Akamai Customer Story

North Texas City Reduced Risk with Microsegmentation

Three-person IT team secured critical infrastructure, addressed CJIS compliance, and reduced ransomware risk in weeks

Deployed 98% of agents in weeks

Reduced lateral attack risk fast

Gained full network visibility

Protecting critical city systems and CJIS data

A midsize North Texas city in the Dallas-Fort Worth metro area needed to secure critical infrastructure, protect Criminal Justice Information (CJI), and meet CJI Services (CJIS) compliance requirements — without adding complexity for its three-person IT team. With a flat network and no visibility into internal traffic, the city faced significant risk of lateral movement and ransomware spread. By deploying Akamai Guardicore Segmentation, it gained deep visibility, enforced Zero Trust policies, and segmented its environment in weeks — dramatically reducing risk while strengthening compliance and resilience.

Securing a complex environment built for connectivity

Despite its small IT team, the city supports a complex environment: multiple facilities connected via a hub-and-spoke dark fiber network, a police department with a jail and CJIS-regulated systems, supervisory control and data acquisition (SCADA) systems controlling water treatment, and building infrastructure like cameras, elevators, and door access controls.

Over time, the network was built for connectivity, not control. “Our network had multiple virtual LANs, but anybody from anywhere within the city could route to an internal network,” the CIO recalled.

Each facility had its own VLAN, but there were no access controls restricting east-west traffic. A compromised device in a utility building could potentially reach sensitive police systems, including computer-aided dispatch (CAD), CJIS data, and physical security infrastructure.

The city had strong perimeter defenses and endpoint protection, but nothing stopping internal movement.

“I do not want our city to be on the front page of a newspaper because we weren’t secure enough,” the CIO continued. “We don’t have a large staff, so when we invest in software, it has to make a real impact.”

North Texas City

Location
Texas

Industry
Public Sector

Solution
Akamai Guardicore Segmentation

Akamai

Closing security gaps with microsegmentation and Zero Trust

Traditional segmentation — VLANs, firewalls, and Access Control Lists — wasn't designed to control how systems interact inside the network. These coarse controls are hard to maintain, break during changes, and leave too much implicit trust between systems.

To close that gap, the city adopted Akamai Guardicore Segmentation.

Akamai Guardicore Segmentation is a software-based microsegmentation solution that:

- Provides real-time visibility into all application flows
- Maps asset dependencies and auto-labels unknown assets
- Enforces granular, Layer 7 policies to stop lateral movement
- Applies policy consistently across operating systems, environments, and infrastructure — on-premises, cloud, VMs, bare metal, containers, and legacy systems

By shifting the security perimeter to each workload, the city moved to a Zero Trust model — where every connection must be explicitly allowed.

"Akamai gave us that extra layer in our defense-in-depth strategy," the CIO explained.

Rapid deployment by a lean team

The city prioritized rapid deployment to immediately enable visibility and policy enforcement. With just three people on staff, it needed a solution that was powerful but manageable. Akamai provided installation guidance and training, allowing the experienced team to move quickly and independently.

The Deputy CIO packaged the Akamai Guardicore Segmentation agent using the city's existing remote monitoring and management tool, and pushed it across the environment. Within 30 days, the city had deployed 98% of agents.

"Deployment was simple," the Deputy CIO said. "We were surprised how fast we could roll out the solution."

Agents serve a dual purpose, enforcing traffic and generating the visibility needed to confidently apply policies. "Akamai Guardicore Segmentation gave us immediate visibility and control," he continued.

From visibility to enforcement in weeks

Working with an Akamai implementation engineer, the city adopted Essential Policies — pre-built protections targeting high-risk traffic like dangerous ports, malicious IPs, and ransomware pathways. Because these policies don't require asset labeling, the team moved into enforcement within the first month, accelerating its timeline by weeks.

More complex systems required iteration. Ringfencing the Genetec server — supporting cameras, door access, and jail security — took several passes to identify all required traffic. With a hardware-based approach, that unexpected traffic could have caused outages or rollbacks. Using software-based monitoring, the team observed real communication patterns, refined policies, and confidently moved to enforcement without disruption.

