security and architectural savings from the first hours of deployment, balancing robust protection with a frictionless end-user experience. Users maintain their preferred browsers and native workflows, with zero performance degradation or latency introduced into daily tasks. IT and security teams achieve unmatched time to value with rapid deployment that requires no complex network rerouting or downtime, hardware appliances, or proxy configurations.

To learn more about how Akamai Workforce Protector can safely accelerate your AI adoption without slowing down your business, visit akamai.com/akamai-workforce-protector.

Akamai API Security

Govern and protect every API, from code to runtime

Akamai API Security gives organizations a reliable system of record for API risk. By discovering APIs (from traffic, specifications, and code), assessing posture, detecting runtime abuse, testing APIs before deployment, and mapping findings to owners and remediation context, Akamai helps teams reduce API exposure across the full lifecycle, from code to runtime.

APIs are the connective tissue of modern digital business. They connect customers, partners, applications, data, automation, and AI-enabled workflows. They also expose the business logic and sensitive data attackers want to exploit.

The challenge is that APIs change constantly. They appear in code before they appear in production. They run across clouds, gateways, mobile apps, partner ecosystems, and internal services. Some are managed. Some are forgotten. Some expose sensitive data. Some power AI services. Some operate outside the visibility of existing controls.

Attackers are changing, too. Frontier LLMs, AI agents, and automated tooling make it easier to discover weak paths, test business logic, exploit shadow APIs, and scale abuse faster than security and application teams can respond. This does not change why APIs are targeted. It changes the speed and scale at which attackers can find and abuse them.

With Akamai, security teams can understand what APIs exist, how they are used, where risk lives, who owns the fix, and how to address API weaknesses before they lead to data exposure, fraud, or disruption.

How Akamai API Security helps

- **Establish a comprehensive API inventory**
Akamai provides visibility into the full API landscape by discovering APIs and MCPs across diverse environments, including runtime traffic, cloud infrastructure, gateways, specifications, and source code repositories. By surfacing managed, shadow, zombie, and AI-driven endpoints, Akamai helps security teams eliminate blind spots and understand exactly what is exposed publicly or internally.
- **Govern API posture and compliance**
Akamai helps teams move from reactive API issue management to policy-driven API governance. Security teams can assess API posture, identify policy violations, track improvement over time, and map API findings to over 10 compliance frameworks and best practices.
- **Detect runtime abuse and business logic risk**
API attacks often use valid credentials, legitimate API calls, and normal-looking workflows. Akamai analyzes API behavior to detect suspicious activity, abnormal usage, sensitive data exposure, authorization gaps, partner misuse, and business logic abuse. This allows security teams to identify risky behavior that static controls may miss and use enforcement points such as WAAP, gateways, or response workflows to reduce impact.

Akamai API Security benefits

Reduce API risk across the business

Gain a clearer view of API exposure, sensitive data access, ownership, posture, and runtime behavior.

Improve resilience

Identify risky APIs and suspicious behavior before they result in data exposure, fraud, downtime, or business disruption.

Strengthen governance and compliance

Turn API findings into measurable posture, policy alignment, and evidence for audit, regulatory, and executive risk conversations.

Accelerate remediation

Map API risks to owners, repositories, file paths, and code context, where available, so teams can fix issues faster.



- **Connect API risk to code and owners**

Akamai connects runtime and posture issues to the development context, such as repository, file path, and last committer. This allows security teams to reduce MTTR, eliminate ownership ambiguity, and give developers the evidence they need to fix API issues faster.

- **Test APIs before production**

Akamai helps teams test APIs before they reach production. Active API security testing can run pre-production, on demand, or as part of CI/CD workflows to identify vulnerabilities, policy gaps, and OWASP API risks earlier in the lifecycle. Organizations can reduce production exposure and improve API security coverage without relying on manual testing alone.

Built for modern applications and AI security

Akamai API Security is part of the Akamai Application Protection Platform, giving organizations a practical path to defense in depth across applications, APIs, automation, and AI-enabled workflows. When paired with Akamai App & API Protector, API Security extends WAAP with deeper API and MCP discovery, posture governance, runtime behavior analysis, testing, compliance visibility, and remediation intelligence. App & API Protector provides inline protection for relevant traffic, while API Security helps teams understand and govern API risk across the lifecycle.

