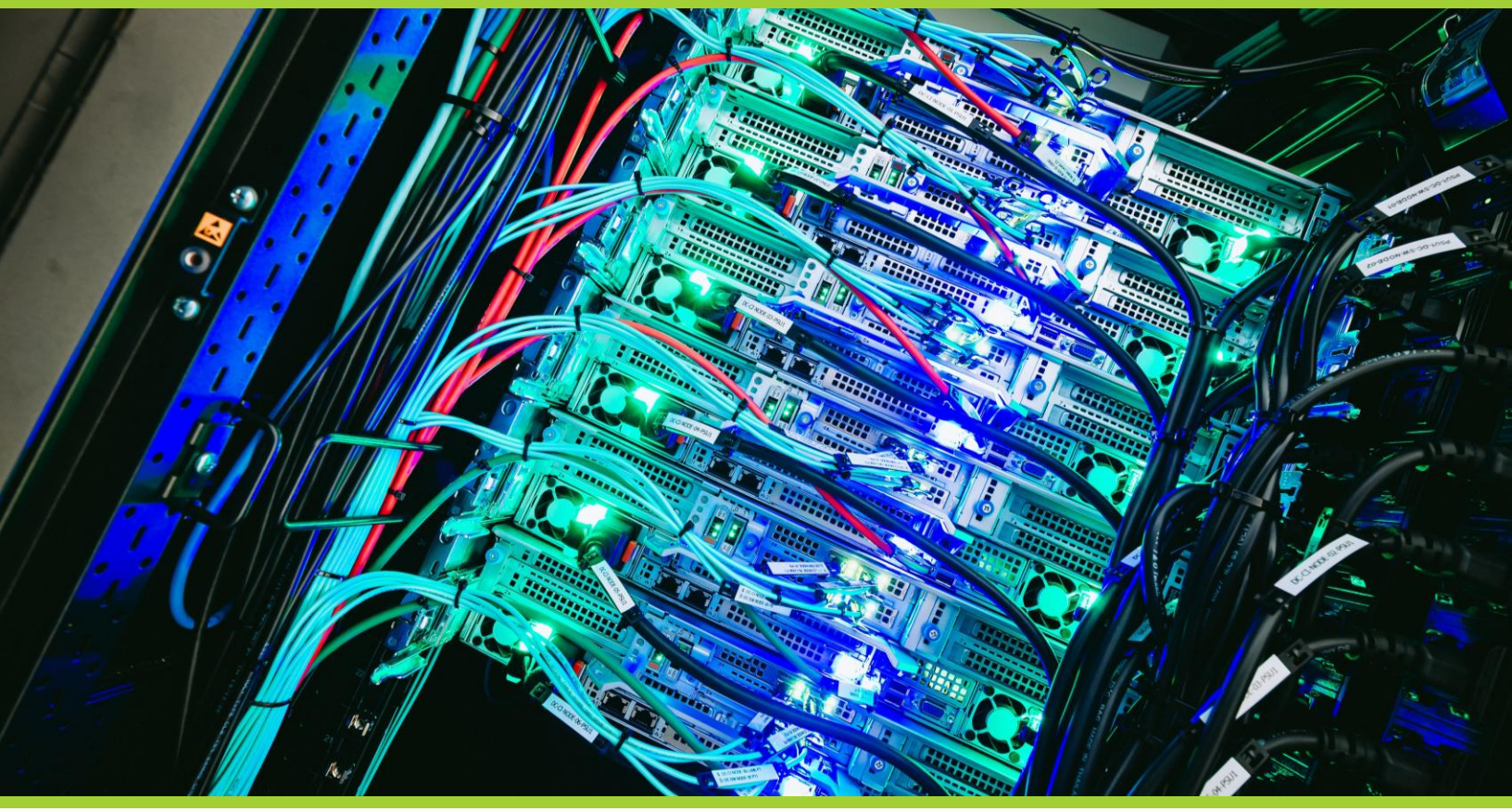
Illinois Department of Innovation & Technology



