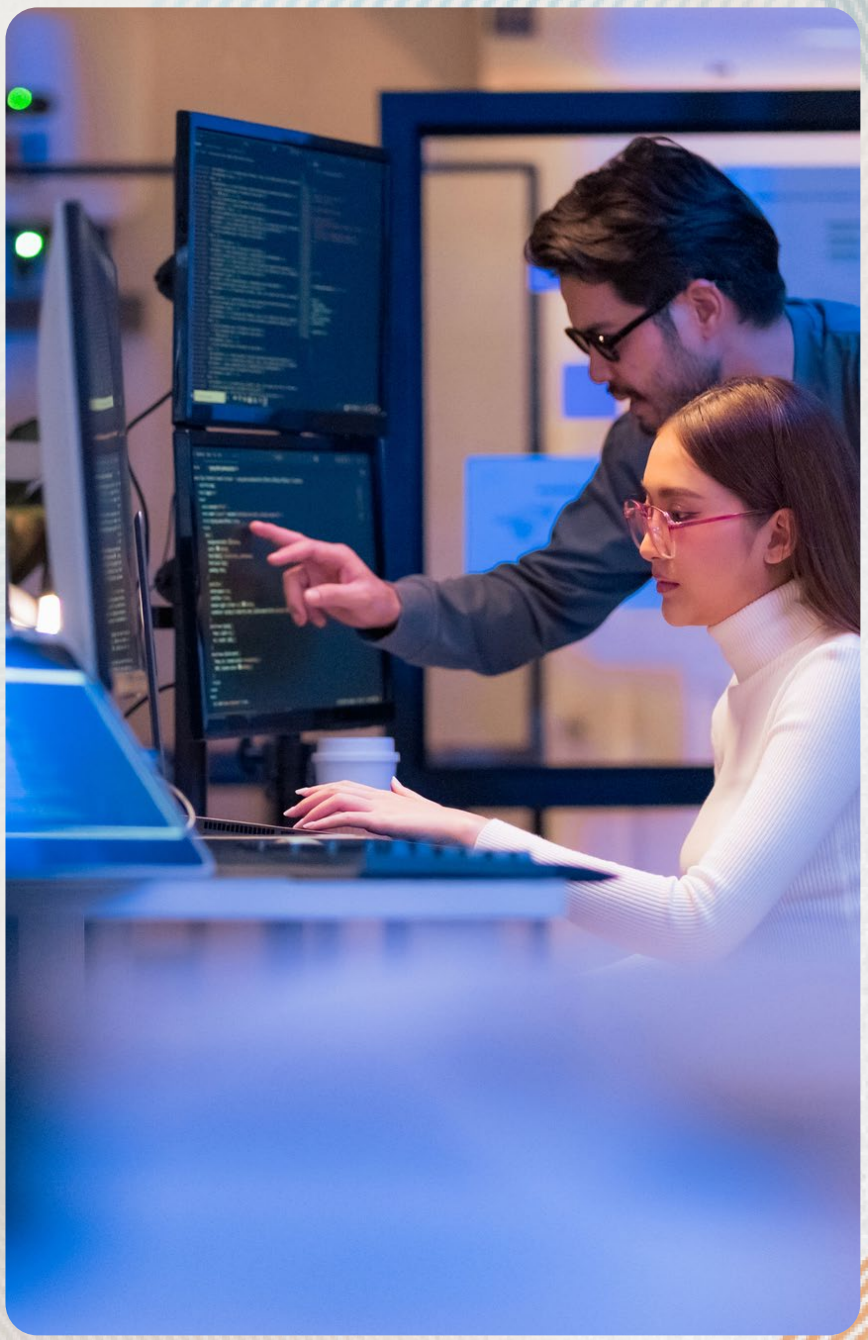
tufin

Confidence & Control:

Achieving Zero Trust & Segmentation in Complex Networks

5 Indicators Your Zero Trust and Segmentation Strategy Is on Track



DARKREADING

Introduction: Why uncertainty persists in cyber readiness

Confidence in cyber readiness is lagging. According to PwC's 2026 Global Digital Trust Insights, only about half of business and tech executives say their organizations are 'somewhat capable' of withstanding cyberattacks targeting specific vulnerabilities.