Akamai API Security benefits

Secure APIs earlier

Test APIs before deployment to uncover vulnerabilities, policy gaps, and OWASP API risks before they reach production.

Support safe AI adoption

Automatically discover AI-related API endpoints, including LLM, GenAI, and MCP-related APIs, so teams can understand where AI-driven interactions enter the environment.

Extend WAAP protection

Pair Akamai API Security with Akamai App & API Protector to combine deeper API lifecycle governance with inline enforcement for relevant traffic.

Ready to see which APIs you actually expose?

Contact **Akamai** to learn how Akamai API Security can help you discover, govern, test, and protect APIs from code to runtime.

Akamai API Security Active Testing

Continuous automated API security penetration testing

Akamai API Security Active Testing continuously simulates real attack paths against your APIs to find vulnerabilities that scanners and periodic penetration tests often miss. It helps AppSec, DevSecOps, and development teams deliver safer API implementations quicker to market.

APIs change faster than traditional security testing can keep up. New endpoints appear with every release. Authentication flows become more complex. Business logic changes across environments. AI-assisted development accelerates API creation and increases the amount of code that may look correct but has not been validated in real-life conditions.

Active Testing helps teams close that gap. It is not another scanner, and it is not a replacement for manual penetration testing. It fills the space between them, continuously and automatically pentesting APIs by simulating realistic attacks, validating exploitability, and giving teams the evidence they need to fix issues before release.

Why Akamai API Security Active Testing is different

It fills the gap between scanners and pentests

Scanners are useful for crawling, fuzzing, and input validation, but they often miss API risks that depend on authorization, workflow order, object access, and business logic. Manual pentesting goes deeper, but it is periodic and hard to scale across every API and release. Active Testing gives teams automated, continuous, and repeatable API security testing that keeps pace with development.

It validates real-world exploitability

Code analysis and static tools can point to possible issues, but they cannot tell how an API behaves with real authentication, state, dependencies, and business logic — resulting in a lot of false-positive noise. Active Testing sends real traffic to APIs under test (using simulated but realistic conditions), helping teams confirm whether an issue is actually exploitable and giving developers clearer evidence to understand, reproduce, and fix it.

It is built for how APIs actually break

APIs are often exploited through broken object access, weak authorization, excessive data exposure, partner misuse, workflow abuse, and multistep interactions, not just malformed input. Active Testing is designed to test those API-specific paths so teams can find vulnerabilities that traditional web application scanners often miss.

Akamai API Security Active Testing benefits

Find vulnerabilities scanners miss

Simulate API-specific attack paths to uncover authorization gaps, business logic flaws, and multistep workflow risks.

Extend the value of pentesting

Increase API security coverage between manual engagements with continuous, repeatable testing.

Build fast and fix continuously

Run tests during development and pre-production, on demand, on a schedule, or through CI/CD workflows.

Validate real exploitability

Prioritize issues based on runtime-tested evidence instead of theoretical findings.

Give developers actionable proof

See affected endpoints, triggered tests, reproduction context, and business risk so teams can fix issues faster.

Support AI-era development safely

Active Testing capabilities are exposed through MCP so AppSec and development teams can use agents and AI coding assistants to run tests, analyze evidence, and accelerate remediation with suggested code fixes.



How Akamai API Security Active Testing helps

Test APIs before they reach production	Simulate API-specific attack paths	Reduce setup friction	Give developers evidence they can act on
Run API security tests in lower environments, pre-production, and controlled production scenarios. Teams can test APIs on demand, on a schedule, or as part of CI/CD workflows.	Test APIs the way attackers abuse them, including workflows, authorization gaps, object access patterns, and business logic paths.	Onboard APIs from specifications, Akamai API Security inventory, or AI coding assistant workflows. Run scans using Akamai-managed SaaS workers, customer-managed remote workers, CI/CD workflows, or scheduled testing.	Show which endpoint is affected, what test triggered the issue, why it matters, and how teams can reproduce or validate the risk. Use agents and AI coding assistants to interpret testing findings and suggest code fixes faster.

Part of Akamai API Security

Active Testing is part of Akamai API Security, helping teams connect API discovery, posture, runtime behavior, testing, and remediation. When used with Akamai API Security inventory, teams can prioritize which APIs to test first and identify which issues should be fixed before release. With MCP, teams can also bring Active Testing functionality and evidence into the agents and AI coding assistants developers already use.

