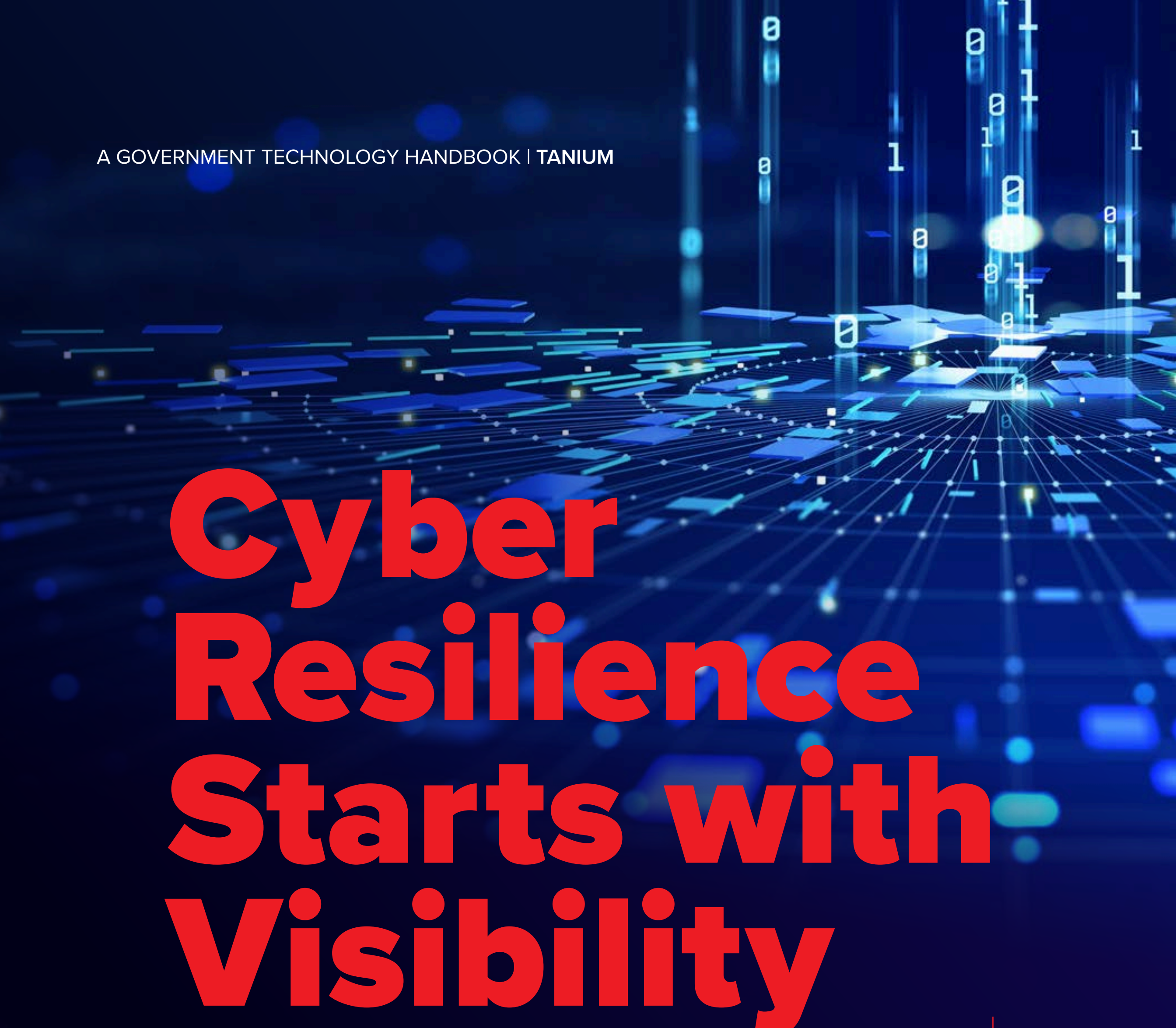
A GOVERNMENT TECHNOLOGY HANDBOOK | **TANIUM**



Cyber Resilience Starts with Visibility

Real-time understanding of assets is the foundation for endpoint protection.

