AKAMAI PRODUCT BRIEF

Software Defined Network 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.

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

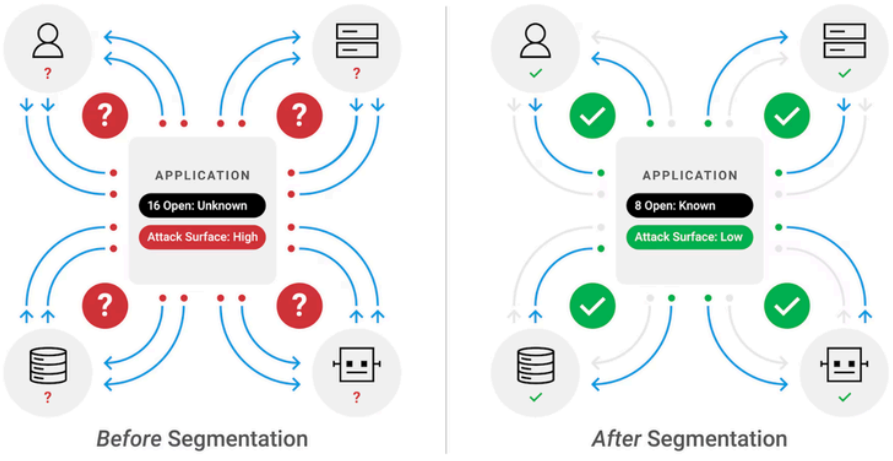
Move from visibility to protection using readiness signals, clear policy rationale, and phased enforcement workflows that validate safety before changes reach production.

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.



Before Segmentation

After Segmentation

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 AIpowered 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.

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.

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.

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.

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.

What you can achieve

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

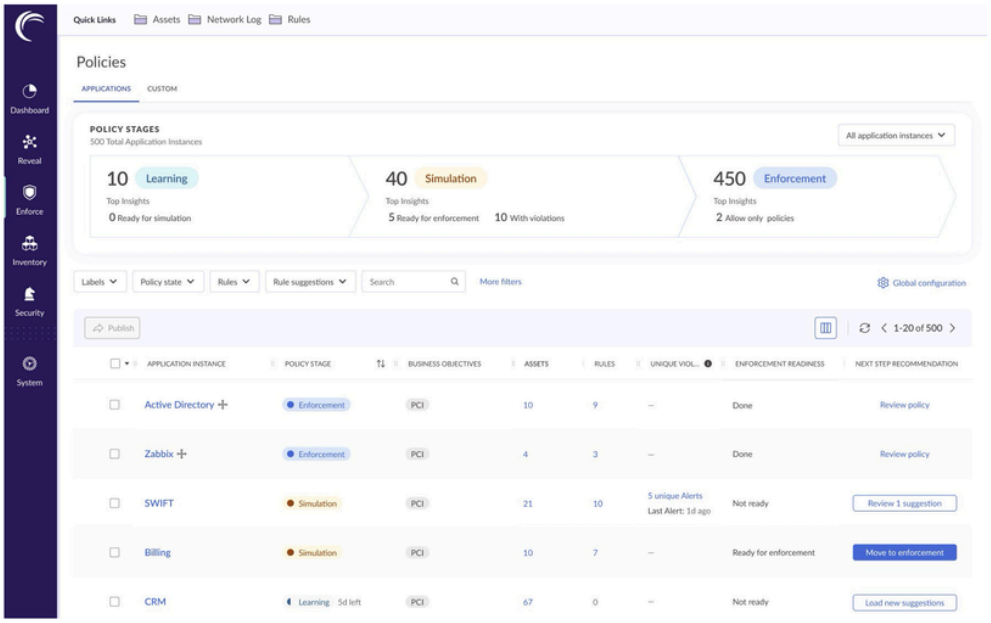
Security and IT teams often avoid large-scale segmentation because they can't prove what will break. Akamai Guardicore replaces guesswork with evidence: application context, policy rationale, and readiness signals that support confident decision-making.

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 enforcementready segmentation, using explainable AI and proof-driven workflows

Supported Platforms and Technologies

»We are designed to integrate with your existing infrastructure.

»Our OS support expands continuously with our customers' needs.

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.

How it works

Discover continuously

Deploy lightweight sensors and integrate with existing telemetry sources to build a living map of assets and communications across your environment.

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.

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.

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.

Gartner Peer Insights Customers' Choice 2026

★★★★★

"Our experience with Guardicore has been outstanding. The platform offers robust and reliable microsegmentation capabilities that have significantly enhanced our network security posture."

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.

Evolane Guardian

Standard support is offered 24/7/365 for all Akamai customers. In addition to on-demand professional services for consulting or single-project work, Evolane provides levels of guardian services

To learn more, click here and visit our Akamai partnerpage on the Evolane website.