Test APIs before attackers do

Visit [Akamai.com](https://akamai.com) to learn how Akamai API Security Active Testing can help your teams continuously validate API security, uncover exploitable risks, and reduce exposure before deployment.

App & API Protector

In today's connected world, protecting web applications and APIs from the wide range of emerging and evolving threats is critical for business success. However, securing digital interactions amid cloud journeys, modern DevOps practices, and constantly changing applications introduces new complexities and challenges.

Deploying an all-encompassing web application and API protection (WAAP) solution strengthens your security posture by adaptively updating protections and proactively delivering insights on targeted vulnerabilities.

Akamai App & API Protector is a single solution that brings together many security technologies, including web application firewall (WAF), bot mitigation, API protections, and distributed denial-of-service (DDoS) protection. App & API Protector is recognized as a leading WAAP solution for swiftly identifying and mitigating threats beyond the traditional WAF to protect entire digital estates from multidimensional attacks. The platform is easy to implement and use, provides holistic visibility, and automatically implements up-to-date, customized protections via Akamai Adaptive Security Engine.

Extend WAF security with Akamai App & API Protector Hybrid

Built to secure distributed applications, App & API Protector Hybrid extends Akamai's proven, core WAF capabilities beyond our platform for consistent security across applications and APIs deployed in various environments, including on-premises, multicloud, and off-CDN infrastructures.

The power of adaptive security

App & API Protector goes beyond rulesets with the Adaptive Security Engine. With this innovative technology, security protections are continually and automatically updated, with customized policy recommendations implemented in a single click. The Adaptive Security Engine provides modern protection by combining machine learning, real-time security intelligence, advanced automation, and insights from more than 400 security professionals and threat researchers. Adaptive Security Engine is unique because it:

- Analyzes the characteristics of every request in real time at the edge for faster detection
- Learns attack patterns by using both local and global data to make customer-specific protection adjustments
- Adapts to future threats, which ensures updated protections even as attacks evolve

Benefits for your business

-  **Trusted attack detection**
Evolve with the threat landscape; protect against established and emerging threats, including DDoS, botnets, injections, application and API attacks, and more
-  **One product, broad protections**
Maximize your security investment with a solution that includes WAAP, bot visibility and mitigation, DDoS protection, security information and event management (SIEM) connectors, web optimization, API acceleration, and more
-  **Hands-off security**
Alleviate time-intensive manual maintenance with automatic updates and proactive self-tuning recommendations powered by Akamai Adaptive Security Engine
-  **Ease of use**
Use the improved UI design to simplify onboarding and comprehensive security operations, which are aided by setup and troubleshooting guides
-  **Unified visibility**
Analyze your full scope of security metrics in a single dashboard or proactive discovery report via the shared telemetry of Akamai's security solutions



Adaptive Security Engine alleviates the burden of time-consuming, manual tuning with zero-touch updates for a nearly hands-off experience. At launch, this technology was proven to increase detections by 2x and reduce false positives by 5x. Recent updates to our machine learning-powered algorithms now reduce false positives by an additional 4x. Security professionals can be heroes again, with more time to focus on enabling secure — and customer-friendly — digital business operations.

New: Behavioral DDoS Engine

The new Behavioral DDoS Engine both strengthens and simplifies application-layer DDoS defense and is powered by machine learning. Behavioral DDoS Engine's behavioral- and anomaly-based detection algorithms look at various traffic dimensions like country source, network fingerprint, and other HTTPS request attributes to create tailored protections and provide a hands-off approach against application-layer DDoS attacks.

Behavioral DDoS Engine's use of machine learning improves the efficacy and decision-making on traffic dimensions for use in creating traffic profiles or baselines. The scoring mechanism for different sensitivity levels considers the risk appetite of your business for detecting attacks and minimizing false positives.

Leading attack detection — As your digital environment grows, so does the depth and breadth of your protections as an Akamai customer. In addition to the automatic updates and adaptive self-tuning that Adaptive Security Engine delivers, App & API Protector provides analyst-recognized leading detections for DDoS, bot, malware, and more attack vectors. Confirm your Akamai protections against emerging and advancing CVEs with our threat research tool.

Application security — App & API Protector features a full suite of defenses and customizations to allow security to be tailored to your organization's needs. Effective capabilities like Client Reputation, client lists, novel attack detection, and more give you the advantage against adversaries while simplifying security operations. The Akamai WAAP solution's advanced application-layer defenses fight back against DDoS, SQL injections, cross-site scripting, local file inclusion, server-side request forgery, and other attack vectors.