But in cybersecurity, 'somewhat' is not enough.

When we look deeper, the issue is not about organizations knowing what needs to be secured or which requirements must be met. The real challenge is achieving certainty in governance, especially amidst increasing AI initiated and influenced activity and less direct human oversight.

Security professionals—from CISOs to their security teams—struggle to determine if their existing network access controls, policies, and applications are truly optimized to deliver the protection they are intended to provide. While teams may know that these security controls exist or their policy intent, there is often limited certainty about whether they are governed effectively or operating as intended on a continuous basis.

Network security posture must address this problem to enable the security outcomes those controls produce in the broader, interconnected global network.

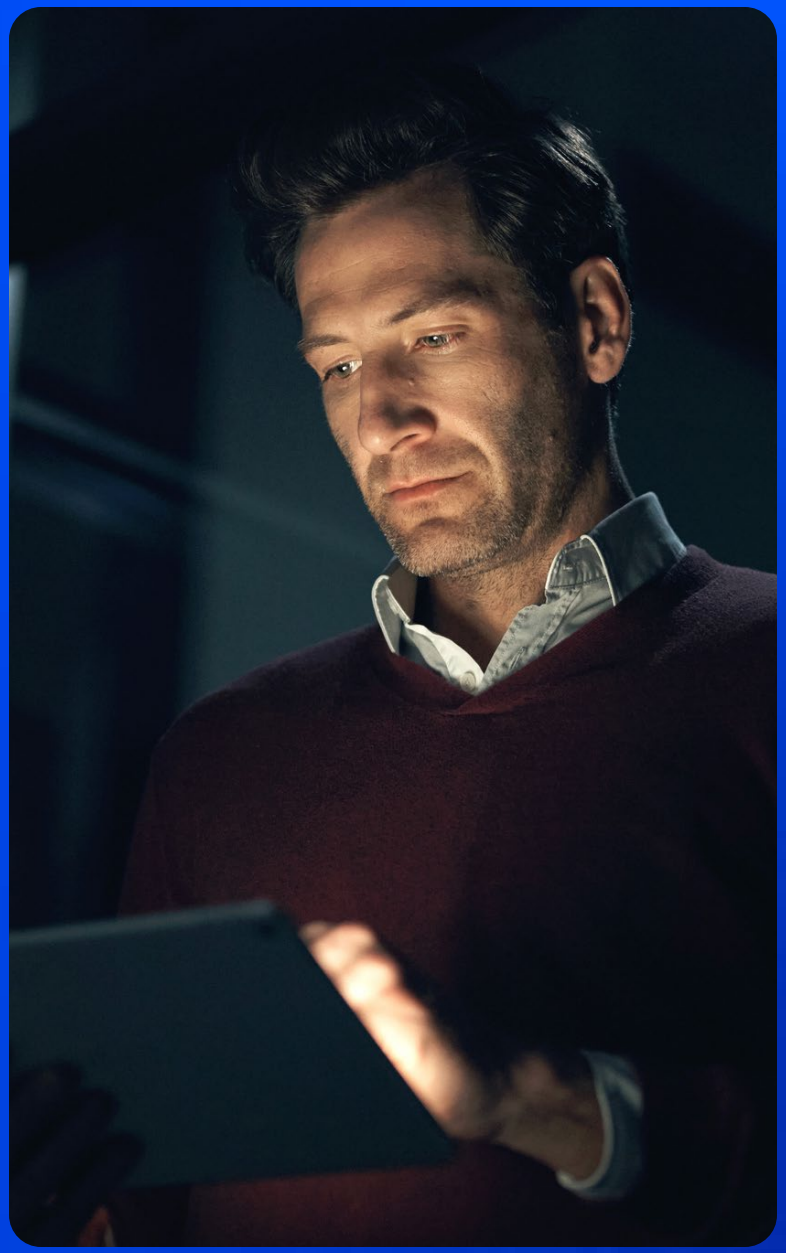
Erez Tadmor, Global Field CTO at Tufin, says the disconnect stems from traditional reporting being control-centric rather than exposure-centric.

