Technology Partner Solution Brief

Akamai + Tufin: More Secure Together

Executive Summary

Akamai Guardicore Segmentation enforces Zero Trust at the workload level to limit lateral movement, reduce ransomware spread, and meet compliance requirements (e.g., PCI DSS, HIPAA, etc.). Tufin extends Akamai's AI-powered enforcement with unified visibility, and continuous compliance, connecting segmentation into a broader network security solution across hybrid environments. Together, Tufin and Akamai ensure that Zero Trust segmentation is part of a governed, operationalized, and scalable enterprise security strategy.

Barriers To Your Success

Hybrid enterprises face growing policy sprawl across firewalls, cloud environments, SASE platforms, SD-WAN infrastructure, and microsegmentation controls. As security architectures become more distributed, rule management grows inconsistent and visibility across enforcement layers becomes limited.

Organizations commonly struggle with:

- Fragmented policy management with no unified visibility
- Manual, error-prone troubleshooting across NGFWs and segmentation tools
- Limited end-to-end visibility into application access rules
- Unintended exposure from permissive rules, open ports, and misconfigured zones
- Segmentation policies misaligned with organizational and compliance requirements
- Siloed, manual change processes causing delays and misconfigurations across hybrid environments

Security and network teams are further pressured to validate changes manually, respond quickly to audits, and demonstrate compliance across increasingly complex environments. While microsegmentation strengthens security posture, when supported by unified visibility and policy orchestration, it simplifies operations and enables consistent, enterprise-wide governance across complex environments.

Akamai & Tufin: More Secure Together

Akamai Guardicore Segmentation delivers fine-grained, AI-powered workload microsegmentation that enforces Zero Trust principles across the enterprise. Tufin extends this capability through a unified control plane that provides centralized visibility, tag-based governance alignment, policy analysis, and comprehensive change tracking across environments.

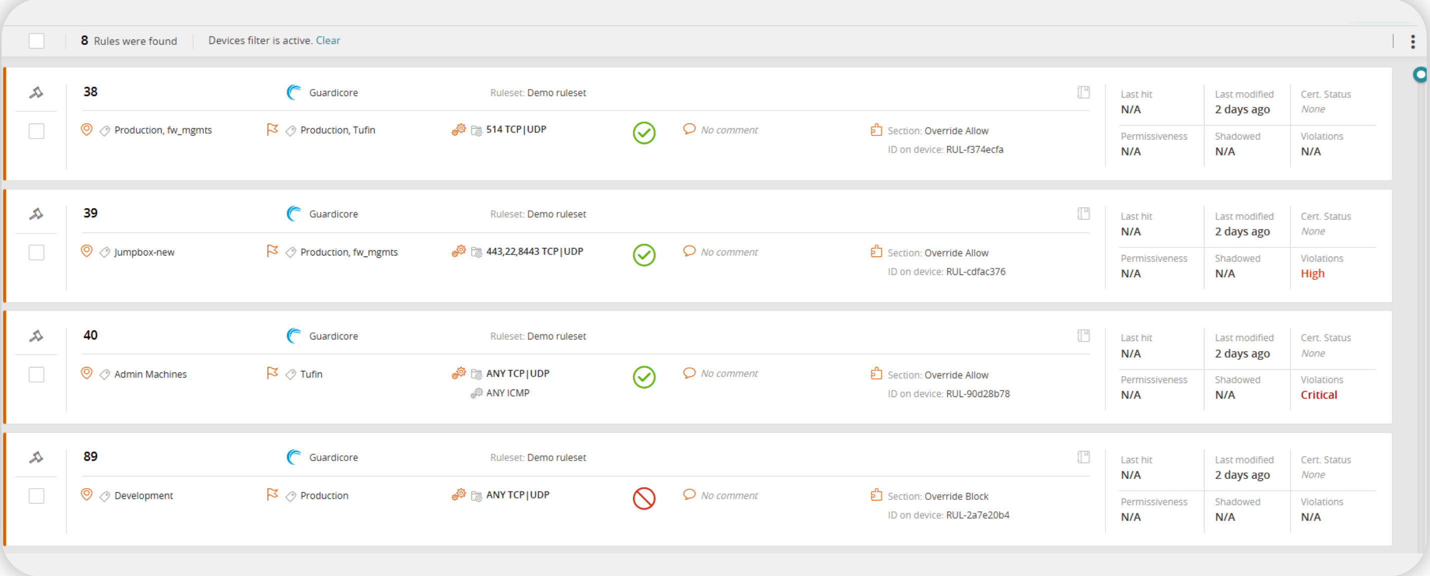
By integrating enforcement with compliance, segmentation policies become fully visible and auditable within broader network security workflows. Security and compliance teams can quickly assess policy alignment with enterprise standards, understand the impact of changes, and maintain consistent security posture across hybrid infrastructure. Together, Tufin and Akamai ensure that Zero Trust segmentation is not only enforced, but continuously governed and scaled with enterprise-wide control.

