The Enterprise Approach to Unified Endpoint Management and Security

How Tanium helps government IT operations and security teams gain unparalleled visibility and control

Introduction

The top priority for state CIOs in 2020 is cybersecurity and risk management, according to a survey by the National Association of State Chief Information Officers (NASCIO).[1] Similarly, cybersecurity was the No.1 technology trend likely to have an increased focus over the next year according to the Center for Digital Government's (CDG's) 2019 Digital Cities and Counties surveys. Consider the plight of Dunwoody, Ga., which lost an estimated $80,000 in the wake of a cyberattack.[2] Or North Dakota, where state government officials reported cyberattacks increased by 300 percent in 2019.[3]

To reduce their risk, governments have been investing in software to protect their network endpoints. Unfortunately, this strategy still leaves infrastructure open to bad actors and malicious code. The problem is, governments usually implement point solutions — dozens or hundreds of discrete software products, each to solve a different issue. Without a complete inventory and central control of the enterprise, an IT organization can't fully protect its infrastructure and data.

This paper explains how Tanium's platform for enterprise-wide, unified endpoint management and security helps make governments strong and agile in the face of ever-evolving security threats. Used on its own, or alongside legacy solutions, Tanium's operations and security platform helps keep the entire IT infrastructure safe while helping organizations operate more efficiently.

Why Point Solutions Don't Work

In many government IT organizations, two main obstacles obstruct efforts to manage and secure a network's endpoints. The first of those is poor visibility.

All too often, IT managers lack a full picture of what devices and software are operating on their infrastructure. When Tanium audits an organization's network, it typically identifies 10 to 20 percent more endpoints than managers realized were present.

This knowledge gap can create risk. When managers don't know what is on their network, they can't keep those endpoints up to date, patch them as needed, safeguard them against new cybersecurity threats or otherwise maintain what we call good IT hygiene. Trying to secure a network without a comprehensive understanding of its endpoints is like trying to burglar-proof a building without knowing the number and location of its doors and windows. It doesn't matter how well you've locked and alarmed most of the potential entry points. Leave a single tap in the system, and a thief can find a way in.

Two main obstacles obstruct an agency's efforts to manage and secure network endpoints:

1. POOR VISIBILITY

2. POINT SOLUTION SPRAWL

In the case of a government network, one unsecured "window" could lead to a ransomware attack that costs the agency millions of dollars, or a breach that leaves terabytes of sensitive data lost and unrecoverable.

Consider a large government agency that has 30,000 endpoints of all types — workstations, servers, laptops, printers, point-of-sale systems, identification card scanners and the rest. If IT staff are unaware of 10 percent of those endpoints, that means approximately 3,000 devices could be going unpatched and unsecured, leaving them — and the entire network — highly vulnerable to hacking and malware.

Poor visibility also drives up costs. If IT managers aren't aware of the assets on their network, when renewal notices for licensing agreements arrive, how can they know if employees are actually using all the software these agreements cover? The organization could go on for years paying fees for software it doesn't need.

The second obstacle that keeps organizations from properly managing and protecting their networks is point solution sprawl. Today, a typical set of endpoints may have anywhere from eight to 20 different agents, each of them implemented to address a specific management or security issue. Each of those agents needs its own infrastructure, along with staff who have the necessary skills to support it. All of this drives up network maintenance costs. In addition, someone needs to keep each agent, and the dedicated infrastructure it may require, up to date with patches. If the IT department doesn't stay current with those updates, the agent — while trying to protect the endpoint — could instead create its own vulnerabilities. Every delayed patch creates a new risk.

What's more, there may not be integrations among these disparate niche solutions. That means there may not be a way to obtain a true, comprehensive picture of a network without conducting heavy manual manipulation of data from each agent. In that situation, getting an enterprise-wide update on the status of an organization's endpoints can take weeks or months. By the time IT staff have gathered the data from multiple sources, normalized it and compiled a complete report, that information is long out of date. In a world where new cyberthreats arise every day, and where malicious code can become active the instant it invades a system, long delays in understanding the status of endpoints leave an enterprise at risk.

Given the prevalence of hybrid cloud environments in government IT, the challenge of enterprise-wide endpoint security is becoming even more complex and difficult. In a hybrid cloud environment, endpoint agents can be spread across many physical locations, where they don't communicate with one another and are harder to monitor.

Tanium's Enterprise-Wide Solution

At many government agencies, management tries to approach cybersecurity as a top-down issue. This is a mistake. Cybersecurity is actually an operations issue. An agency cannot protect its IT infrastructure until it gains a comprehensive view and thorough control of its endpoints, across the enterprise. IT management must be able to answer questions such as:

- How many computers and other devices are on the network, and are they authorized to be there?
- What applications are installed? Are they all up to date?
- What are users doing? Is that activity authorized?
- How comfortable are you with your patch/vulnerability/risk posture?
- Have you recently experienced a breach or an outage that could have been prevented?

Continued on page 4

THE ADVANTAGES OF AN ENTERPRISE SOLUTION

As it gives IT staff the ability to see, manage and secure endpoints throughout the enterprise, Tanium's solution offers several additional features that make it a superior solution:

IT DOES NOT REQUIRE AN ORGANIZATION TO REMOVE ITS LEGACY POINT SOLUTIONS. Tanium's solution can supplement niche products already in place, filling in gaps to provide comprehensive visibility and security across the enterprise. An agency can use Tanium's dashboard to monitor endpoints, including those protected by other solutions. This approach protects an agency's existing investments, conserving taxpayer dollars. It also lets an agency implement Tanium's technology incrementally.