"The complexity wasn't a setback. It proved the discovery process worked as designed," the Deputy CIO explained.

> **The added security of Akamai Guardicore Segmentation helps me sleep better at night.**
>
> CIO

Securing crown jewels and critical infrastructure

The city first segmented its most sensitive systems, including Active Directory, public safety networks, and operational technology such as the SCADA systems controlling its water treatment plant.

For Active Directory, the team used a built-in template within Akamai Guardicore Segmentation. This automatically allowed required communication while blocking everything else.

“Akamai Guardicore Segmentation ensured departments that didn’t need access were blocked,” the CIO said.

The city ultimately ringfenced about 20 critical systems, including police networks, the emergency operations center, security cameras, and access control systems. The Genetec server alone saw a 99% reduction in risk.

Visibility uncovered hidden risks

Before deployment, the city had no clear view of internal traffic. Akamai Guardicore Segmentation provided a real-time map of all connections and dependencies.

“The biggest impact was the added visibility,” the Deputy CIO said. “We could drill in, investigate, and then secure it.”

The CIO added, “It gave us more granularity, seeing the ports that were being used. It alerted us to things that weren’t necessarily malicious, but gave us additional insight into what was going on.”

This visibility revealed unexpected internet-to-SCADA traffic. After the city raised the issue, the vendor tightened controls, eliminating the exposure. According to the Deputy CIO, “That situation demonstrated how visibility can drive remediation beyond our internal teams.”

Stopping ransomware by limiting lateral movement

With segmentation in place, the city significantly reduced its risk of ransomware spread. By enforcing policy controls, Akamai Guardicore Segmentation largely eliminated Remote Desktop Protocol (RDP) traffic across the city’s network and tightened SSH controls, ensuring only authorized access and preventing lateral movement.

“That was a big win, because RDP is one of the main ways malware spreads,” the Deputy CIO explained.

According to the CIO: “Akamai Guardicore Segmentation gave me comfort that we weren’t just dealing with north-south traffic. It added that extra layer alongside our firewall and endpoint protection.”

Demonstrating CJIS compliance with real enforcement

In addition to documenting controls, CJIS compliance requires organizations to prove that access to Criminal Justice Information is restricted, monitored, and continuously enforced.

With microsegmentation in place, the city can now:

- Limit access to CJIS systems to only authorized users and services
- See and verify every connection to sensitive systems
- Enforce policies consistently across departments and environments
- Produce clear evidence of control for audits

On a network where any city employee's machine could route to the police department's CJIS systems, compliance was aspirational at best. With enforced segmentation in place, it's now something the city can prove.

Continuous improvement with proactive threat hunting

The city uses Akamai Guardicore Segmentation's Hunt service, a managed threat-hunting operation as part of the solution's extended Exposure Analysis & Response capabilities. The service combines the visibility from deployed agents with Akamai's global threat intelligence to proactively identify vulnerabilities, compromised assets, and abnormal traffic patterns across the environment.

Rather than requiring the city to wait for alerts, the Hunt service delivers periodic reports with prioritized, actionable findings. "I always review the Hunt reports," the Deputy CIO explained. "They give me a checklist of what to fix — it's eye-opening."

The threat hunting service drove real action: The team investigated port-scanning activity surfaced by the service, and used the findings to build and update the RDP and SSH controls that enabled improvements. For a lean IT shop without a dedicated security analyst, the service effectively acts as an extension of the team.

A stronger, more resilient foundation for the future

In just weeks, the city transformed its security posture, reducing its attack surface, improving visibility, and gaining control over internal traffic. Despite its small team, it now protects critical infrastructure, limits the spread of attacks, and enforces CJIS-aligned controls across its environment.

"With Akamai Guardicore Segmentation in place, we can rest easy," the CIO concluded.

© 2026 Akamai Technologies | Support |
| Published 05/26