> **"Most organizations measure what is visible and reportable. But network security posture is not defined by the presence of controls. It is defined by outcomes."**
>
> **Erez Tadmor,**
> **Global Field CTO, Tufin**

Modern networks are highly dynamic, with access requirements changing continuously and enforcement points being updated frequently. Without unified connectivity modeling across all enforcement layers, organizations see enforcement points in isolation—not the attack graph they collectively create.

The result? Confidence in tooling, but uncertainty in outcomes.

This playbook aims to change that by helping organizations navigate the growing complexity, align strategies across teams, and ensure that network security is implemented correctly.



Zero trust vs. Segmentation: Where security becomes fragmented

Microsegmentation, cloud firewalls, and edge controls, such as SASE architectures, are all effective individually at reducing risk at a local level:

> **Microsegmentation** limits east-west lateral movement and reduces blast radius by enforcing least-privilege communication between workloads.
>
> **Cloud firewalls** and security groups isolate workloads and restrict north-south exposure.
>
> **SASE** delivers cloud-based, identity- and context-aware security controls at the network edge, securing remote user, branch, and internet-bound connectivity.

Together, these controls are expected to provide unified protection, yet in practice, they fragment network-level enforcement across platforms, teams, and environments. It happens because the policy intent is translated separately into each platform, and different teams own different enforcement domains. The outcome is limited visibility within the local domain and no unified validation of effective reachability across the domains and throughout the entire network.

“When security intent is fragmented, verification becomes complex, and network policy drift becomes inevitable,” says Tadmor. “The risk often accumulates in the seams between platforms, not necessarily within them.”

As enforcement becomes more distributed, it becomes increasingly harder to answer critical questions: Is security intent applied consistently? Are controls aligned? Is network security de facto working as designed?

These challenges often manifest as friction between zero-trust initiatives and segmentation strategies, stemming from distributed architectures without unified network access validation. In distributed environments:

- Security pushes for tighter isolation and high governance.
- Network teams must implement changes across multiple enforcement platforms.
- Business units demand rapid access provisioning/enablement.
- Policy states change continuously.

Without automation and unified policy modeling, coordination becomes manual, error-prone, and pretty often do not scale.

“When policy intent is decoupled from infrastructure and validated centrally across all enforcement points, both security and network teams benefits as they operate from a shared model of reachability and risk,” says Tadmor. “This reduces conflict, accelerates compliant change, and improves consistency.”

5 Signs You're Doing Zero Trust and Segmentation the Right Way

The combination of zero trust and segmentation delivers measurable security value. They reduce lateral movement, limiting the blast radius, and enable faster containment and mitigation during incidents.

However, their full value depends on continuous validation. Zero trust is not simply the deployment of identity-aware controls. It is the ongoing ability to prove what is reachable, what is not, and why.

> **"When segmentation and trust boundaries are defined clearly and validated continuously, organizations materially reduce both breach probability and breach impact."**
>
> **Erez Tadmor,**
> **Global Field CTO, Tufin**

The following five indicators reflect whether network security is working as you intended and have the same underlying principle of continuous validation for effective reachability.