How It Works

Akamai Guardicore enforces workload-level segmentation using Zero Trust principles across hybrid infrastructures. Tufin's unified control plane aggregates Guardicore policies and contextualizes them alongside firewalls, cloud security controls, and SASE enforcement points, providing a single, end-to-end view of how access is governed across the environment.

Within this unified framework, organizations can:

- Define and visualize segmentation strategy with a centralized, matrix-based model
- Compare intended design to enforced policies to validate security alignment
- Identify gaps, violations, and overly permissive access paths
- Detect policy drift before it creates operational or compliance risk
- Maintain continuous audit readiness with centralized tracking and rule history



☐ 8 Rules were found | Devices filter is active. Clear

☐	38 Production, fw_mgmts	Guardicore Production, Tufin	Ruleset: Demo ruleset 514 TCP|UDP	✓	No comment	Section: Override Allow ID on device: RUL-f374ecfa	Last hit N/A	Last modified 2 days ago	Cert. Status None	Permissiveness N/A	Shadowed N/A	Violations N/A
☐	39 Jumpbox-new	Guardicore Production, fw_mgmts	Ruleset: Demo ruleset 443,22,8443 TCP|UDP	✓	No comment	Section: Override Allow ID on device: RUL-cdfac376	Last hit N/A	Last modified 2 days ago	Cert. Status None	Permissiveness N/A	Shadowed N/A	Violations High
☐	40 Admin Machines	Guardicore Tufin	Ruleset: Demo ruleset ANY TCP|UDP ANY ICMP	✓	No comment	Section: Override Allow ID on device: RUL-90d28b78	Last hit N/A	Last modified 2 days ago	Cert. Status None	Permissiveness N/A	Shadowed N/A	Violations Critical
☐	89 Development	Guardicore Production	Ruleset: Demo ruleset ANY TCP|UDP	⃠	No comment	Section: Override Block ID on device: RUL-2a7e20b4	Last hit N/A	Last modified 2 days ago	Cert. Status None	Permissiveness N/A	Shadowed N/A	Violations N/A

Unified visibility across Akamai Guardicore and hybrid environments.

All segmentation changes are captured and managed within Tufin, ensuring complete visibility into rule evolution over time. Compliance guardrails reinforce alignment with organizational standards and regulatory requirements, enabling consistent governance and a unified operational view of security posture across the entire security stack.

Driving Business Outcomes

By unifying segmentation enforcement and policy governance, the solution reduces risk exposure across hybrid environments while improving operational efficiency. Centralized visibility and integrated policy validation enable organizations to deploy secure services faster without sacrificing oversight or compliance.

Organizations benefit from:

- Reduced risk through unified segmentation visibility and cross-team alignment
- Faster service delivery with embedded policy validation
- Stronger compliance with centralized change tracking and audit-ready reporting
- Lower operational overhead by reducing manual analysis and troubleshooting
- Consistent governance across hybrid environments without slowing innovation

With centralized rule and tag visibility, full change history, and standardized governance processes, security teams can maintain policy alignment across environments while preserving agility and responsiveness.

Why Akamai & Tufin?

Tufin and Akamai Guardicore Segmentation together deliver unified visibility, policy governance, and segmentation enforcement across hybrid infrastructure. By connecting security policy management with microsegmentation controls, the joint solution ensures consistent security intent, continuous compliance, and streamlined operations across on-premises, cloud, and hybrid environments. Organizations gain a cohesive framework that aligns segmentation strategy with enterprise-wide security policy and audit requirements.

Organizations gain centralized querying and analysis of Guardicore policies, comprehensive change tracking, and compliance guardrails aligned with enterprise standards. Akamai Guardicore enforces workload-level segmentation, while Tufin governs, validates, and audits segmentation policy across the enterprise. Together, they provide the control, transparency, and scalability required to operationalize Zero Trust segmentation across complex hybrid environments.

About Tufin

Tufin helps enterprises simplify network complexity. As the leading Network Security Posture Management platform, Tufin serves as the unified control plane for modern hybrid networks spanning on-premises, cloud, SASE, microsegmentation, and multi-vendor environments. Trusted by thousands of organizations worldwide, Tufin delivers continuous risk visibility, reduces exposure through policy-driven automation, and enables continuous compliance and audit readiness at scale.