DDoS protection and granular rate controls — Recognized as a market-leading DDoS solution, App & API Protector provides DDoS protection on multiple fronts. It starts by instantly dropping network-layer DDoS attacks at the edge for risk mitigation and resource savings. Then, it automatically detects and mitigates sophisticated Layer 7 DDoS attacks at the edge for hands-off and real-time protection against the evolving landscape of DDoS threats. Granular rate controls customize your DDoS defense specifically for your traffic and attack profiles.

Bot visibility and mitigation — Gain real-time visibility into your bot traffic with access to Akamai's directory of known bots. Investigate skewed web analytics, prevent origin overload, and create your own bot definitions to permit access to third-party and partner bots without obstruction. Expanded bot controls, including browser impersonation detection, conditional actions, and crypto challenges, are now included in App & API Protector.

OWASP Top 10

Akamai mitigates risks in both the OWASP Top 10 and the OWASP API Security Top 10. Learn more about how App & API Protector and Akamai security protect customers from large, common, or emerging threats.

To learn more about Akamai's protections against the OWASP Top 10, [download the white paper](#).



API protections — Akamai's industry-leading API protection increases your security by providing visibility to traffic across your digital estate, proactively revealing vulnerabilities, identifying environment changes, and protecting against hidden attacks. With App & API Protector's API capabilities, you can:

- Automatically discover a full range of known, unknown, and changing APIs across your web traffic, including their endpoints, definitions, and traffic profiles
- Easily register newly discovered APIs with just a few clicks
- Detect and mitigate attacks that target APIs, including DDoS, injection attacks, and specification violations
- Control sensitive data handling with App & API Protector's personally identifiable information reporting feature to remain compliant

Performance and more from the largest global network — Being on the Akamai platform provides customers with a competitive edge due to its unmatched global scale, offering real-time visibility into a significant portion of global internet traffic. This vast data enables Akamai to deliver actionable threat intelligence to help organizations stay ahead of evolving security threats and allowing for faster detection and mitigation of attacks across various environments. The platform also provides a proven performance increase and a 100% availability SLA.

Malware protector — This add-on module can scan files at the edge — before they're uploaded — to detect and block malware from entering your corporate systems as malicious file uploads. With no additional app or API configuration required, you free up the time you'd spend setting up protection in each system individually.

Best-in-class defense with simplified security operations

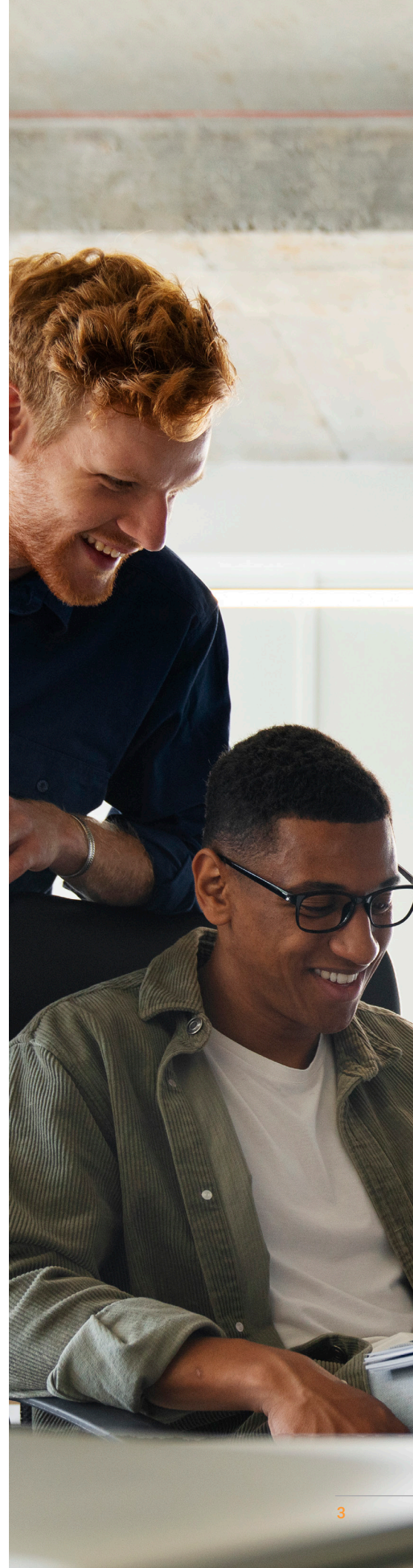
Key capabilities within App & API Protector improve the operational experience within your organization while improving the experience and performance for customers outside of it.