Contents

03 Introduction

04 Four Keys to Understanding the New Threat Environment

12 A Path for Planning & Implementing Endpoint Visibility

18 A Coordinated Approach to Endpoint Visibility

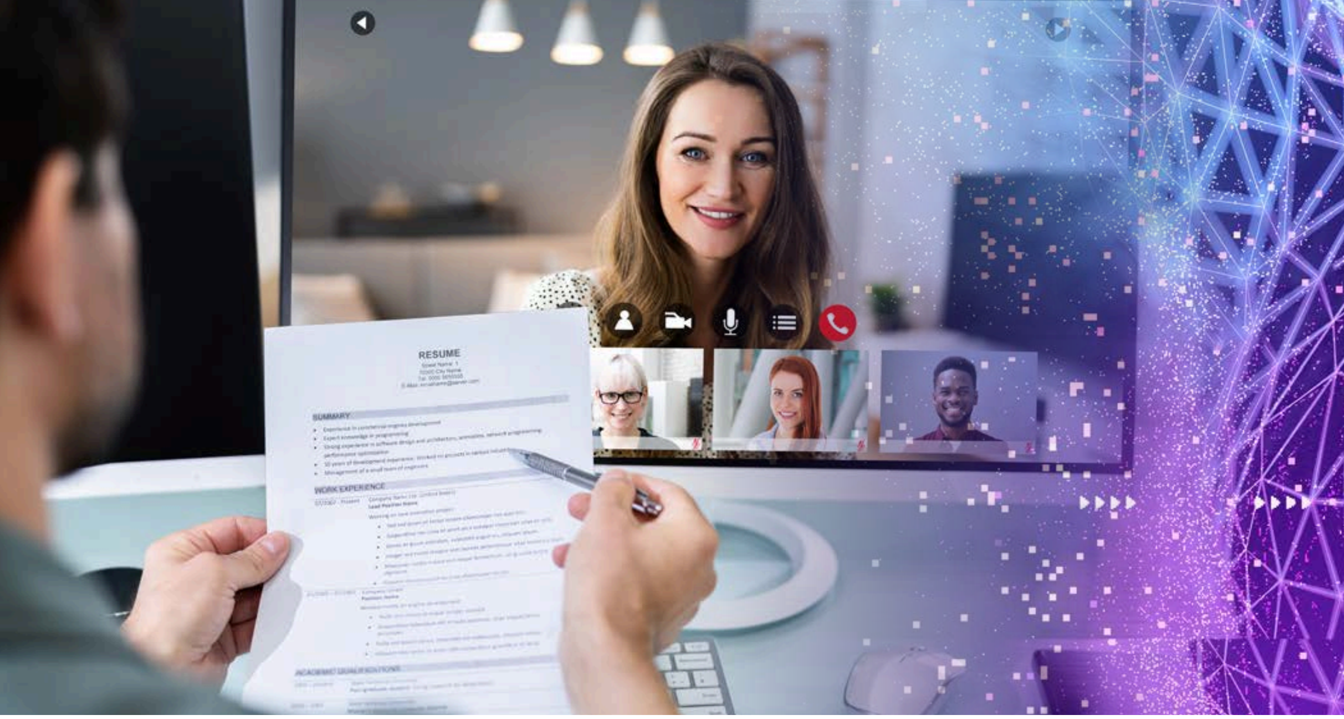
Introduction

The old ways are not coming back. People are mobile and digital — and they intend to stay that way. Government agencies and education institutions that transformed the way they interacted with constituents and students in response to COVID-19, such as launching bold user-facing mobile applications, have changed for good. And when it comes to supporting public employees, faculty and staff, remote and hybrid work options will be essential to agencies and education institutions in attracting and retaining talent.

For all the benefits of these changes, they also bring significant new risks organizations cannot afford to ignore. Every single endpoint – every laptop, desktop, printer, mobile device, server and connected sensor – is an attack vector. With cyberattacks on the rise, agencies and education institutions must adapt to better protect sensitive data and reduce their risk exposure by gaining real-time, accurate visibility into all the devices on their networks.