TANIUM WORKS EQUALLY WELL ON PREMISES, IN THE CLOUD AND IN COMPLEX HYBRID ENVIRONMENTS. This is particularly important, given an agency could have multiple cloud providers for different purposes, based on business needs and cost considerations. The more complex the environment, the more crucial it is to have a single source of truth to understand things like the cost of licenses and regulation compliance. Without a platform that helps monitor and control its endpoints, no matter their location, the enterprise will become more vulnerable over time.

IT REDUCES THE TIME, LABOR AND EXPENSE REQUIRED TO KEEP ENDPOINTS PROTECTED. The U.S. Air Force implemented Tanium's technology in a system it calls Automated Remediation and Discover (ARAD), which it ordered to be deployed on nearly all of its systems by May 2017. That same month, when the WannaCry ransomware attack hit computers around the world, the Air Force used ARAD to implement protections against this malware. The process took less than an hour.[4]

The administrator who located the WannaCry threat through ARAD needed about 20 seconds to locate 52 endpoints that displayed a total of more than 500 vulnerabilities to the attack. Using the results of this query, the financial management team at Ellsworth Air Force Base determined which endpoints were most vulnerable and what needed patching. The team took seconds to complete this inquiry, rather than the weeks it would have taken before to assemble the necessary information.[5]

Ellsworth Air Force Base

Continued from page 2

The best way to gain control over the agency's IT infrastructure is to implement a solution specifically designed to address the enterprise. Tanium's solution for unified endpoint visibility and control helps provide that system-wide oversight within four main functional areas:

Core. Tanium's core platform is a central hub that receives information from the agents on the infrastructure and consolidates that data in a single dashboard. There, managers gain real-time visibility into and control over endpoints. Through this single pane of glass, they can quickly find answers to their questions, allowing them to gain insights through trends in data. The core platform can also integrate with third-party tools and exchange data with them.

Operations. This set of tools provides a real-time inventory of endpoints — a single source of truth about what is happening on the network and on individual devices. Staff use it, for example, to maintain an up-to-date record of devices, software assets and dependencies. It allows staff to manage software distribution and keep patches current, understand user activity on the devices, and perform other work to help make sure systems are healthy and performing well.

Risk. Tools in this area help track sensitive data on the network, keeping staff informed on how that data is being used, how well it's being managed and whether any of it has been compromised. The risk capability also monitors unauthorized changes or access to this data. Using these tools, an agency can more easily comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

Security. Tanium's security tools help detect, investigate and remediate security issues in minutes — not the hours or days that some other solutions require. As hardware and software manufacturers monitor new threats and potential vulnerabilities in their products, Tanium compiles that information and incorporates it into its security tools, helping to ensure endpoint protection is current.

Bringing an End to Point Solution Sprawl

When a government agency implements Tanium's solution, agency leaders and elected officials can rest assured their enterprise is operating more resiliently. At the same time, the technology frees IT staff from the routine tasks required to maintain disparate point solutions, allowing them to focus on projects with greater value to the enterprise and the public.

By providing real-time inventory and up-to-date patching of vulnerabilities, Tanium's solution reduces the risk that an agency will fall victim to ransomware, averting shutdowns and potentially saving thousands of dollars.

Tanium's technology allows IT leaders to take advantage of the benefits of cloud products, confident of their ability to manage its endpoints in the most complex hybrid environments. Finally, Tanium's solution provides real-time visibility, empowering IT leaders with comprehensive control of the enterprise.

The age of point solution sprawl is over. Governments require a holistic, unified endpoint platform that reduces costs and risks. The Tanium platform for enterprise endpoint visibility and control provides that level of visibility, giving governments a fast, thorough and cost-effective way to protect their networks and data.

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

Endnotes

1. State CIO Top 10 Priorities, NASCIO, https://www.nascio.org/wp-content/uploads/2020/01/NASCIO_CIOTopTenPriorities.pdf
2. J.D. Capelouto, "Georgia City Estimates $80K Cost After Cyberattack," *Atlanta Journal-Constitution*, January 28, 2020, Georgia City Estimates $80K Cost After Cyberattack
3. Sydney Mook, "North Dakota Reports 300 Percent Increase in Cyberattacks," Grand Forks Herald, Jan 17, 2020, https://www.govtech.com/security/North-Dakota-Reports-300-Percent-Increase-in-Cyberattacks.html
4. Jared Serbu, "Air Force to release new 'fast-track' cyber approval process," Federal News Network, December 1, 2018, https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2018/12/air-force-to-release-new-fast-track-cyber-approval-process/
5. Tyra Jackson, "WannaCry? Not about ARAD," Ellsworth Air Force Base, August 11, 2017, https://www.ellsworth.af.mil/News/Commentaries/Display/Article/1276428/wannacry-not-about-arad/

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**

For: TANIUM

Tanium offers a unified 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 government and enterprise organizations, including more than half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium ranks 7th on the Forbes list of "Top 100 Private Companies in Cloud Computing" for 2019 and 10th on FORTUNE's list of the "100 Best Medium Workplaces." **Visit us at www.tanium.com and follow us on LinkedIn and Twitter.**