THREATLOCKER®

X

City of CHAMPAIGN

Case study

How a 24/7 city government reduced cyber risk with Zero Trust enforcement

CUSTOMER PROFILE:

City of Champaign, Illinois

Full-service municipal government supporting police, fire, public works, finance, legal, HR, and administrative operations.

Region served:

Champaign and the surrounding metro area.

Technology leaders:

- **Mark Toalson**, IT Director
- **Brian Perkinson**, Network Engineer

A TURNING POINT THAT RESHAPED THE CITY'S APPROACH TO CYBERSECURITY

Mark Toalson remembers believing the city had a strong security posture. Then a breach in late 2019 and early 2020 exposed how much risk lived inside the environment. The incident forced a complete reassessment of how the team protected public safety systems, citizen services, and the essential digital tools every city department relies on.

Everything the city does now depends on stable, secure technology. Police officers upload evidence. Fire stations operate around the clock. Public works interacts with unknown devices at unpredictable times of day. Finance, HR, legal, planning, and administrative teams depend on continuous uptime. If any one of these systems fails, operations across the city feel the impact.

Toalson had multiple security layers in place, including two different MDR solutions. Even so, he identified a gap: nothing in the stack could reliably stop an attacker who made it past the first line of defense. He needed a control point that could block malicious execution and contain risk automatically. **ThreatLocker® filled that gap.**

> ThreatLocker provides that extra key to block anomalies that nothing else can do. It gives me a great deal of comfort as an IT director.
>
> City of CHAMPAIGN — **Mark Toalson**
> IT Director

FROM UNKNOWN SOFTWARE TO ENFORCED INTENT WITHOUT SLOWING THE CITY DOWN

For a municipality, disruption is not an option. During deployment, the IT team started in ThreatLocker Learning Mode to observe normal activity without interrupting day-to-day work. The team rolled out the agent through Active Directory Group Policy and let staff continue using their systems as usual.

As Learning Mode recorded activity, it built an allowlist that reflected how each department actually operated. It also exposed what software was really in use, including applications the team did not always know had been installed. Champaign got a clearer picture of its environment and a more accurate starting point for policy.

“Learning Mode built our allowlist for us and gave us a clear software inventory across departments. That made the process smooth without a lot of manual work.” — **Brian Perkinson**, Network Engineer, City of Champaign

With that baseline in place, the team could tighten controls with confidence. They were no longer guessing what might break. Instead of chasing every new threat, they focused on allowing only what the city intentionally needed. Everything else stayed out.

COMPLETE VISIBILITY INTO WHAT’S ALLOWED, BLOCKED, AND WHY

Unified Audit became the city’s window into what was happening behind the scenes. For Toalson and Perkinson, this visibility solved a longstanding problem: determining whether an issue came from a real threat or from policy doing its job.

Unified Audit let the team see exactly what was blocked, what was allowed, and whether an update or background change inside an application required attention. It also helped them answer a common question from users: is something broken or is something being protected.

“Unified Audit lets us look granularly at our policies. We can see the things we do not control and understand what is really happening.”

This clarity strengthened troubleshooting and reduced confusion in an environment where dozens of departments have unique workflows and unpredictable patterns of device use.

REDUCED WORKLOAD AND INCREASED CONTROL

With ThreatLocker® in place, Toalson and Perkinson can support public safety systems, administrative departments, and community services with greater confidence. The platform reduced the team's workload, increased control across a wide digital footprint, and created a security posture that protects the city even during overnight hours when police and fire are most active.

The team also gained something intangible but essential: the freedom to offer new services without wondering if they were expanding the attack surface beyond what they could manage.

> ThreatLocker helped us focus our security so that we can confidently add new technologies and services for the citizens we serve.
>
> City of CHAMPAIGN
>
> — **Brian Perkinson**
> Network Engineer

About ThreatLocker

ThreatLocker is a global cybersecurity leader helping organizations proactively stop cyberattacks. The ThreatLocker Zero Trust Platform features Allowlisting, Ringfencing™, and Network Control to prevent breaches before they happen, including zero-day attacks, through an allow-by-exception approach that is straightforward to deploy, scale, and manage to keep business operations running uninterrupted. Built for simplicity, scalability, and speed, the ThreatLocker security stack reduces complexity, accelerates compliance, and empowers businesses to take control of their cybersecurity before threats strike. Headquartered in Orlando, Florida with a growing global footprint, ThreatLocker protects millions of networks and endpoints worldwide. Major partners include JetBlue, Heathrow Airport, the Orlando Magic, and the Indianapolis Colts. The company was recently ranked among the top performers on the Inc. 5000 list of fastest-growing private companies.