Microsegmentation:
From Perimeter Defenses to Precision Enforcement

Cybersecurity

State of Illinois
Illinois Department of Innovation & Technology

Initiation: January 2023
Completed: December 2025

Contact: Michael Schnepf | Deputy Chief Technology Officer
Email: Michael.Schnepf@illinois.gov

Illinois Department of Innovation & Technology

Microsegmentation:
From Perimeter Defenses to Precision Enforcement

Executive Summary
Modernizing Network Resilience

Before this project began, Illinois' network security relied on a traditional perimeter centric approach: a few central firewalls were expected to defend a large, aging, and increasingly interconnected environment. Over time, the network grew more complex, with legacy applications, cloud services, and high-volume interagency traffic creating visibility gaps that perimeter tools simply couldn't address. Once a threat actor slipped past the outer defenses, there were limited internal controls to detect and prevent lateral movement.

This created a reactive security posture that struggled to keep up with modern threats, inconsistent enforcement across systems, and recurring audit findings.

To address these challenges, the State of Illinois set a clear project goal: to enhance the overall network security posture and simplify network complexity by decentralizing security enforcement. Rather than depending on perimeter firewalls, the State of Illinois continued down the path to a Zero Trust future by adopting a **microsegmentation framework** that enforces security policies directly on each endpoint. This shift reduces lateral movement risks, increases internal traffic observability, and creates consistent protection levels across both legacy and modern environments.

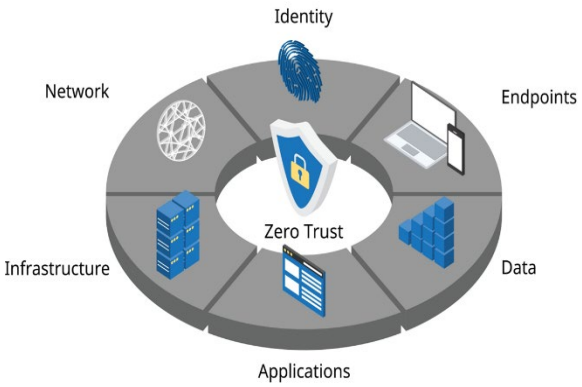
With this objective, the Illinois Department of Innovation & Technology (DoIT) successfully deployed **microsegmentation controls across 3,000 servers,** providing granular visibility and control over **roughly 550 million daily traffic flows**. This marks a major evolution in Illinois' cybersecurity approach and aligns with a core pillar of the state's strategic security roadmap: proactive risk mitigation.

Key Improvements

- **The Pivot:** Replaced aging, reactive central firewalls with decentralized, host-level enforcement.
- **The Scale:** Secured 3,000 servers and gained visibility into 550M+ daily traffic flows.
- **The Outcome:** Reduced lateral movement risks and established a proactive, audit-ready security posture.
- **The Strategy:** Standardized consistent protection across diverse legacy and modern environments.

Idea

Decentralized Security Enforcement



At the heart of this project is a pivot away from centralized defenses and toward a distributed, **Zero Trust model.** By enforcing security policy directly at the host level, the Illinois Department of Innovation & Technology (DoIT) created thousands of individual enforcement points, dramatically reducing how far an attacker could spread if they breached a single system. This approach prevents a compromise on one machine from turning into access to entire network segments or critical applications.

This shift not only modernizes security but resolves longstanding audit findings and compliance challenges. Legacy systems, previously difficult to secure due to their age or architectural constraints, now benefit from compensating controls that shield them from unnecessary exposure. The result is a significantly reduced attack surface, minimized financial and compliance risk, and a level of protection that now meets, and exceeds, the standards required by auditors.

Proactive Risk Mitigation

Remediating vulnerabilities and isolating critical assets strengthened the resilience of Illinois' digital infrastructure. By embedding continuous policy refinement into daily operations, the team ensured that security evolves alongside threats, legislative requirements, and agency needs. This transformation shifts Illinois from a reactive approach to one that provides consistent, automated reduction of risk.

