runZero

Case Study

How runZero serves as the cornerstone for North Carolina's K–12 exposure management program

Challenge

Coordinating cybersecurity across hundreds of schools

North Carolina's 343 Public School Units (PSUs) faced an enormous cybersecurity challenge — tens of thousands of users, complex environments, and minimal IT support. As Samuel Carter puts it: *"If you had a Fortune 500 company with 50,000 users, you'd expect a multi-hundred-person IT team. Instead, you've got maybe five people — and that's in a well-resourced district."*

Samuel Carter is Systems Architect at the Friday Institute for Educational Innovation, part of the team overseeing the North Carolina K-12 cybersecurity program. Funded by the North Carolina Department of Public Instruction (NCDPI), the program's mission is to protect student data, minimize disruptions, and strengthen the security posture of hundreds of diverse, resource-strapped schools.

"Our goal is to support teachers and students in the classroom by making sure major cyber incidents don't take schools offline," Samuel explains. But with small IT teams, few dedicated cybersecurity staff, and sprawling environments filled with on-prem systems, SaaS tools, student devices, and third-party providers, that's no small feat.

"Trying to provide tools and services to an audience that doesn't traditionally have a cybersecurity background or expertise is very challenging," Samuel notes.

> In security terms, schools are rich in data, poor in resources. They're in the business of educating, not doing cybersecurity."

Samuel Carter
Systems Architect

Problem

No visibility, no coordination, and rising cyber threats

North Carolina's schools were flying blind, with minimal centralized cybersecurity solutions or attack surface visibility — and bad actors took advantage. In 2019, ransomware shut down some schools for days, and in some cases, weeks.

The surge in attacks prompted the state legislature to act, allocating funding and mandating improvements. A major issue on the ground was a lack of coordination and shared resources.

"Each school district was doing their own thing to the best of their ability, but with no coordination. We were duplicating both effort and spending."

At the heart of the problem was a lack of visibility into a highly complex and dynamic attack surface that encompasses a wide array of users — students, teachers, researchers, guests — accessing over 1.3 million IT, OT, and IoT devices across on-premise, cloud, and mobile networks.

"We've got everything from laptops and HVAC systems to vape sensors, card readers, and all kinds of smart devices," Samuel says. *"You wouldn't believe how many robot vacuum cleaners are running around North Carolina classrooms!"*

Asset data was limited in every sense. *"Most asset inventory was just for insurance purposes — serial numbers in various spreadsheets. Nothing that told you what a device did, what was on it, or where the risks were."*

To build a unified and scalable program for the school system, NCDPI needed a solution that could work across hundreds of differently configured, lightly resourced districts — and be usable by staff with limited cybersecurity expertise. It needed to provide visibility across millions of assets and provide exposure detection for all types of devices, including many unknown and unmanageable assets.

> Knowing your assets is foundational to any cybersecurity program, but we didn't have a statewide tool for that. You can't secure assets you don't know about."

Solution

Scalable, agentless discovery and exposure management that's easy to use

After evaluating a number of solutions, runZero stood out for its agentless approach, ease of use, speed, and ability to scan all types of networks and devices.

"Agent-based models are a non-starter for a school environment — they just don't work with that many devices and that few staff."

Initially, the Friday Institute team piloted runZero with seven school districts. Onboarding was fast and hands-on: "Within 30 minutes, we can get a district set up and viewing their assets in runZero. That fast time to value was extremely important."

Within three months, runZero had been rolled out statewide across hundreds of schools and integrated with the state's identity management system. Each district can access the platform, while Samuel and his team have the state-level visibility and oversight they need.

Samuel values runZero's ability to surface richer, more actionable data about their assets and risks compared to other tools: *"runZero tells us more: login pages, screenshots, model numbers — details that help us act faster."*

"runZero's simplicity is a key benefit. Even someone who doesn't know much about cybersecurity can quickly learn and start using it."

After trying runZero, districts said: 'If the state doesn't buy this, we'll buy it ourselves.' That's when we knew we had a winner."

Outcomes

Comprehensive coverage, reduced risk, and faster response

With runZero, North Carolina's schools gained something they'd never previously had: a real-time, accurate view of everything on their networks — from laptops to HVAC systems to robot vacuum cleaners — and any associated exposures that needed to be addressed. That visibility led to tighter security, faster threat response, and more cost-effective decisions.

"runZero gave us a level of visibility we'd never had before. You can't protect what you don't know you have — and runZero shows what you didn't even think to look for."

Districts have used runZero to uncover and resolve a wide variety of risks, such as misconfigured and unknown devices, outdated systems, and anomalies like printers in the wrong VLAN or servers in unexpected locations. Some vulnerabilities posed serious risks.