Simple Start onboarding — Great security tools only work if you use them. Akamai is devoted to building an easy-to-use platform that enables productivity and strong protections. You can onboard quickly with our Simple Start, or apply protections to new applications in just a few clicks.

Dashboards, alerting, and reporting tools — Web Security Analytics is Akamai's AI-enabled attack telemetry dashboard. Here, you can analyze security events, create real-time email alerts using static filters and thresholds, and use customizable reporting tools to continually monitor and assess the effectiveness of your protections across the Akamai platform.

DevOps integrations — Seamlessly integrate security into DevOps workflows with GitOps, ensuring that security aligns with fast-paced development. Akamai's APIs, available through CLI or Terraform, allow complete management of App & API Protector via code and match every action available in the user interface.

SIEM integrations — SIEM APIs are also available, and pre-built connectors to Splunk, QRadar, ArcSight, and more are automatically included with App & API Protector.



Included solutions — To increase visibility and performance, App & API Protector now features many of Akamai customers' most-loved products, including:

- **Site Shield**
Prevent attackers from bypassing cloud-based protections and targeting your origin infrastructure
- **mPulse Lite**
Get in-depth visibility into user behavior, address real-time performance problems, and measure the revenue impacts of digital changes
- **Akamai EdgeWorkers**
Explore the benefits of serverless computing, including improved time to market and logic execution nearest to end users
- **Akamai Image & Video Manager**
Intelligently optimize both images and videos with the ideal combination of quality, format, and size
- **Akamai API Acceleration**
Boost your API performance by easily managing access, scaling for spikes in times of demand, and enhancing API security

Free tier offerings may have restrictions on use. Contact Akamai for more information.

Advanced Security Management

The optional Advanced Security Management module has automation and configuration flexibility for those customers with more complex application environments and advanced security needs. The Advanced Security Management option includes additional security configurations, rate policies, security policies, application-layer DDoS controls, custom WAF rules, positive API security, and access to IP reputation threat intelligence (Client Reputation) out of the box.

Managed Security Service

Standard support is offered 24/7/365 for all Akamai customers. In addition to on-demand professional services for consulting or single-project work, Akamai provides levels of managed services — fully managed WAAP service, managed attack support, and specialized security operations center support.



[Speak with an expert](#) to learn more.

Firewall for AI

Akamai Firewall for AI is a purpose-built security solution designed to protect AI-powered applications, large language models (LLMs), and AI-driven APIs from emerging cyberthreats. By securing inbound AI queries and outbound AI responses, the firewall closes security gaps that generative AI introduces.

With real-time detection, policy-based enforcement, and adaptive security measures, this firewall protects against prompt injections, sensitive data leaks, adversarial exploits, and AI-specific denial-of-service (DoS) attacks.

Seamlessly integrating with edge, cloud, hybrid, and on-prem environments, Firewall for AI ensures consistent security, safety, governance, and compliance while preserving performance.

AI-specific threat protection

Firewall for AI provides comprehensive security for AI-driven applications by identifying and mitigating AI-specific vulnerabilities that traditional security tools fail to address.

- **Prompt injection defense** — protects against attackers manipulating AI models through deceptive inputs.
- **Data loss prevention (DLP)** — detects and blocks sensitive data leaks in AI-generated responses, and protects against receiving sensitive data in the requests.
- **Toxic and harmful content filtering** — flags hate speech, misinformation, and offensive content before delivery.
- **Adversarial AI security** — protects against remote code execution, model backdoors, and data poisoning attacks.
- **Denial-of-service mitigation** — mitigates AI-driven DoS attacks by controlling excessive query usage and model overload.

