How to Mature Endpoint and Visibility Management for Public Sector Agencies

In an increasingly connected world, securing endpoints can be a challenge, but with the right steps and tools, any organization can be ready for whatever comes next.

By Chris Cruz

State, local, and educational organizations are tasked with serving constituents, students, businesses, and staff by delivering services, expanding economic opportunities, and improving crisis response. With increasing emphasis on cybersecurity readiness, IT leaders have been tasked with protecting communities and departments, with less resources to execute across all areas. With users being more distributed than ever, the endpoint has become the most vulnerable frontier from a cybersecurity perspective, and it needs to be secured.

How to Be More Confident in Your Patching & Compliance

Many organizations don't have confidence in answering questions such as: "How many devices do we have?" "How are we measuring data privacy risk today?" or "How do we scope an attack that has been around longer than 90 days?" No matter how confident you are in answering these questions now, it's never too late to look at maturing your cybersecurity posture. According to the CSO Pandemic Impact Survey, 61 percent of security and IT leaders are concerned about increased cyberattacks targeting remote workers. It's time to get ahead of the curve.

According to the CSO Pandemic Impact Survey, 61 percent of security and IT leaders are concerned about increased cyberattacks targeting remote workers. It's time to get ahead of the curve.

But where to start? How can organizations begin maturing their cybersecurity posture? It all starts with visibility of their endpoints – on-premises, in the cloud, or fully remote. Because you can't control what you can't see, organizations must first shed light on all of the endpoints that are inside or even outside of their environment. Are your endpoints doing the heavy lifting for endpoint visibility and discovery? The most effective technologies use agents installed on networks to passively or actively identify the devices they are physically near or those they have recently contacted. Central scans can be configured, but are often not as useful due to complicated network firewalls and perimeters.

Barriers to Visibility

When organizations think about cybersecurity, a common sentiment is that a hack is "bound to happen" and "there's nothing we can do beyond what we're doing now." And because budgets are tight and the problem is complex, it's no wonder the news headlines are full of new examples of ransomware attacks on the public sector. Many of the tools that organizations use today do not give full visibility and control to endpoints because those tools must be loaded on every known endpoint. Luckily, there's been a lot of development around the practice of finding unknown and unmanaged endpoints.

Another strategy to dealing with a hack is falling back on insurance coverage; some organizations see it as their best defense. For now, you can outsource financial risks, but what about the lasting impact of a public relations disaster? And, what about the value of having a good offense? Banking on insurance coverage may be increasingly expensive in the long run, so it's best to be proactive with securing your endpoints and thinking outside of the box to do so.

Closing the Gap

To close these gaps, organizations need endpoint management and security tools that provide the visibility, control, and rapid response required for managing endpoints efficiently, thus improving and accelerating incident response, and achieving strong IT hygiene at scale. Once you've got visibility into the assets you have milling-about in your environment, it's time to focus on controlling those assets in a comprehensive way.

To close these gaps, organizations need endpoint management and security tools that provide the visibility, control, and rapid response required for managing endpoints efficiently, thus improving and accelerating incident response, and achieving strong IT hygiene at scale.

For example, if you find that unpatched laptop, the next step is to patch it as soon as possible, and to make sure you can answer questions like, "Why is this laptop not patched?" and "Where is it located?" What if the next 30 laptops you find are on different versions? What if users continue to decline the updates? How do you monitor for configuration drift? Having control over these scenarios and the ability to find the information you need, in realtime, is critical to your organization's success.

When it comes to having comprehensive control, there are a few areas where organizations can focus. One area is tool and cost optimization control. With a distributed user-base, this need is greater because IT administrators have even less oversight around what tools are being used. The first step to cost reduction is identifying the problem: 1) do you have unused or underutilized hardware (hardware with little load) and 2) do you have underutilized software? If only 75% of users with licenses for a particular software have logged in within the last six months, do they really need it? Being able to pose and quickly answer questions like these will be highly impactful in increasing efficiency and reducing operating costs.

Once your costs and tools are optimized, the next step to endpoint management maturity is focusing on data privacy. How are you measuring your data privacy risk today? What are your biggest concerns? These are tough questions to answer across an entire distributed environment, but having the right tools can help you avoid opening Pandora's box, by giving you a comprehensive view into the sensitive data being stored in your environment, and the steps you can take to secure that data.

Securing your organization is no longer a "budget-allowing" line item. It's not nice-to-have; it's a must-have, essential spend that every state and local government and educational institution must plan for.

Hackers are moving faster now than ever. How do you plan to respond to incidents on-premises or off? How are you working to reduce mean time to resolution? Effective incident response is about confidently running through the stages of an incident: from better identification, to scoping, all the way through to remediation and lessons learned. Incident response does not happen in a vacuum; many incidents are the result of missing patches and lack of compliance or not following the rules. Getting a handle on these activities is tough – but necessary, and possible with the right tools.

Being Ready for.... Whatever Comes Next

Securing your organization is no longer a "budget-allowing" line item. It's not nice-to-have; it's a must-have, essential spend that every state and local government and educational institution must plan for. Is your organization ready for reduced shadow IT? Endpoint compliance? IT cost optimization? Mature endpoint management? Make sure you're ready for whatever comes next.

Tanium has helped numerous government, and educational organizations gain unprecedented visibility and control over their IT environment. For a complimentary gap assessment and to learn more about how your organization can improve its cyber hygiene, visit https://www.tanium.com/cyber-hygiene-assessment/.

About Chris Cruz

Chris Cruz has over 30 years of experience in government. Most recently, he served as Director and CIO for the County of San Joaquin, California. Prior to this position, he served as the State of California's Deputy CIO, where he led the State's Data Center and Information Cyber Security Program for four years.

Cruz's government experience has spanned healthcare, public health, finance, food and agriculture, law enforcement, general government, and IT infrastructure, project management, applications, and procurement. In addition to these government entities, Cruz spent several years in executive leadership positions, serving as the CIO for both the California Department of Food and Agriculture and Department of Health Care Services, and he was the first CIO for the Health Benefits Exchange, now referred to as Covered California.

Cruz is a staunch believer that you can never have enough security to protect your most critical assets, and serves as an advisor to the Tanium State, Local, and Education business at Tanium.

About Tanium

Tanium offers an endpoint management and security platform that is built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.