This handbook explores why real-time, accurate endpoint visibility stands at the center of ensuring digital access for students, constituents, public employees and more. By understanding the evolving threat environment and the real-time visibility technologies that can them adapt, organizations can embark on a journey to a mature — and secure — future of digital government and education.

Four Keys to Understanding the New Threat Environment



Government and education IT leaders must confront permanent changes in the desires and expectations of their key audiences: constituents and employees. Four new realities have emerged.

1 The Endpoint is the New Perimeter

The mobile revolution and bring-your-own-device approach to computing had already been eroding the notion of a conventional security perimeter for years. Then the pandemic, which forced workplaces and schools to close their doors and send employees and students home, rapidly accelerated this shift.

“Almost every CISO and CIO or security team I speak with agrees that the traditional endpoint enterprise perimeter has evaporated,” says Deborah Snyder, senior fellow with the Center for Digital Government (CDG) and the former CISO for the state of New York. The erasure of the security perimeter poses a host of challenges for IT leaders across state and local governments, as well as in education.

“It’s more critical than ever to really understand what’s loaded on an endpoint,” says Michael Makstman, CISO for the city and county of San Francisco. “What software is running? What state is the software in? If we can’t see what’s on our endpoints, attackers could potentially exploit them.”

Far too many IT teams are unable to determine whether the devices and applications on their networks have the latest security patches. Moreover, today’s attack surface includes not only devices, but also any applications and solutions provided by third-party vendors. Private sector software-as-a-service (SaaS) providers, for instance, have become prime targets for cybercriminals attempting to access public networks.

Conventional endpoint management techniques might scan devices every 30 days, giving invaders days or weeks to navigate systems undetected. What does it take to close these gaps?

“We need complete telemetry into the endpoint — the different operating

Obsolete hardware and unpatched software are prime cyberattack vectors, which makes endpoint visibility an indispensable and foundational security capability for organizations.

systems, the different configurations," says Mauricio Angée, associate vice president and CISO for the University of Miami Health System.

Fortunately, a new wave of visibility management software makes this telemetry available. "Now, we can look at which devices are most vulnerable, are not patched and don't have the security controls in place," Angée says.

These endpoint visibility tools install small software agents on devices that send critical endpoint data to network administrators, creating full network visibility around the clock — and across the enterprise. Giving organizations better access to real-time data helps improve risk modeling, but it also makes it much easier to see problems the moment they arise.

"Access to accurate and real-time data is so important, but these tools also give government organizations the control they need to turn around and immediately remediate vulnerabilities, all within a single pane of glass," says Gary Buonacorsi, chief IT architect and chief technology officer for state, local and education with Tanium, a leading provider of network-visibility technologies. The software gives IT leadership a much more accurate, up-to-date picture of the risks on their networks.

"I was just astounded to find so much old, unpatched software," says Walton County (Florida) School District CISO Michael Pinnella. "We even found a couple of Windows 7 machines on our network that we didn't know about."

Obsolete hardware and unpatched software are prime cyberattack vectors, which makes endpoint visibility an indispensable and foundational security capability for organizations.

"I think endpoint management is going to be one of the most important assets in our tool kit," Angée says. The tools will help state, local and education jurisdictions in three crucial areas: Zero-Trust security, regulatory compliance and cyber insurance coverage.

2 Trust is Not Enough

Legacy security tools were predicated on the idea of trusting people to act with integrity once they entered a network. Cybersecurity experts call this model castle-and-moat security: Once users get past the moat, they can roam the castle to their heart's content.

Malicious users exploit this notion of implicit trust.

“Attackers are opportunistic,” says CDG's Snyder. They use automated scripts to identify and infest vulnerable targets. Organizations therefore must make it more difficult to gain – and maintain – access to the network, she says. “The harder you make it for them to get in and stay in, the more disincentive there is.”