Benefits for your business

-  **Unified AI security posture**
Standardized AI security across edge, cloud, hybrid, and on-prem
-  **Automated AI threat detection**
AI-specific protections without manual rule tuning
-  **Seamless WAAP integration**
Extends web application and API protection (WAAP) with AI defenses
-  **Prevent AI misuse and legal risks**
Blocks data leaks, IP theft, and regulatory violations
-  **Simplified AI security**
No need for in-house engineers to manually enforce security policies
-  **Multicloud flexibility**
Protects AI workloads across environments
-  **Enterprise-grade AI protection**
Backed by Akamai's global threat intelligence



Flexible deployment options

Firewall for AI offers multiple deployment models tailored for different AI architectures and cloud environments.

Deployment model	Description
Akamai edge integration	Protects AI applications inline at the Akamai edge with low-latency security enforcement.
REST API	Scans AI inputs and outputs via API-based risk detection and scoring.
Reverse proxy deployment (roadmap capability)	Routes AI traffic through Akamai's secure proxy for deep inspection and filtering.

This flexibility allows organizations to secure LLMs deployed anywhere, including multicloud, hybrid, and on-prem environments.

How it works

AI traffic analysis

The firewall monitors and analyzes AI interactions, inspecting incoming user prompts and AI-generated outputs to detect potential threats before they reach the model or end user. By analyzing the AI query-response cycle, the firewall effectively prevents security risks while preserving application performance.

Risk scoring and adaptive threat response

AI interactions are evaluated against multiple security indicators, including prompt injections, sensitive data exposure, and adversarial exploits.

Security enforcement actions

Firewall for AI enforces three critical security measures based on risk score and customer risk appetite:

- **Monitor:** Logs detected threats for analysis without interfering with AI queries or responses.
- **Modify:** Adjusts AI-generated outputs inline, removing or altering unsafe content while maintaining a natural conversation flow.
- **Deny:** Blocks high-risk inputs from reaching the AI model and prevents unsafe responses from being returned to users.

Compliance and governance confidence

Firewall for AI can help to meet security and compliance standards. As AI-driven applications introduce new regulatory challenges, maintaining oversight of data privacy, model integrity, and security risks is critical.

Regulatory alignment

The firewall can help organizations comply with privacy, safety, and security guidelines. By enforcing AI-specific security policies, businesses can mitigate risks related to data protection regulations, ethical AI usage, and corporate governance mandates.



Security analytics and logging

Firewall for AI provides detailed audit logs and real-time security analytics, giving security teams visibility into AI security events. By monitoring query patterns, threat indicators, and response behaviors, organizations can proactively detect anomalies, enforce policy controls, and generate compliance reports.

Enterprise-grade AI protection

Backed by Akamai's global threat intelligence, the firewall continuously adapts to emerging AI security threats. By leveraging real-time data insights from AI security research and threat modeling, organizations can maintain a resilient security posture while ensuring their AI applications operate safely and responsibly.



Speak with an expert to learn more.

Akamai Guardicore Segmentation

Modern environments don't stand still. As cloud, Kubernetes, OT, and AI workloads change, attackers exploit those shifts to move laterally and escalate a single foothold into a wide-ranging breach. Akamai Guardicore Segmentation unifies segmentation with exposure-aware detection, automated response, and continuous validation. Our AI-powered platform transforms segmentation into a fast, safe, and low-friction experience. By continuously understanding application communications and prioritizing risk, we're helping organizations reduce attack surface, contain lateral movement, and confirm that Zero Trust protections continue to remain effective as systems evolve.

Security teams are being asked to do two things at once: move faster and reduce risk. But most segmentation efforts stall because environments keep changing, making it harder to prove that enforcement won't disrupt the business. Static discovery snapshots go stale, flow-only maps lack application context, and manual policy writing can't keep up with hybrid IT sprawl. The result is painfully familiar: visibility without intelligence, intelligence without action, and action without assurance.

Akamai Guardicore Segmentation is built for risk containment in dynamic environments. It continuously learns what exists, how it communicates, and what that behavior means for operational risk. Then, it turns that understanding into enforcement-ready segmentation policies you can trust, with validation that they won't impact production.

Why traditional approaches fall short

Many solutions start and end with network flows. They show who talked to whom, but they don't show what that communication represents, whether it is required for the application to function, or what happens if it is abused. Other solutions promise AI-powered recommendations but deliver generic, point-in-time outputs that still require weeks of manual analysis and cross-team coordination to validate. That gap between insight and enforcement is where attackers win in fast-changing environments, by moving laterally and expanding the blast radius.