1. You've managed segmentation by decoupling policy from infrastructure.

2. You've clearly defined ownership and scope across your network segments.

3. You now automate network security policy enforcement and access changes.

4. You continuously monitor and maintain a zero-trust segmented environment.

5. You can assess attack surfaces across cloud, on-premises, and hybrid environments.

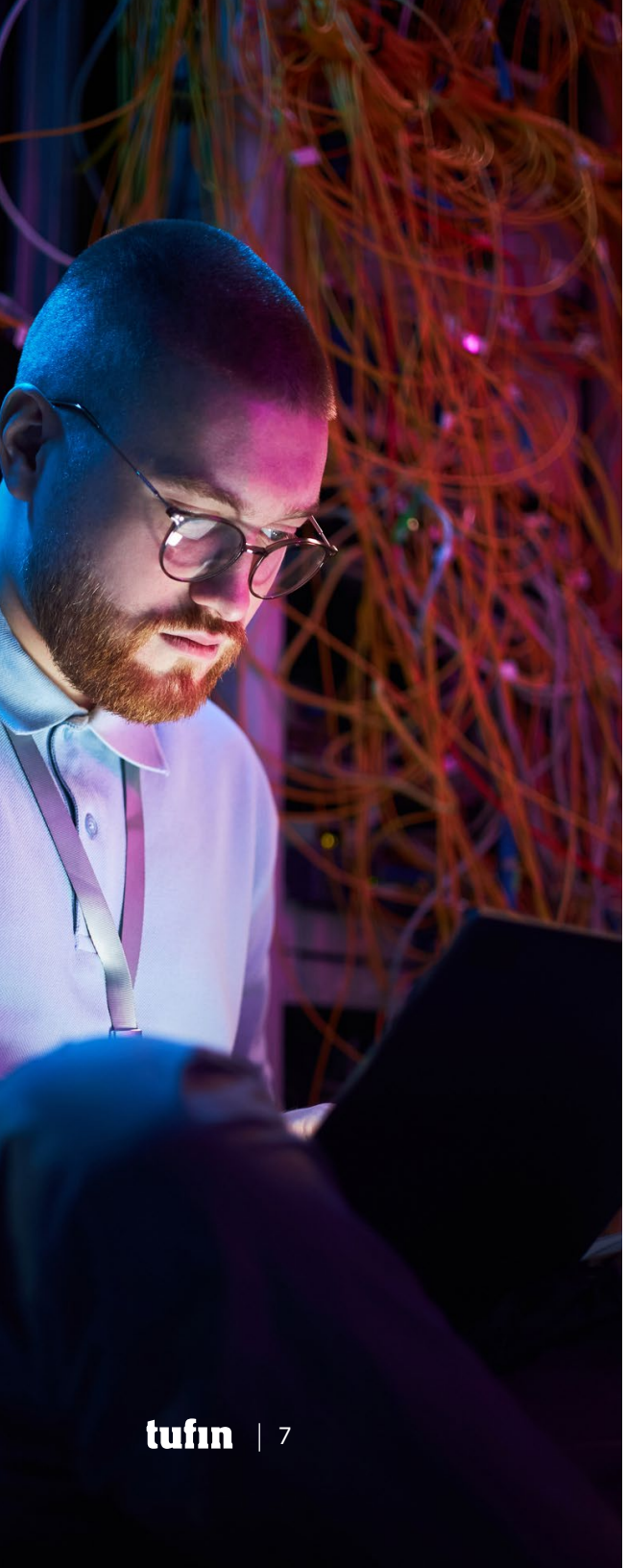
1. You've managed segmentation by decoupling policy from infrastructure.

"Decoupling policy from infrastructure is important because it forces you to look at everything from an organization perspective, not from a technology or a silo perspective," says Ricky Egge, Director of Solutions Engineering, Americas, at Tufin.

To manage segmentation effectively across hybrid environments, organizations must decouple segmentation policies from the underlying network infrastructure. This approach allows policies to follow apps and workloads, from the datacenter to the cloud, without being limited by specific platforms. The result is improved visibility and a stronger security posture.

HOW TO DO IT RIGHT:

- Deploy policy automation to implement changes quickly and consistently.
- Use policy analysis to enable fast, precise provisioning of new or changed access.
- Create predefined workflows to handle common changes, ensuring user accountability and comprehensive audit trails.
- Use automation to define and manage your segmentation policy.



2. You've clearly defined ownership and scope across your network segments.

Modern networks span multiple vendors, devices, and platforms. Increasingly, these environments are managed by different business units, each with distinct priorities and objectives. Without clearly defined ownership, accountability is lacking, and efficiencies decline.

By establishing ownership across all parts of a network, organizations can know who is responsible in the event of a security incident or breach. Decisions can be made quickly when the owner provides context and background.

Egge emphasizes that ownership is not just about infrastructure. "Having liaisons within organizational silos is key. It's not just owning different parts of the network. It's also the end systems and the applications," he says. "The owners of those systems are important because they understand their purpose, the business impact, and what happens if they're not available."

