IT Modernization and Tools Rationalization for Federal Agencies

Why federal agencies must abandon legacy methods of data centralization and adopt a new, modern approach to endpoint security with real-time data instrumentation at the edge

Table of Contents

Introduction:
What SolarWinds Reveals About Federal Government Cybersecurity 3

Yesterday's Tools:
Why Existing Security Solutions Won't Stop Today's Threats 4

The Looming Data Crisis:
Why Legacy Approaches Will Break Even If Things Go Back to "Normal" 5

New Research:
How Legacy Approaches Fail to Deliver Acceptable Outcomes 5

A Practical Approach:
How to Rationalize and Modernize Agency Tooling 6

Meet Tanium:
How the Tanium Platform Drives IT Modernization 9

The Need to Change Now:
Why Agencies Must Update Their Tools 10

Making the Change:
Learn How Tanium Can Help 11

Introduction: What SolarWinds Reveals About Federal Government Cybersecurity

In 2020, the federal government experienced a massive public breach. The government's technology vendor, SolarWinds, was hacked and multiple agencies were compromised — including the Pentagon, the State Department and the Treasury.[1]

Like most breaches, we may never know the full extent of the damage that it caused, but it has already taught us three hard lessons about government cybersecurity:

1. Federal agencies are more vulnerable than anyone thought.
2. Their security tools are no longer effectively defending them.
3. Agencies require a new approach to managing, utilizing and securing their data that is appropriate for modern environments and threats.

Federal agencies must take these hard lessons to heart and upgrade their security, adapt to their current threat landscape, and more effectively secure their assets. This ebook provides guidance for each of these crucial steps. It will explore:

- Why existing security tools are no longer keeping federal agencies safe
- A practical approach that federal agencies can follow to rationalize their security tools and modernize their IT infrastructure
- How agencies can bring this approach to life with Tanium
- Why agencies have a unique need to upgrade their tooling right now

Yesterday's Tools: Why Existing Security Solutions Won't Stop Today's Threats

There is a simple reason why federal agencies recently experienced one of their biggest public breaches in history, and why their existing tools were unable to defend them against this threat. Technology has advanced and the tools and tactics employed by cyber adversaries have evolved, yet many agencies haven't yet adopted the right tools to secure their networks and data.

Here are some major changes that have occurred:

- **The federal workforce moved from a majority on-premises environment to a mostly distributed workforce.** According to recent findings from the Pew Research Center, 71% of employees have continued to perform most of their work at home all or most of the time, compared to just 20% before the pandemic.[2]

  Deloitte reports that the federal government workforce followed a similar trend, stating, "…just 22% of federal employees teleworked for even a single day in 2018, the most recent year for which data is available. Yet, virtually overnight, over 75% began working remotely at various agencies and continue to do so effectively."[3]
- **Massive endpoint distribution beyond the traditional perimeter increased risk.** Agencies have spent more than a decade building in-depth defense around their on-premises workforce with what most would now consider to be legacy tooling. Almost overnight, most of their employees left the office and began to work remotely. The traditional perimeter that most agencies relied on to protect sensitive data and government devices was no longer effective because it was designed to protect only the things within its walls.
- **Government agencies flooded their networks with new endpoints, data and connections.** According to recent research, after COVID-19, organizations increased their volume of heavily used devices by 11%, increased the volume of sensitive data stored on their devices by 62%, and adopted 176% more collaboration apps.[4] While some federal employees continued to use their government-furnished equipment, others turned to bring-your-own-devices (BYOD) to continue their work and access agency networks and data.

These events have turned many federal agencies into large soft targets. The on-premises model and the security practices, assumptions, and tooling that supported it collectively put federal networks and endpoints at significant risk. And yet, many agencies continue to try to secure their networks with security tools designed to defend their old, mostly on-premises networks.