In addition, we know that detection alone does not reduce risk. Most security tools surface alerts without reachability or blast-radius context, leaving teams unsure of which threats matter or how far an attack could spread. Investigations are slow and manual, requiring analysts to correlate data across network, workload, identity, and application tools. As environments evolve, segmentation controls drift and teams lack a continuous way to validate whether Zero Trust policies still work.

Benefits for your business



Contain faster

Limit lateral movement and reduce ransomware impact by enforcing least-privilege communications. This shrinks attacker pathways and blast radius without waiting months for manual mapping.



Enforce with proof

Move from visibility to protection using readiness signals, clear policy rationale, and phased enforcement workflows that validate safety before changes reach production.



Eliminate guesswork

Use process-level context to understand what is running and how it behaves, replacing tribal knowledge with clear, reliable insight.



Prioritize by risk

Focus your efforts where they matter most by evaluating exposure in business terms — including reachability and blast radius — and track measurable attack surface reduction over time.



A new approach: Continuous understanding, proof-driven action

Akamai Guardicore Segmentation provides capabilities that are critical for Zero Trust, from continuous discovery and enforcement to detection, investigation, and ongoing validation. The goal is not just to “see” the environment at a single point in time but to continuously understand it well enough to act and validate that actions remain correct over time.

- **Continuous discovery that never stops learning**

Zero Trust depends on knowing what exists and understanding how it’s supposed to behave. Akamai Guardicore Segmentation leverages AI to maintain an always-current inventory and communication model across data centers, cloud, Kubernetes, OT/IoMT, and emerging AI workloads. As assets appear, change, or disappear, the model updates automatically. That way, you’re not making today’s decisions based on yesterday’s snapshot.

- **Application understanding at the process level**

Seeing connections is not the same as understanding an application. The platform ties network communications directly to the processes and services that generate them, building true application context without relying on undocumented assumptions or prolonged “app mapping” projects. By grounding visibility at the process level, teams gain a clear, accurate picture of how applications actually function in production.

- **Business-risk reasoning**

Beyond visibility, the platform leverages AI to evaluate exposure in terms that matter to the business, including reachability, blast radius, and criticality. This allows teams to understand not just what is communicating but what is truly at risk. With that context, security and IT teams can prioritize the controls that reduce the most risk first and demonstrate measurable risk reduction.

- **Proof before impact**

Segmentation delivers its value when enforcement is real and rules aren’t left in “monitor-only.” Akamai’s unique approach generates enforcement-ready segmentation policies with explainable rationale and readiness signals so teams can validate safety before impact. Policies can move through staged workflows (draft, alert, block) and be measured for readiness, reducing outage risk and enabling consistent least-privilege enforcement across thousands of workloads.

- **Exposure-aware assurance**

Zero Trust is not static. Controls drift, environments change, and attackers probe for pathways. The platform adds an assurance layer that detects suspicious behavior in the context of exposure and reachability, then accelerates investigations with AI-led analysis that produces clear findings and next-best actions. Continuous validation measures whether segmentation controls are actually limiting blast radius, highlights gaps and unintended exposures, and feeds insights back into policy. This creates a continuous feedback loop that strengthens Zero Trust over time.

How Akamai Guardicore Segmentation works

1. **Discover continuously.** Deploy lightweight sensors and integrate with existing telemetry sources to build a living map of assets and communications across your environment.
2. **Understand automatically.** Convert raw communications into application context with AI that correlates process-level visibility with customer-specific intelligence so you know what’s actually running and why it matters.
3. **Enforce safely.** Generate enforcement-ready segmentation policies and validate them through a phased workflow. This allows teams to move into protection with confidence and reduce attack surface without disrupting operations.
4. **Assure with confidence.** Monitor, validate, and measure the effectiveness of segmentation policies over time. Confirm that controls are working as intended, identify policy drift or new exposure, and demonstrate sustained risk reduction as applications and infrastructure evolve.

What you can achieve with Akamai Guardicore Segmentation

Contain lateral movement and reduce ransomware impact. By restricting communications to only what is truly needed, Guardicore limits attacker pathways and reduces blast radius when prevention fails. Segmentation becomes a containment control you can quickly operationalize.