Equipped with a new understanding of asset-related risks, schools are taking proactive steps to strengthen their cybersecurity posture.

"We're seeing a lot more awareness, self-correction, and proactive measures by schools. runZero opened people's eyes to the risks posed by assets that don't fit in the traditional IT bucket, and schools are using this information to help improve their cybersecurity posture."

An unexpected benefit has been tracking down misplaced assets. When a district reported a missing Chromebook, Samuel used runZero to find it — in another district.

runZero also supports districts to achieve greater cost efficiencies, from effectively prioritizing funding for refreshing assets to unlocking lower insurance premiums via a more accurate asset inventory.

> We discovered some exposures with runZero that could have been catastrophic if they had been found by the wrong person."

At the state level, runZero is central to external scanning and threat response. For example, detecting exposed services that other solutions missed helped the Friday Institute hold third-party vendors accountable and spot risks earlier. Centralized monitoring also eases the burden on schools.

"runZero lets us actively monitor multiple threat intelligence feeds at state level. Schools don't have time to monitor threat intel for thousands of assets — so we use runZero to do it for them."

runZero has even smoothed IT staff transitions. With small teams and high turnover, districts often lose institutional knowledge when someone leaves. *"runZero helps new staff get oriented fast. It gives them a starting point to lead their district's cybersecurity."*

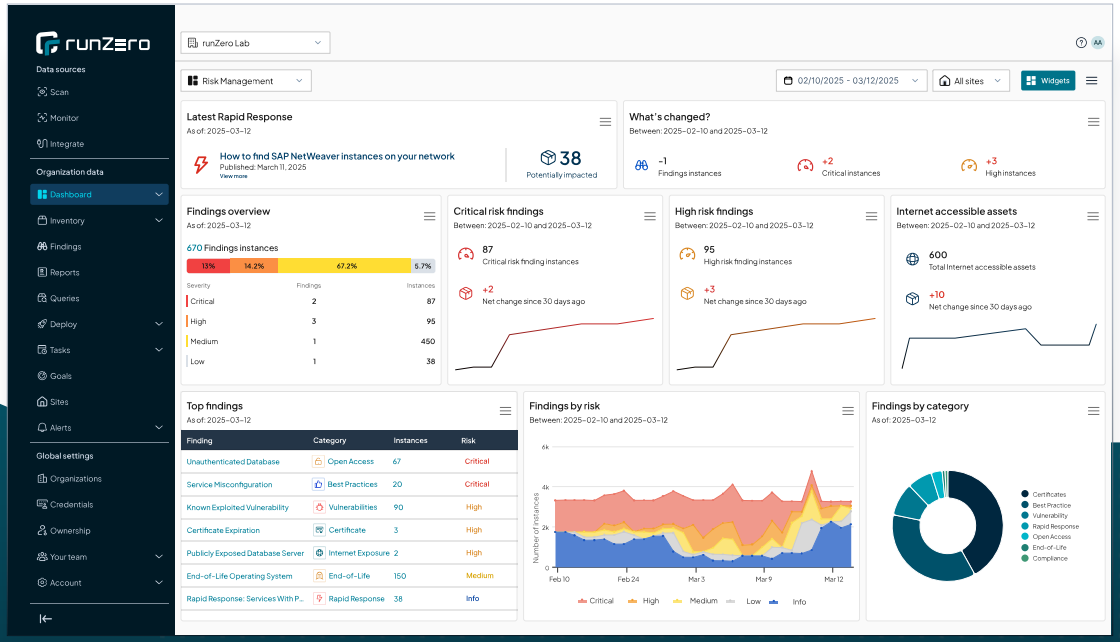
"runZero helps schools spend more effectively because we can use data to prioritize which assets need replacing."

The runZero advantage

For the Friday Institute and the state of North Carolina,
runZero is more than a tool — it's a critical pillar and trusted partner.

"runZero is a cornerstone of our entire K-12 cybersecurity program, helping us truly grasp what assets we have so we can take appropriate actions. It enables us to be very effective and deliberate in our actions to protect K-12 students and staff. The runZero team has been a trusted partner from the start — they've really helped us and genuinely care about what we're doing."

Samuel Carter
Systems Architect



runZero provides a single source of truth for exposure management across your total attack surface: internal, external, IT, OT, IoT, mobile, and cloud. Providing the most complete and accurate visibility into every asset and exposure, runZero helps you mitigate risks faster, meet compliance requirements, and ensure you continuously discover the assets and exposures that others miss.

Try runZero for Free

Discover the runZero Platform for yourself.
Visit runZero.com or start a free 21-day trial.

250724