

City of Boston: Securing an almost 400-year-old city in the digital age

Increasing public trust by accelerating IT modernization and strengthening cyber resilience with Tanium Autonomous IT



ORGANIZATION

City of Boston

INDUSTRY

Public Sector

HEADQUARTERS

Boston, MA

MANAGED ENDPOINTS

3,500+

USE CASE

Tanium
Autonomous IT
Platform with
Microsoft Intune
and ServiceNow
CMDB



The City of Boston is one of America's oldest and most storied municipalities—a dense, vibrant network of neighborhoods, public spaces, universities, hospitals, libraries, and essential services. Every day, more than 650,000 residents depend on the city to keep life running: traffic lights must function, snow must be cleared, potholes repaired, 911 calls routed, schools and libraries open, and election systems protected.

Behind these services is the Department of Innovation and Technology (DoIT), which secures and operates the systems that keep Boston moving.

Led by Chief Information Security Officer Greg McCarthy and Director of Cybersecurity Operations Phillip Cheetham, Boston's cybersecurity program has evolved significantly in the last decade. What began as a two-person team is now a 20-person organization responsible for endpoint management, identity and access control, compliance, cyber operations, and governance—mirroring the city's broader shift toward digital service delivery.

"Our goal was to get City Hall out of City Hall," McCarthy says, describing Boston's vision to allow residents to interact with government securely from anywhere.



Limited endpoint visibility leads to significant security risk

Modernizing technology in a centuries-old city came with structural challenges. As Boston's IT footprint expanded across police, fire, public health, public works, libraries, and elections, endpoint visibility suffered. "The first idea of security is knowing what your technology is—and we had no good way of inventorying or managing it," McCarthy says.

Endpoints were scattered everywhere—offices, homes, city vehicles, and even public works trucks. Remote work during the pandemic made visibility even harder. Legacy scanning tools were slow, costly, and unable to provide visibility in real time across Boston's more than 3,500 endpoints, Cheetham explains. This lack of endpoint telemetry created significant risk. A major vulnerability or outage could impact emergency services, traffic systems, elections, or other critical public-facing operations.

Challenges:

- A highly distributed endpoint environment spanning offices, remote workers, vehicles, and frontline operations, increased operational complexity and risk.
- Inconsistent and incomplete endpoint visibility across a growing, multidepartment city IT environment.
- Legacy security tools were slow, costly, and ineffective at scale, increasing risk to critical public services.

Benefits

- Closed-loop exposure remediation across 3,526 distributed endpoints citywide.
- Consolidation and retirement of legacy solutions.
- Faster, more efficient Windows 11 deployment.
- Rapid deployment and validation of secure remote access for city employees during the pandemic.

Outcomes

- Accelerated IT modernization and technology adoption.
- Strengthened cyber resilience through reduced exposure windows which help prevent outages to critical public services.
- Lower operational overhead and improved staff efficiency, freeing resources for higher value IT and security initiatives.
- Uninterrupted government operations, enabling secure remote work at scale during COVID-19.

A single platform unifies IT operations and security

Boston turned to Tanium to answer the foundational question: What assets exist across our environment? That first step eventually grew into a broader platform modernization effort that would unify endpoint management and security, leveraging real-time intelligence and automated cyber hygiene.

“The specific feature that sold us was definitely the near real-time intelligence that Tanium provides,” Cheetham says. McCarthy agrees. “You can’t wait three or five hours for answers. You need endpoint intelligence that is up-to-date to make decisions that protect the city,” he says.

By using Tanium in tandem with Microsoft Intune, the city strengthened resilience across its environment through autonomous patch management and configuration enforcement. As a result, the city now applies policies consistently and operates with greater speed, improving compliance, simplifying operations, and reducing reliance on legacy tooling.

Following a recent migration to ServiceNow ITSM, the city also plans to use Tanium to enrich their CMDB with real-time endpoint intelligence. This integration will create a continuously accurate asset inventory and establish a single, trusted source of endpoint truth the city can act on with confidence. With Tanium, Boston gained a true understanding of what was happening across all 3,500+ endpoints at all times.



Key benefits and outcomes

Accelerated modernization and OS upgrades

One of the city's most visible modernization efforts was its Windows 10 to Windows 11 migration. Tanium helped the team identify which systems could be upgraded rapidly, determine which hardware was incompatible, diagnose issues like insufficient disk space, and track migration progress across the city.

These trusted, autonomous workflows provided by Tanium's dashboards allowed the team to watch Windows 10 numbers fall and Windows 11 adoption rise, providing clarity and speed, reinforcing operational continuity and modernization goals.

Improved cyber resilience and rapid incident response

When widespread outages and critical vulnerabilities emerged—including Log4j—Boston relied on Tanium to identify affected endpoints, deploy remediation packages, validate fixes, and shrink exposure windows.