These legacy security tools:

- **Were built on hub-and-spoke architecture.** They require dozens or hundreds of staging servers to perform simple endpoint management and security tasks. This requirement prevents them from scaling quickly alongside rapidly changing networks, and forces them to consume a high amount of bandwidth to scan and apply security controls to large, distributed networks.
- **Use centralized data collection.** To perform any security analysis and make any security decisions, they must first pull all relevant data from the network and store it in a central repository. This process prevents them from scaling data collection as the volume and velocity of data in their network has grown and forces them to make security decisions from limited, stale data sets. The result is uninformed security actions or total inaction.
- **Perform security analysis on stale data sets.** Because they can perform periodic spot scans only on their networks, they are commonly forced to perform security analysis on endpoint data that is days, weeks, or months old. This gap prevents them from performing real-time analysis of fast-moving modern threats, or from feeding new security models like Zero Trust with accurate, relevant data.
- **Require dozens of siloed point tools.** Most legacy security tools are point solutions designed to solve a single, specific problem. This narrow focus forces agencies to adopt an increasing number of point tools

to secure the increasing diversity of asset types and vulnerabilities in their networks. Our own research showed that 48% of federal agencies have 11 to 25 different security tools, and 21% have 26 to 50 different security tools. These point tools commonly don't work well together and create increasing complexity, cost, risk, and blind spots. Research from the Ponemon Cyber Resilience Study found that 63% of security teams are spending more time managing their tools than they spend combating threats, and 53% of teams believe their excess volume of security tools is actually making their security posture worse.[5]

Federal agencies are still utilizing legacy security tools that were built years ago to secure endpoints that stayed within the perimeter. At the time, that tooling wasn't inherently bad; it operated in the way in which it was intended and met the needs of agencies. But today's networks are very different, and legacy tooling simply wasn't designed to identify and protect endpoints distributed at scale and massive amounts of data.

It's critical to find a new approach— and find it ASAP.

The Looming Data Crisis: Why Legacy Approaches Will Break Even If Things Go Back to "Normal"

It's tempting to believe these problems with legacy security solutions will go away if and when we get to the other side of this pandemic and agencies consider returning to their offices. However, this thinking is a fallacy. The pandemic simply accelerated digital transformation changes that were already occurring, and that will continue to accelerate over the coming years – no matter what happens next.

The instrumentation, collection, centralization, normalization, and analysis of endpoint data in a timely fashion now drives all decisions in IT. This pivot has brought the industry to an inflection point where there is already so much data that it's becoming impossible to store it in a usable manner through centralized collection methods and legacy tooling.

This problem will only increase as data volume explodes in the coming years. International Data Corporation (IDC) projects data volumes will increase at a compound annual growth rate of 61% and increase from 33 zettabytes in 2018 to 175 zettabytes by 2025. At that point, IDC projects there will be 41.6 billion connected devices producing almost 80 zettabytes of data per year.[6]

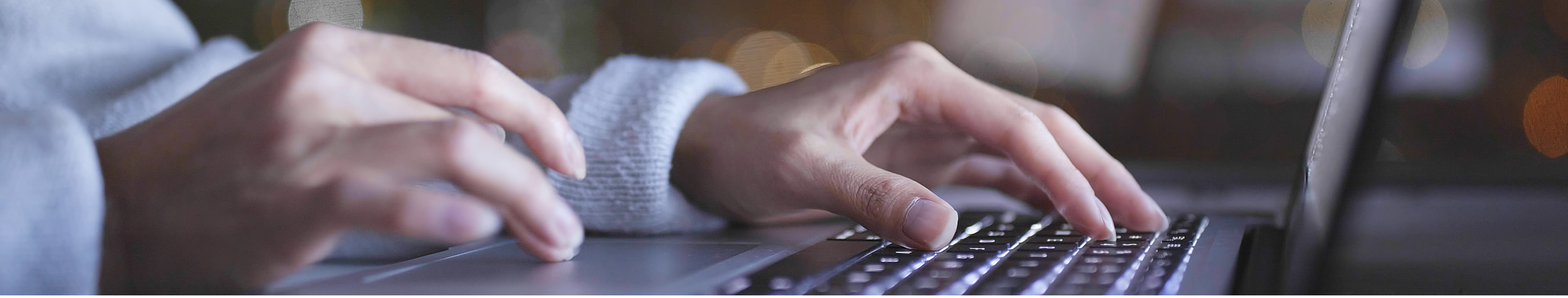
This explosion in data volume is rapidly creating an untenable situation for legacy approaches to data instrumentation, collection, and analysis.

