

North Carolina powers whole-of-state cyber resilience with Autonomous IT

Securing government agencies, communities, and endpoints with real-time intelligence and control at scale

NCDIT NORTH CAROLINA
DEPARTMENT OF
INFORMATION
TECHNOLOGY

ORGANIZATION

State of North Carolina
Department of
Information
Technology

INDUSTRY

Public Sector

EMPLOYEES

78K+ state employees
& 200K+ across
counties

HEADQUARTERS

Raleigh, NC

ENDPOINTS

168K



Big state. Big target.

The ninth largest state in the U.S., North Carolina is home to more than 11 million residents across 100 counties. Its scale—and the mix of large urban centers and rural communities—means cybersecurity has to work across many different environments and teams, not just a single agency or a single network.

For state governments, cyber resilience is closely tied to operational continuity. When systems are unavailable, the impact shows up immediately in the critical services communities depend on, like EMS, law enforcement, public transportation, and utilities, among others.

“We are a high-target state,” North Carolina Chief Information Security Officer Bernice Russell-Bond explains. “We have institutions and universities doing significant research and generating intellectual property. We have numerous military bases and two ports. Charlotte also has the second largest financial footprint behind New York City.”

But the reality of securing state governments is anything but easy. Disparate agencies with different budgets, resources, priorities, and tooling reveal a disconnect that can create blind spots—the kind threat actors seek to exploit.

“Threat actors see us as a target for disruption,” says Russell-Bond. “All of our systems are connected, so we have to be secure. Because if one system gets compromised, there’s a risk to all of the systems. There’s a risk to the state.”

SecureNC explored

Russell-Bond leads the day-to-day efforts of SecureNC, a statewide program supported by the N.C. Department of Information Technology’s Enterprise Security and Risk Management Office (ESRMO). ESRMO supports SecureNC by strengthening cybersecurity, risk management, and operational resilience with a whole-of-state approach that extends modern capabilities like visibility, control, and response to program participants (cities, counties, school systems, and other organizations) statewide.

And this approach is reinforced by laws allowing the state IT security function to intervene in any North Carolina entity when there is a security threat, helping align response expectations and enabling coordinated action when needed without forcing every local team to adopt an enterprise-sized security model.

“Cybersecurity is not an individual sport. It’s a team sport. It’s everyone’s responsibility, but there are challenges,” Russell-Bond says. “When resources are limited or unavailable, either due to funding or staffing, cybersecurity can become an afterthought—reactive. The irony is it costs more to be reactive.”

Challenges

- Uneven resources across jurisdictions
- Lack of consistent endpoint visibility and risk management across the state
- Need to coordinate response across many independent environments

Benefits

- Browser patching automated and time spent reduced from 10 hours to eight minutes a month
- Increased visibility across multiple tiers of government
- Ease of implementation and usability across agencies
- Automated, repeatable workflows across SecureNC participants
- Google Chrome Browser version sprawl reduced from 117 versions to four



“All of our systems are connected, so we have to be secure. Because if one system gets compromised, there’s a risk to all of the systems. There’s a risk to the state.”

Bernice Russell-Bond
Chief Information Security Officer
North Carolina Department of Information Technology

Enabling whole-of-state security

Improving security would take more than guidance and policy alone. It required deep endpoint intelligence and automation—capabilities that could be adopted in a practical way by participating organizations and used when response timelines were tight.

To support those requirements, SecureNC selected Tanium to help establish a consistent foundation for endpoint visibility and action. Tanium's Autonomous IT Platform supported the state's core needs across endpoint management and security operations, enabling teams to identify what they have, understand what needs attention, and take targeted steps to address issues across their environments.

"Tanium is a strong partner for SecureNC," Russell-Bond says. "It gives us a single platform to verify access risk posture across every agency under our umbrella. Then we can automate risk-based responses with AI and improve security without sacrificing user experience."

Just as importantly, platform automation helps teams do more with the resources they have—turning repeatable work like routine checks, patching tasks, and response steps into reliable workflows that can be applied consistently across different agencies and jurisdictions.

Tanium was designed to be easy to adopt, extending a common set of capabilities across participating

organizations while still accounting for different starting points and technical realities—supporting collaboration without requiring a one-size-fits-all operating model. Participating municipalities also get access to hands-on product training, established best practices, and collaborative support to help protect critical systems and data.

Tanium Autonomous IT delivers resilience at scale

With Tanium supporting SecureNC, participating organizations have a stronger foundation to manage endpoints and improve day-to-day cyber readiness. The program is positioned to help teams answer key questions during investigations, prioritize vulnerabilities, and coordinate remediation steps using consistent endpoint data. One example shows what that can look like in practice.

At the state level, Tanium automates browser patching. That shift reduced the time spent on browser patching from about two and a half hours per week to about eight minutes per month. "Vulnerabilities can happen at any time. So we need real-time information," Russell-Bond says. "Tanium gives us that."

It also helped shrink the number of active Google Chrome versions at a given time—from 117 down to four, with the remaining differences limited to minor version changes. Because Chrome releases patches multiple times a week, the state now automatically



patches Chrome each morning with no manual intervention, keeping browsers continuously updated. The same kind of automation matters even more for smaller jurisdictions, where IT may be staffed by a part-time manager supported by an external vendor.

Unstoppable cybersecurity is a team sport

These capabilities provide consistent endpoint visibility across the state, allowing teams to identify and prioritize vulnerabilities, support investigations and incident response with the context needed to scope and contain issues, and enable targeted, scalable actions that improve cyber hygiene. The result is simpler, centralized security operations built on a unified approach supported by real-time endpoint data and autonomous workflows.

SecureNC reflects a pragmatic view of cybersecurity as shared infrastructure. By pairing a whole-of-state strategy with a consistent endpoint foundation, North Carolina is working toward a stronger baseline for public-sector cyber readiness—one designed to help organizations of different sizes unite to improve visibility, coordinate response, and reduce avoidable risk over time.

In the past four months, nine counties, two higher education institutions, two public school districts, and three cities have enrolled in the program, with another 28 currently evaluating enrollment in the program (eleven counties, four higher education institutions, four public schools, and nine cities/towns).

“The partnership with North Carolina and Tanium is going to make us unstoppable,” says Russell-Bond.

For further information, please visit www.tanium.com



“Tanium gives us a single platform to verify access risk posture across every agency under our umbrella. Then we can automate risk-based responses with AI and improve security without sacrificing user experience.”

Bernice Russell-Bond
Chief Information Security Officer
North Carolina Department of Information Technology



Autonomous IT. **Unstoppable Business.**