Preventing Lateral Movement

Recent threat activity has validated the approach. On several occasions, adversaries bypassed outer defenses—but micro-segmentation policies stopped them from moving inside the network. Without these controls, attackers could have traveled from the initially compromised host to file shares, application servers, or sensitive data repositories. Instead, host-level safeguards contained the threat to the first system it touched, preventing access to critical systems and protecting high-value data assets. These events underscore the critical importance of decentralized enforcement in modern cyber defense.

Strengthening Compliance & Security

Since the microsegmentation solution was deployed, DoIT has **maintained a 100% pass rate** on network security audits. A key driver of this success is the solution's ability to apply compensating controls to end-of-life systems awaiting upgrade or decommission. The solution has created a consistently strong security posture across an otherwise diverse infrastructure.

Implementation

A Cross-Functional Effort

This project succeeded through close collaboration between DoIT's network, infrastructure, and cybersecurity teams, who led the planning, coordination, and execution of the initiative. While a value-added reseller provided deployment support, DoIT's teams directed the implementation strategy and worked closely with agency CIOs and operational stakeholders to ensure alignment across all environments. This state-driven, cross-functional approach ensured smooth adoption and consistent standards statewide.

Challenges and Resolutions

One of the most complex phases was transitioning from "learning mode" to "active enforcement," where security policies would begin actively controlling traffic. Because Illinois' infrastructure includes thousands of interconnected applications, policy tuning required careful, iterative testing to avoid unexpected disruptions. To address this complexity, DoIT implemented a rigorous validation cycle supported by two full-time engineers dedicated to continuous policy optimization. This sustained operational focus ensures the environment remains agile, resilient, and aligned to evolving application behavior.

Systems, Processes, and Adoption

The solution uses the Akamai Guardicore SaaS platform along with small on-site components that collect and send detailed traffic data. Together, this setup creates a unified view of activity across both cloud and traditional data center systems, supporting microsegmentation principles through consistent visibility. Today, **the platform has reached 100% adoption** across its intended customer base. Through consistent execution and governance, DoIT has standardized micro-segmentation practices statewide, bridging the gap between legacy on-premises systems and modern cloud deployments so all new services inherit a secure baseline from day one.

Risk Management and Operational Maturity

Rather than a "set-and-forget" tool, the platform is continuously operationalized under DoIT's governance model. Real-time flow analysis, scheduled policy reviews, and cross-departmental change coordination ensure that risks are addressed proactively and that the environment remains robust against emerging threats.

Highlights

- Initiative led by DoIT to standardize security across all agencies
- Direct collaboration between DoIT network, infrastructure, and cybersecurity teams
- Over 1,000 interconnected apps protected with unexpected disruption avoided
- Project achieved 100% adoption and optimization success

Impact

Moving From Reactive to Proactive Defense

Reaching full enforcement across state agencies, and managing **more than 10,000 rulesets,** marks a turning point in Illinois' cybersecurity journey. For the first time, **more than 550 million daily flows** are actively protected by host-level policies that stop threats as they occur rather than only reporting on them.

Improving Enterprise Efficiency

The project's impact reaches far beyond security. By centralizing the management of security policies, the state replaced a patchwork of inconsistent legacy controls with a unified, easier-to-operate system. Tasks that previously required coordination across multiple teams and tools are now handled through a single platform with consistent, predictable outcomes.

Audit preparation, once a month-long manual effort involving data pulls, documentation reviews, and cross team verifications, has been transformed into a near-automated state of readiness.

By reducing the potential impact of attacks, simplifying operations, and standardizing protections across diverse environments, the project has made Illinois' digital ecosystem more secure, more resilient, and more efficient, positioning the state for long-term success in a rapidly evolving threat landscape.

Quick Facts