New Research: How Legacy Tools Fail to Deliver Acceptable Outcomes

Recently, Tanium conducted a survey of 200 cybersecurity leaders and operators who work for federal agencies. The survey asked them about the security tools they were using and whether those tools were delivering effective defenses. This survey revealed that:

- 69% of federal cybersecurity teams are using 11 to 50 (or more) security tools, but only 1 in 3 groups reported a utilization rate above 50%.
- Even with dozens of tools, most cybersecurity teams aren't collecting the accurate, real-time security data that they need to reduce their risk.
- Nearly all of these teams are actively looking for a way to improve their security tool utilization, increase their tools' interoperability, reduce their costs, and improve the user functionality and convenience of their security tool stack by performing IT modernization and tools rationalization.

Legacy approaches can't manage today's data volumes, let alone tomorrow's. They commonly don't collect comprehensive data from the environment because they typically can't communicate with remote devices. And they collect data so slowly that data is usually already stale by the time it's staged for instrumentation. In the future, legacy approaches will experience a true crisis in their ability to work with data at scale, with accuracy, and with the speed required.



To address these issues, 99% of the federal cybersecurity leaders and operators in the survey are working to rationalize and consolidate their cybersecurity tools.

The rest of this ebook will outline a practical approach to guide this rationalization, consolidation, and modernization process. It will offer a few core principles of this approach that will help agencies focus their investments and efforts on the solutions critical for better security in a modern ecosystem.

A Practical Approach: How to Rationalize and Modernize Agency Tooling

One point must be clear: Existing cybersecurity tools aren't fundamentally "wrong," they're simply obsolete.

Cybersecurity leaders must accept that the world has changed, and that these tools are no longer appropriate for modern networks. They can't be fixed with tweaks, bolt-on features, new configurations or further investment. Instead, federal agencies must accept a new approach to cybersecurity that is driven by new strategies, tactics and tools. This approach is built around four core principles:

1. Embrace distribution.
2. Perform data instrumentation in real time at the edge.
3. Bifurcate data collection and instrumentation.
4. Consolidate valuable data into platforms and build interoperable ecosystems.

These four principles correct the fundamental mismatch between legacy security approaches and modern environments. By following them, agencies will help ensure their next approach to cybersecurity delivers the value — and most importantly, the security — that their existing approaches no longer provide.

Principle One: Embrace Distribution.

Legacy on-premises approaches designed around tools with hub-and-spoke architecture are no longer effective. Their replacement must be a new approach that works natively for remote, distributed networks. In most cases, such an approach means a move away from on-premises systems and toward cloud-based systems, or systems that otherwise operate in a distributed manner.

By embracing distribution and cloud, teams will:

- Reduce their infrastructure costs and complexity.
- Be able to perform security tasks faster and more frequently.
- Minimize effort and bandwidth requirements for security tasks.
- Scale visibility and control much faster as networks rapidly expand.
- Reduce their blind spots and vulnerabilities throughout their distributed networks.

Principle Two: Perform Data Instrumentation in Real Time at the Edge.

Legacy approaches to centralized data collection can't keep up with today's environments. Their replacement must be a new approach that pushes as much data collection, analysis, and action onto the endpoint itself. In most cases, such an approach means a move away from performing data instrumentation within data stores and instead performing data instrumentation on the endpoint itself through edge computing approaches.

