

Tufin Streamlined Security Policy Control

Partnership enabled modern Zero Trust by uniting policy management and microsegmentation



Unified
policy control



Reduced
tool sprawl



Accelerated
Zero Trust

Helping customers simplify Zero Trust in the AI era

Tufin helps enterprises manage security policy across hybrid networks, cloud environments, and firewalls. As AI-driven threats push companies to strengthen internal defenses, more organizations are adopting Akamai Guardicore Segmentation for deeper east-west traffic visibility and control. Through integration with [Akamai Guardicore Segmentation](#), Tufin lets customers manage segmentation policies alongside firewalls and cloud controls in one place. This helps simplify Zero Trust and reduce operational complexity.

AI threats are pushing security deeper into the network

Security teams are under more pressure than ever. Networks are growing larger and more distributed. Applications now run across data centers, cloud platforms, and edge environments.

At the same time, AI has changed the pace of attacks. Threat actors can scan for weak spots, probe systems, and adapt quickly. That makes it harder for traditional perimeter defenses to keep up.

To respond, companies are focusing more on internal segmentation. [Microsegmentation](#) has become one of the strongest ways to stop attackers from moving laterally once they get inside.

“Granular segmentation is critical for companies looking to address today’s complex threat environment,” said Raymond Brancato, CEO of Tufin.

More security tools can create more complexity

The challenge is that stronger security often means more tools. Most large enterprises already manage firewalls, cloud controls, endpoint tools, and compliance systems. Adding microsegmentation can improve protection, but it can also add more work.

tufin

Location

Boston, Massachusetts
tufin.com

Industry

Software and SaaS

Solution

Security

Product

[Akamai Guardicore Segmentation](#)



“Our customers are investing in numerous tools to handle their increasingly complex networks,” said Brancato. As a result, teams may need to switch between multiple consoles to review policies, investigate issues, or make changes. That slows response times and increases the chance of mistakes.

Brancato said customers want fewer management layers, not more. “CISOs are concerned about adding another tool,” he said. “They don’t want another environment to manage.”

One control plane for a growing security stack

That concern is exactly what the Tufin and Akamai partnership addresses. “Together, we created an integration that lets customers take advantage of Akamai Guardicore Segmentation while managing policies through the Tufin Orchestration Suite,” said Brancato.

- **Akamai Guardicore Segmentation:** Provides workload-level visibility, application-aware labels, and east-west traffic controls to stop lateral movement.
- **Tufin Orchestration Suite:** Unifies policy management across firewalls, cloud systems, and segmentation environments.

Customers can keep using the tools they trust while reducing the operational burden. “Tufin enables customers to manage Akamai Guardicore Segmentation as part of their security stack,” he added.

Acting as the control plane, Tufin gives customers visibility into segmentation policies, firewalls, and cloud environments from one place. For security teams, that unified view means less friction and faster policy review and enforcement.

Application-level context makes security smarter

One of the greatest strengths of Akamai Guardicore Segmentation is how deeply it sees into the network. Because the Akamai platform sits directly on the host, it can track which process starts each connection. That creates rich labels tied to applications and workloads.

Such depth gives teams a much clearer picture of how applications actually behave. That visibility becomes even more powerful when connected to Tufin.

“Customers are looking to understand their network not just from an IP perspective, but from the application perspective,” said Brancato. “Akamai Guardicore Segmentation brings that context.”

By pulling those labels and application insights into Tufin, customers can make better decisions about policy, compliance, and risk. “Akamai’s solution enables us to provide overall context for their entire environment, from an application-centric point of view,” he continued.



**This partnership
gives customers
the value of
microsegmentation
without managing
another console.**

Raymond Brancato
CEO, Tufin

Faster Zero Trust without more overhead

One of the biggest barriers to **Zero Trust** is speed. Security teams know they need better segmentation, but rolling it out across a large environment can take time. Akamai's integration with Tufin helps speed that process.

AI features within Akamai Guardicore Segmentation make microsegmentation simpler, faster, and more effective. Customers can see segmentation policies inside Tufin and understand how those policies connect to the rest of their network controls. That helps them reduce manual work and scale segmentation without adding more people.

The next step of this partnership will go even further. "We will provide visibility into policies, as well as the ability to update those policies," said Brancato.

Helping customers get the full value of microsegmentation

For modern enterprises, microsegmentation has become a core part of defending against AI-powered attacks. But to work at scale, it needs to fit into the broader security stack.

That's why this partnership matters. Akamai Guardicore Segmentation gives companies the deep, application-level visibility needed to control east-west traffic. Tufin gives them a way to manage that control alongside the rest of their environment.

"Together, we help customers strengthen Zero Trust without adding unnecessary complexity. They get the full value of Akamai Guardicore Segmentation while managing it through a platform they already trust," Brancato concluded.



Tufin helps enterprises govern and secure connectivity across today's complex multi-vendor networks. As the leader in network security posture management, Tufin provides the trusted control layer organizations need to understand exposure, automate policy changes safely, and maintain continuous security posture across on-premises, cloud, SASE, microsegmentation, and hybrid environments. Built on customer-proven network automation playbooks and the industry's only Dynamic Network Connectivity Graph, Tufin is bringing Multi-Vendor Agentic Network Security to the enterprise — helping organizations move from visibility to governed, AI-driven action. For more information, please visit tufin.com or follow us on [LinkedIn](#).