This is the core of a Zero-Trust approach to security, which is an application of the principle of least privilege, giving access only to the systems employees need to do their job. A Zero-Trust architecture requires three points of verification:

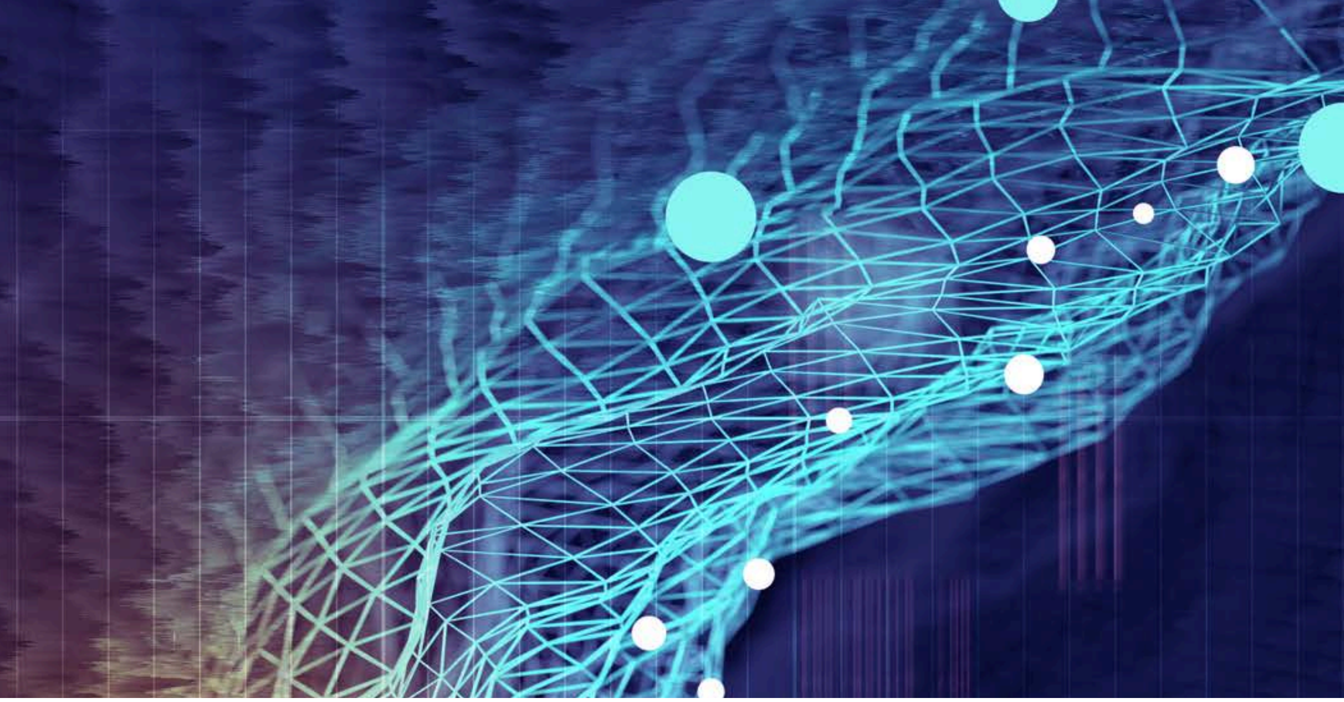
- **Users.** Every network user must be authenticated and granted access only to the resources required to do their work. A robust Zero-Trust strategy employs identity and access management tools to continuously re-confirm users with processes like multi-factor authentication and behavioral tracking, which uses learning algorithms to extrapolate identity from a person's unique patterns of online activity.

- **Applications and data.** All software and data on the network must be verified and judged to be safe. “Zero Trust is also about protecting data at the point of production,” says Matt Marsden, vice president for technical account management, public sector, at Tanium. As organizations generate massive volumes of data, it becomes critical to ensure data is protected at its source.