HOW TO DO IT RIGHT:

- Extend ownership planning to newly adopted, merged, or acquired networks before integration.
- Regularly review ownership to reflect organizational or architectural changes.
- Conduct periodic check-ins with owners to ensure alignment with security policies and posture.
- Lead ongoing training to educate owners about new risks or threats.

3. You now automate network security policy enforcement and access changes.

No more ticketing systems for approvals or Excel files for tracking because you've left manual processes behind. Now you can keep up with the pace of change requests, cleanups, recertifications, and audits with fewer delays and risks.

Automation reduces turnaround time while ensuring changes are compliant, validated, and auditable. Egge notes that automation isn't a switch you flip on and off.

> **"Automation is a dial you turn up as you get more comfortable with the different technologies and integrations. Being able to automate changes is the only way to get it done effectively and in time."**
>
> **Ricky Egge,**
> Director of Solutions Engineering, Americas, Tufin

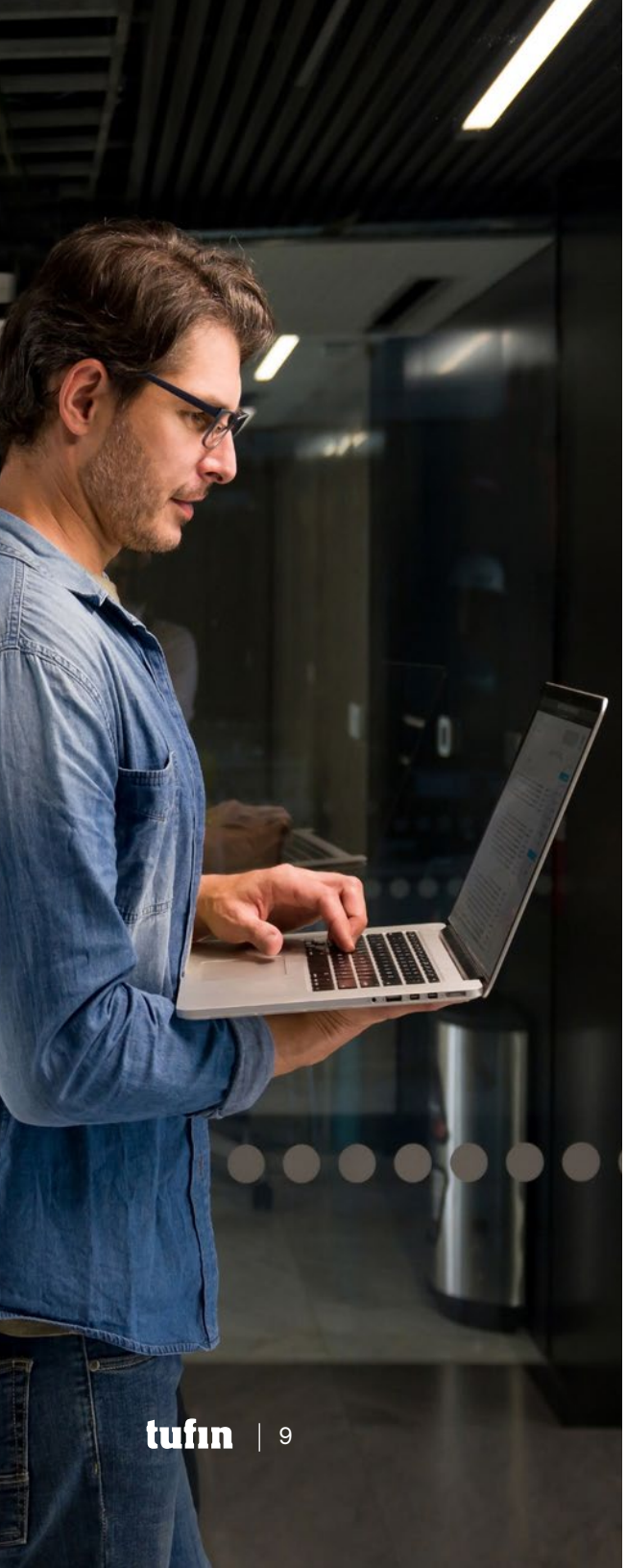
AI and machine learning are further accelerating security and access management by validating compliance, prioritizing vulnerabilities based on real exposure, supporting application deployment validation, and assisting with policy recertification—but only when grounded in trusted connectivity context and governed workflows.