"If we had to wait many hours, we could have been a victim of a breach. Tanium allowed us to remediate Log4j in real time," McCarthy says.

By shortening exposure windows and enabling rapid, governed action, Boston strengthened its ability to prevent service outages that could impact 911 dispatch, public health systems, traffic lights, transportation flows, or digital citizen services.

Operational savings through tool consolidation

With Tanium Exposure Management, Boston retired costly legacy vulnerability tools that were difficult to scale and maintain. Consolidating capabilities into a unified autonomous IT platform allowed the city to simplify workflows, increase accuracy, and reduce the operation burden on staff.

"Tanium has allowed us to consolidate tooling and improve how we manage endpoint devices," Cheetham says.

By turning real-time endpoint intelligence into operational value, Boston increased efficiency and freed staff capacity for more strategic cybersecurity and IT initiatives.

Pandemic agility and continuity of government

During COVID-19, Tanium enabled the city to deploy and validate VPN access for thousands of employees transitioning to remote work. "We wouldn't have been able to send people home if they couldn't connect to VPN. Tanium made that pivot possible," McCarthy says.

For a government responsible for public health and safety, uninterrupted operations were essential—and Tanium made that possible.



"If we had to wait many hours, we could have been a victim of a breach. Tanium allowed us to remediate Log4j in real time."

Greg McCarthy

Chief Information Security Officer
City of Boston

“Tanium was paramount in showing us where our deficiencies were—where we missed machines, why they hadn’t upgraded, and how to fix that.”

Phillip Cheetham

Director of Cybersecurity Operations
City of Boston



How Autonomous IT keeps Boston moving

Since deploying Tanium’s Autonomous IT Platform, the City of Boston’s DoIT team has accelerated IT modernization, strengthened cyber resilience, consolidated tools, and increased the continuity of government.

Accelerated IT modernization

During Boston’s Windows 10 to Windows 11 migration, Tanium’s Autonomous IT Platform enabled the team to quickly identify systems eligible for upgrade, flag incompatible hardware, diagnose issues such as insufficient disk space, and track migration progress citywide, which significantly accelerated adoption.

“Tanium was paramount in showing us where our deficiencies were—where we missed machines, why they hadn’t upgraded, and how to fix that,” Cheetham says.

Strengthened cyber resilience

When widespread outages and critical vulnerabilities emerged—including Log4j—Boston relied on Tanium’s Autonomous IT Platform to identify affected endpoints, deploy remediation packages, and validate fixes. By shortening exposure windows and enabling closed-loop exposure remediation, Boston strengthened its ability to prevent outages that could impact critical public services.

Operational efficiency and cost savings

With Tanium Exposure Management, Boston retired costly legacy vulnerability tools that were difficult to scale and maintain. By consolidating IT operations and security capabilities with Tanium’s Autonomous IT Platform, the city simplified workflows, increased accuracy, and reduced operational burden on staff.

“Tanium has allowed us to consolidate tooling and improve how we manage endpoint devices,” Cheetham says.

Continuity of government

During COVID-19, Tanium's Autonomous IT Platform enabled the city to deploy and validate VPN access for thousands of employees transitioning to remote work, ensuring uninterrupted operations during a critical period.

"We wouldn't have been able to send people home if they couldn't connect to [the] VPN. Tanium made that pivot possible," McCarthy says.

Boston's work with Tanium reflects a broader shift - from siloed tools and limited endpoint visibility to a unified platform approach built on real-time intelligence, rigor, and trust.

"When a resident walks on a newly paved street, votes in an election, or checks a library record, they're interacting with government," McCarthy says. "Tanium helps us keep those services running securely behind the scenes."



Conclusion

The City of Boston demonstrates what is possible when a centuries-old municipality embraces modern endpoint intelligence. With the Tanium Autonomous IT Platform, the city has built a resilient foundation that strengthens public trust, safeguards essential services, and supports the next generation of digital government.

Boston's journey highlights the power of intelligent automation for visibility, rapid response, and unified operations—essentials for any modern city, and indispensable for one of America's oldest.

About Tanium

Tanium is the Autonomous IT company. Driven by AI and real-time endpoint intelligence, Tanium Autonomous IT empowers IT and security teams to make their organizations unstoppable. The company is recognized as a Leader in the inaugural 2026 Gartner® Magic Quadrant™ for Endpoint Management Tools and as a Leader in the IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Device Management 2025–2026 Vendor Assessment. Many of the world's leading organizations trust Tanium's single, unified platform for endpoint management and security to innovate faster, stay resilient and move business forward with confidence, at scale. To learn how Tanium delivers Autonomous IT for unstoppable business – visit www.tanium.com and LinkedIn.



Autonomous IT. **Unstoppable Business.**