- **Devices.** Factoring device posture into the Zero-Trust approve/deny process is pivotal to closing endpoint attack vectors. “We need to validate the health of every device,” says Tanium's Buonacorsi. This means knowing what kind of device it is, determining how much access it should receive and calculating the risk profile for that specific device – all acting as pre-requisites for access.

Chris Cruz learned the value of Zero Trust firsthand, having spent two years as the IT director for San Joaquin County, California, before becoming Tanium's CIO for U.S. state, local and education in 2021. “Zero Trust benefited me the most with our highly distributed workforce,” Cruz recalls. “Beyond our VPN connection, our approach made sure that everything coming through our web content filtering system was being managed and had visibility. And when we decided to include device posture in the mix, we really got a sense for how to bolster our endpoint security across the organization. It's important to have a lock on every door.”

As organizations generate massive volumes of data, it becomes critical to ensure data is protected at its source.



3 Compliance is Getting More Complex

Zero-Trust security and device visibility are also becoming more necessary to comply with stricter regulations and government mandates. In May 2021, President Biden issued an executive order to federal agencies to strengthen their security practices and move toward Zero-Trust architectures.[1] Federal security policies often are extended to state and local jurisdictions, so it's reasonable to expect similar compliance mandates across the public sector.

In years past, agencies could "self-attest" that they were following national standards and industry best practices. That won't be enough in the future, says Buonacorsi.

"Going forward, we're going to see much more strict auditing and compliance verification." Organizations will have to prove their use of a specific security standard — not just at one point in time but on an ongoing basis, he says. "Legislatures are trying to put teeth behind compliance. Trust and continuously verify will become the new model, not just trust-and-assume."

This will have large-scale financial ramifications across the public sector. Future federal aid to state and local jurisdictions could make Zero Trust and other advanced security frameworks a condition of approval.

Because endpoint monitoring and security posture validation play a key role in Zero Trust, they will become part of the new regulatory landscape, Buonacorsi predicts.

Cruz agrees, pointing to California's recent Cal-Secure strategy, a multi-year initiative to harden security statewide.[2] "I can tell you that in California, enforced monitoring, endpoint management, patch management, visibility and control are core objectives in the Cal-Secure plan," Cruz says.

4 Cyber Insurance is Changing

State and local security leaders have another reason to improve endpoint visibility,

The most effective endpoint visibility platforms include a scoring system to help IT leaders understand their compliance levels and potential risks.

embrace Zero Trust and ensure compliance: Insurance companies may give them no other choice.

A few years ago, cybersecurity threats often started with a software vendor announcing a vulnerability and offering a patch. Such announcements often cued cybercriminals to create bots that searched for unpatched versions of the software and attacked the vulnerability automatically. Victims of these attacks would file claims with their insurance companies to recover the cost of fixing everything their adversaries damaged. Insurance companies understood the risks, which helped keep premiums consistent from year to year.

Then came the explosion of ransomware, triggering a surge in the costs of cyberattack claims.[3] Insurers responded by raising premiums and reducing coverage.

“It seems the market is undergoing a major correction in recognizing that cybersecurity loss is real,” Makstman in San Francisco says.

The University of Miami’s Angée agrees. “Now we’re talking about co-insurance – ‘We’ll cover half, you cover half.’ That has never been seen,” he says.

In the past, problems arose when customers self-reported their security compliance without actually having adequate controls or endpoint visibility tools in place.

“A lot of people checked the box that said, ‘Yes, we are compliant,’ but they got breached anyway,” Buonacorsi says. Continuous endpoint monitoring could have helped keep them compliant and prevented the breach, leading insurers to start insisting that policyholders have those and other specific controls in place.

The most effective endpoint visibility platforms include a scoring system to help IT leaders understand their compliance levels and potential risks. This IT risk score can illustrate an agency’s maturity on the compliance spectrum — high, medium or low.

“Cyber insurance carriers may decide to use a risk score to determine whether or not they grant insurance to organizations,” says Cruz.

A Path for Planning & Implementing Endpoint Visibility

Because the new security perimeter comprises devices, applications, users and SaaS providers, government agencies and education institutions need to carefully assess their current endpoint visibility and whether their existing tools give them the accurate, real-time data they need.