Tadmor says there's already been changes in app development to being almost completely agentic.

"In the agentic development future, organizations will shift network changes to be agentic and mostly autonomous," he says. "Network agents will work hand-in-hand with app development agents to rapidly implement the policy changes required by agentic development. This will dramatically increase network exposure and the attack surface."

HOW TO DO IT RIGHT:

- Monitor for uncontrolled changes that can introduce security risks or compliance violations.
- Validate that changes do not enable more access than required or approved, preventing unnecessary expansion of the attack surface.
- Ensure security keeps up with development as more organizations adopt DevOps methodologies.
- Streamline change management through a single, policy-aware workflow that accepts requests, automatically identifies the correct enforcement point, validates against policy, implements it, and confirms the result.



4. You continuously monitor and maintain a zero-trust segmented environment.

Zero trust is not a one-and-done initiative. It requires an ongoing plan to monitor, validate, and refine the environment.

“You can’t just roll out zero trust and start segmentation. You must have a plan to monitor the environment and ensure you adhere to your policies and remain compliant. Otherwise, you end up with policy sprawl across the organization,” says Egge. “That's where automated systems can alert you when activities go unchecked.”

Over time, organizations can accumulate thousands of rules, some of which are no longer relevant to current business needs. Egge frequently sees organizations implement zero trust but neglect the ongoing cleanup and optimization necessary for it to be effective. AI can help by detecting drift, surfacing violations, and supporting recertification or by using dedicated agents to manage network posture.

HOW TO DO IT RIGHT:

- Continuously monitor all aspects of your network to detect policy violations, unauthorized access changes, or overly permissive rules.
- Identify highly connected and vulnerable assets to prioritize, apply remediation, and reduce risk exposure.
- Regularly review your rules to ensure they align with where your business is today.
- Account for network expansion, such as new workload types (containers, VMs, servers) and LAN with the deployment of SD-WAN.

5. You can assess attack surfaces across cloud, on-premises, and hybrid environments.

As organizations add devices, applications, workloads, and systems, the number of potential entry points expands. It becomes harder to see where the risks exist.

Exposure isn't limited to infrastructure alone. Vendor and partner access can also expand the attack surface. "A lot of times we don't think about it, but some of the biggest breaches happen because of partners who have access," says Egge.

Organizations must consider not only how to protect their cloud, on-premises, and hybrid environments, but also what happens if an attacker gets access.

> **"What can they talk to? Where can they go? How can they get there? Because you could have a really hard outer shell, and all it takes is a little gap."**
>
> **Ricky Egge,**
> Director of Solutions Engineering, Americas, Tufin

He says it ties back to the importance of maintaining a security policy and posture and implementing segmentation or microsegmentation to make it more difficult for attackers to traverse your network.

HOW TO DO IT RIGHT:

- Assess every way an attacker could gain access to your environment, including open ports, outdated software, misconfigured services, and even user accounts.
- Remove unnecessary partner access, patch known issues, and disable services you're not using.
- Apply policy automatically across your cloud, on-premises, and hybrid environments.
- Enforce segmentation to restrict lateral movement and prevent security incidents from spreading across an organization.

Conclusion:
More confidence equals better outcomes

“Security posture is not defined by what is deployed. It’s defined by what is actually reachable,” concludes Tadmor. Ultimately, security maturity comes down to a simple test. You must be able to continuously prove the absence of unintended attack paths.

By decoupling policy from infrastructure, defining ownership, automating change, and evaluating attack surfaces across all environments, organizations can shift from reactive enforcement to proactive validation. As AI accelerates both network change and attacker speed, confidence will increasingly depend on the ability to govern machine-speed activity with continuous validation of what is actually reachable. The result is a continuous journey towards greater confidence and less uncertainty in network security, ensuring better security outcomes for your organization.

Tufin unifies network security technologies into a single control plane to deliver visibility, automation, and continuous compliance.
Visit tufin.com to learn more.

tufin

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.

Learn More