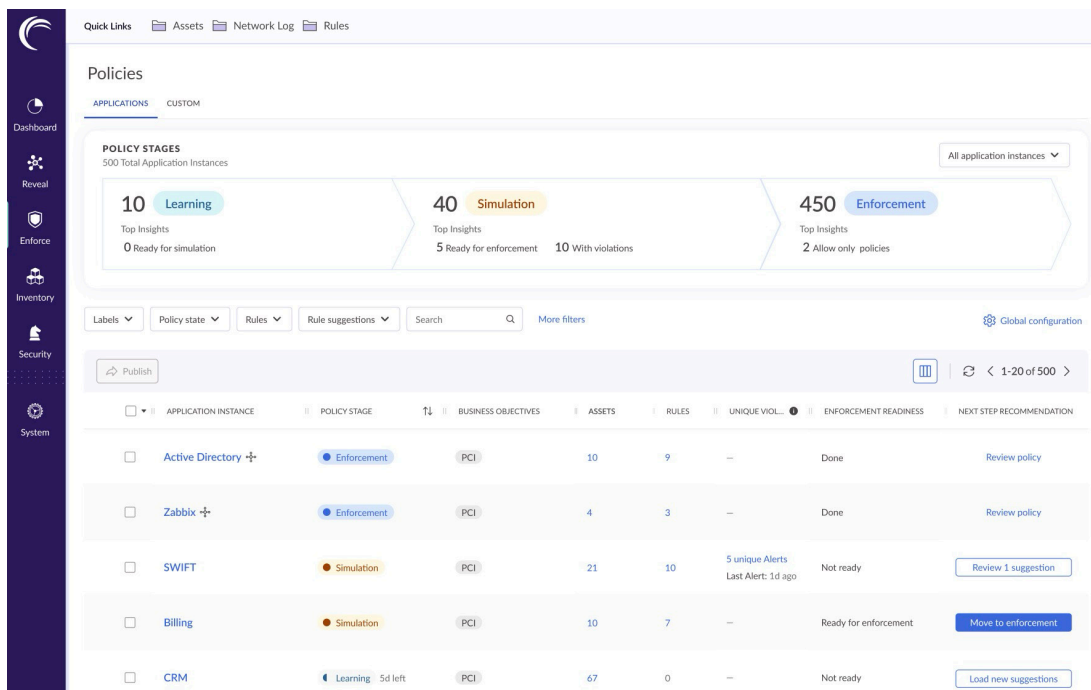
Accelerate Zero Trust outcomes without adding headcount. Akamai Guardicore automates discovery, application understanding, policy design, and validation while keeping people in control of intent and approvals. This allows small teams to scale protection across large, complex environments.

Make enforcement safe for the business. Security and IT teams often avoid large-scale segmentation because they can't prove what will break. Akamai Guardicore replaces guesswork with evidence: application context, policy rationale, and readiness signals that support confident decision-making.

Prove progress over time. Akamai Guardicore helps teams measure risk reduction and explain it clearly to stakeholders. Teams can quickly see what is discovered, what is protected, what is still exposed, and where to focus next.

Governance and control that match how enterprises operate. Segmentation programs succeed when they are repeatable, auditable, and resilient to change. Akamai Guardicore supports governance with explainable recommendations, clear policy intent, and workflows that align security, infrastructure, and application owners. Teams can standardize policy patterns, apply labels and scopes consistently, and use readiness indicators to document why a policy is safe to enforce. Over time, continuous validation helps ensure protections stay aligned as applications evolve so containment doesn't decay as quickly as the environment changes.

Akamai Guardicore Segmentation turns continuous discovery into enforcement-ready segmentation, using explainable AI and proof-driven workflows



AI-powered recommendations. Human-driven security.

Where it fits best

- Organizations pursuing Zero Trust segmentation that must show measurable outcomes to leadership and auditors.
- Hybrid enterprises where a mix of cloud, Kubernetes, devices, and self-hosted environments change faster than static policy can keep up.
- Ransomware and breach containment programs focused on limiting lateral movement and blast radius.
- Operationally sensitive environments where downtime or latency risk makes “trial-and-error” enforcement unacceptable.
- Teams enabling AI initiatives that require stronger controls around workload communications and exposure.

Akamai Guardicore Segmentation turns segmentation into a practical, scalable risk containment program. With continuous discovery, application-level understanding, proof-driven enforcement and comprehensive assurance, security teams can systematically eliminate unnecessary exposure and measurably shrink lateral movement risk across the enterprise.

Reduce your attack surface with confidence.

To learn more, [request a demo](#).