Before investing in new tools, it's a best practice for government organizations to understand how the tool will fit into their existing IT roadmap. And because you can't protect what you can't see, building visibility maturity is the foundation for digital modernization.

The Plan: Create a Visibility Framework

To form a solid foundation that enables certainty, organizations must assess their current environment, assign people to start an implementation roadmap and formulate a risk-based security framework. These processes also make it easier to choose the optimum technology solution that matches to an organization's needs, priorities and goals.

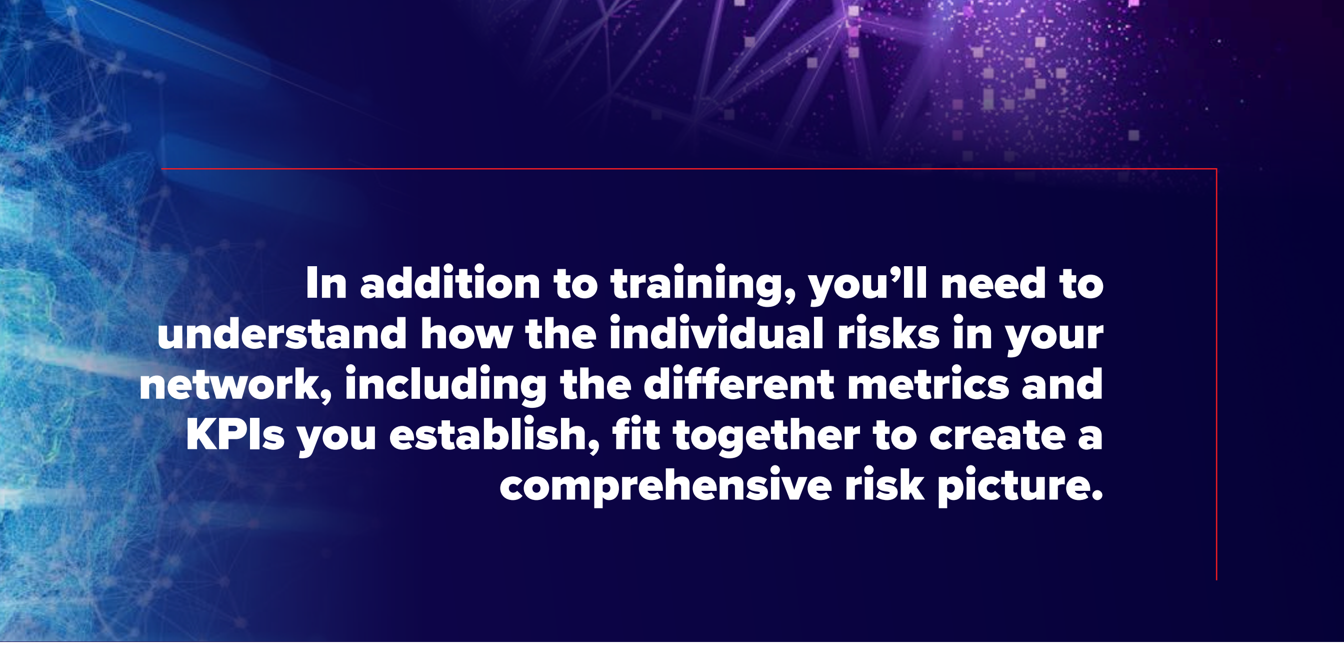
✓ **IT risk assessment.** A comprehensive IT risk assessment is the starting point to secure all endpoints. "You have to know exactly what your estate contains," says Tanium's Marsden. Set egos aside and accept all system shortcomings, he advises. The assessment should identify what's working and what's failing. Depending on your maturity level, you may want to keep tools and processes that are still effective.

The assessment must do more than say, "Let's get better." Be sure to identify specific metrics and key performance indicators (KPIs) to measure progress.

✓ **Steering and governance committees.** Once you've fully assessed your IT environment, you'll need to outline everything you plan to accomplish, including establishing priorities and managing expectations. This requires identifying the right stakeholders to bring into the fold.

Early in the process, form a steering committee of stakeholders who have a vested interest in onboarding new endpoint visibility software.

"Those who are impacted deserve a chance to understand it fully," says Snyder, the CDG senior fellow. "They're your stakeholders." Get their feedback and implement it into your plans.



In addition to training, you’ll need to understand how the individual risks in your network, including the different metrics and KPIs you establish, fit together to create a comprehensive risk picture.

You’ll also need a governance committee that gets key decision-makers on board. This includes security leaders, executives and operations leaders who will help devise a strategy to implement the solution based on the needs and priorities outlined in the IT risk assessment. The governance team will also be responsible for securing leadership buy-in, building consensus across the organization and encouraging adoption.

- **Risk-driven security framework.** You’ll need to bring together new technologies and new risk-management policy considerations, including compliance and insurance, into a holistic cybersecurity framework. Security methodologies like incident response plans must be updated.

- **Training.** Training is essential. “You can’t just buy stuff off the shelf and think your users, operations staff and security teams will step in and know how to use them to their full capacity,” Snyder says. Don’t assume system administrators and support staff will automatically understand the nuances of endpoint visibility technology, either, she says. “Identify your training gaps as you shift to these new technologies. Don’t shirk the expense of services and training.”

  In addition to training, you’ll need to understand how the individual risks in your network, including the different metrics and KPIs you establish, fit together to create a comprehensive risk picture. Stay focused on outcomes rather than outputs, says Marsden. “If you can define a successful outcome, then as regulations are released or updated, you’re not worried about changing individual policies and procedures. You’re just adjusting your tactics to still achieve the same successful outcomes.”

The Implementation: Build Visibility Maturity

Once you’ve created a plan and a framework, you can start assessing, selecting and implementing endpoint visibility software. A successful implementation requires developing use cases, selecting technology partners, creating accountability KPIs and ensuring agility in the future.

- **Develop use cases.** Mapping out use cases is a good way to align your implementation with

your visibility framework. "Develop use cases based on the areas of greatest risk exposure and value to the business from a security risk exposure perspective," Snyder says.

Makstman in San Francisco cautions that you'll need to limit initial use cases to clear, specific needs. Endpoint management and visibility solutions often have a vast array of options, which can make it difficult to know where to start. "We found more success in saying, 'Let's show the value in this use case' and then explore other capabilities," he says.

Makstman notes that implementing endpoint visibility technology may step on the toes of people in different departments. For instance, your tools might uncover vulnerabilities in the utilities department, which may not be accustomed to oversight from IT. "Cybersecurity teams and operational teams often find themselves figuring out new ways of working together," he says.

✓ **Select technology partners.** Finding the right partner is a process that's full of subtleties. The first requirement is deep experience and expertise in your agency's specialty. But success requires you to dig deeper to find the strategic partner that's truly aligned with your interests.

Cruz, for instance, recalls that when he was a government agency CIO, he had developed specific guidelines for choosing technologies. "We didn't just want vendors that sold us software," he recalls. "We wanted partners in opportunity."

What might a partner in opportunity look like? It's a vendor who studies your full computing environment, understands your specific challenges and guides you toward solutions that drive measurable improvements. Moreover, a trusted partner will take you from initiation to implementation to maintenance and support — always optimizing the technology along the way and setting your agency up for success.

This service-driven process builds bonds of trust between organizations and vendors.

Knowing what a partner doesn't look like is also helpful. Buonacorsi recalls the outlook he nurtured over many years as a CIO: "If they were here to sell me a widget today, and I didn't see them for a year until the renewal was coming, that meant they weren't invested in me as a partner."

✓ **Create accountability and KPIs.** Determining measurable goals and staying accountable to them pays dividends throughout the maturation of endpoint visibility technologies. Everyone involved in the implementation needs to feel accountable for the success of the whole project, says Buonacorsi. “It can’t just be operations owning operations and security owning security,” he says.

Organizations must embrace a collaborative approach and a governance structure in which everyone owns the risks to the agency as a whole. This is where you start building accountability into your technology implementation.

Once you have created a collaborative governance structure, then you can jointly develop KPIs to quantify the success of your journey to visibility maturity. Your security governance committee should meet regularly – say, once a month – and make a concerted effort to align executive leadership with overall endpoint strategy.

✓ **Ensure flexibility.** With technologies and cyberattacks evolving so quickly, it’s essential to be as adaptable as possible. It’s imperative to question the status quo, says Buonacorsi. “One of the top challenges for state, local and education organizations is, ‘We’ve always done it that way.’ Government has always been resistant to change, but change is necessary and a constant.”

✓ **Always be alert to unanticipated outcomes.** For instance, the most effective endpoint visibility solutions require installation of a small software agent on every device. This agent is active across the network, which can trigger alerts from other cyber defense tools that scan for anomalies. That’s precisely what the school district in Walton County, Florida, discovered when it implemented endpoint visibility tools.

“Some of our other solutions saw that behavior and thought, ‘Hey, this is almost worm-like’,” says James Gentry, system administrator at Walton County School District. It was an easy fix: Gentry’s team added exceptions to the other solutions to coordinate coverage with the endpoint visibility tools.

Governments tend to stick with what has worked in the past. But in order to respond to new ways of working and increasing cyber threats, they must embrace modern cybersecurity practices to adopt a flexible, agile, adaptable approach.

A Coordinated Approach to Endpoint Visibility

Putting technology to work to automate endpoint security and improve risk management will be crucial for government agencies and educational institutions in the years to come. Assessing current risks and taking a proactive approach to securing the new perimeter can make all the difference.

It's not an easy transition. Developing a framework and a plan for implementation may require an entirely new security paradigm for state, local and educational IT leaders. And staying ahead of ever-evolving cyber threats is a full-time job.

But the underlying principle is simple, Snyder says. "As a practitioner, I can put the future of security in three words: Simplify, integrate and automate."

What to Look for in an Endpoint Visibility Solution

The best converged endpoint management technology should align with your specific organizational needs. To achieve this fit, the solution must be:

- ✓ **Modern.** State-of-the-art endpoint management tools provide real-time insight across a federated IT environment into all your network's endpoints.
- ✓ **Comprehensive.** You need the ability to have full visibility of every device, user, piece of data, application and third-party vendor in your environment. Solutions should use one platform, allowing for a single-pane-of-glass approach for integrating security and operations across an organization.
- ✓ **Multi-tasking.** Find a platform that gives you the ability to control and deploy changes across multiple operating systems, applications and compliance standards. This helps you align your security and operational needs with emerging regulatory, insurance and risk management requirements.
- ✓ **Low-effort.** The best platforms are easy to set up and implement. Monitoring and remediation should be combined in the same tool. User interfaces should also be intuitive and relatively easy to learn.
- ✓ **Collaborative.** A single-pane-of-glass setup, risk scoring and dashboards give everyone involved a unified source of truth on endpoint visibility.
- ✓ **Supported.** The right vendor should provide extensive user support and training as long as employees need it.

Endnotes:

1. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2. https://www.gov.ca.gov/2021/10/22/newsom-administration-announces-first-multi-year-cybersecurity-roadmap-to-protect-californians-privacy-and-security/
3. https://www.insurancebusinessmag.com/us/news/specialty-insurance/ransomware-epidemic-triggers-major-shift-in-cyber-insurance-market-307973.aspx

This piece was developed and written by the Government Technology Content Studio, with information and input from Tanium.

IMAGES PROVIDED BY ADOBESTOCK AND SHUTTERSTOCK.COM

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.govtech.com

Sponsored by: TANIUM™

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Tanium has been named to the Forbes Cloud 100 list for six consecutive years and ranks on Fortune's list of the Best Large Workplaces in Technology. In fact, more than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty. Visit **www.tanium.com** and follow us on **LinkedIn** and **Twitter.**