By performing data instrumentation in real time at the edge, teams will:

- Perform data analysis and action in real time.
- Maintain an accurate picture at all times of their rapidly changing networks.
- Be able to perform analysis and action on their data even as their data volume increases exponentially.
- Respond to critical security incidents and zero-day vulnerabilities in real time.

Principle Three: Bifurcate Data Collection and Instrumentation.

Legacy approaches to collecting, managing, storing and using data can no longer accommodate the need for real-time security response and long-term investigations. A new approach must replace them, one that provides real-time data at any moment as well as historical data for research and trends analysis. In most cases, such a process involves bifurcating data collection and instrumentation — and being able to manage data at the edge.

By bifurcating data collection and instrumentation, teams will be able to:

- Perform security analysis on time-relevant data sets.
- Perform real-time incident response and long-term analysis.
- Collect accurate, timely, relevant data to feed new security models like Zero Trust.

Principle Four: Consolidate Valuable Data Into Platforms and Build Interoperable Ecosystems.

Legacy approaches use an excess volume of siloed point tools that commonly don't integrate well together or share the same view of the network. A new approach must unify the team's core operations and security capabilities within a single platform. This platform must give every member of the team the same comprehensive, real-time view of their enterprise and extend its functionality through an ecosystem of streamlined solutions that work well with each other.

By consolidating their point tools into platforms and building interoperable ecosystems, teams will:

- Lower the number of tools that they need, reducing their costs, complexity, and risks.
- Reduce the number of interfaces they use for their security functions.
- Minimize the complexity, overhead, and friction between teams that must work together to secure the enterprise.
- Create a single source of truth and comprehensive view of their network.
- Improve their tool utilization and efficacy and increase the return on their investments and their function as a whole.

For some federal agencies, these four principles represent a fundamental change in the way they approach security and the types of tools they deploy. But no matter how big a change they might represent, these principles aren't optional. They represent a necessary shift in approach for any agency seeking to sustain their mission and defend their networks moving forward.

Change is never comfortable, but it is a constant. Sometimes change steadily and quietly accumulates in the background. Other times, we reach an inflection point that forces a significant amount of change in a short period of time.

The federal government has been talking about and incentivizing technology changes like these for years. In 2017, the government issued

Executive Order number 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[7] A new executive order is being drafted to further improve government cybersecurity in the wake of SolarWinds.[8]

These initiatives, and others before them, are receiving meaningful funding. The Technology Modernization Fund, for example, was created in 2017 by the Modernizing Government Technology Act.[9] The American Rescue Plan Act of 2021 includes substantial funds for technology modernization.[10] And the government has allocated $18.78 billion to cybersecurity investment over the next year alone.[11]

The need to modernize federal cybersecurity systems isn't new. It has been brewing for years, and the events of 2020 simply forced agencies to start to make these necessary changes to how they defend their networks, systems and data.

The events of 2020 and the transformations they drove were dramatic, but they weren't off course and they won't be elastic — nor will they be the last forcing function that impacts technology and security in government. This past year simply accelerated the changes that were already occurring beneath the surface, and that will continue to develop even after these events are resolved. Even if agencies never experience another forcing function like the pandemic, they'll still need to change their approach to security — and their security tooling — to maintain business continuity, sustain their missions, and deliver effective defenses as their environments continue to evolve.

Adapting to these changes is a tall order. Change is rarely easy, especially for organizations as large and complex as many federal agencies.

But there's some good news, too: Tanium was built for this.

While Tanium didn't predict the pandemic and its impact, the platform was designed to meet the exact needs of this moment. It does so by managing and securing endpoints within rapidly changing distributed environments that are flooded with massive amounts of new devices and data.

Meet Tanium: How the Tanium Platform Drives IT Modernization

Tanium is an endpoint management and security platform that rethinks the fundamental assumptions of legacy security tools. It leverages a new, patented communications architecture to deliver effective endpoint security and management within modern environments.

Legacy hub-and-spoke architecture requires dozens, hundreds, or even thousands of staging servers to operate. Tanium takes a different approach.

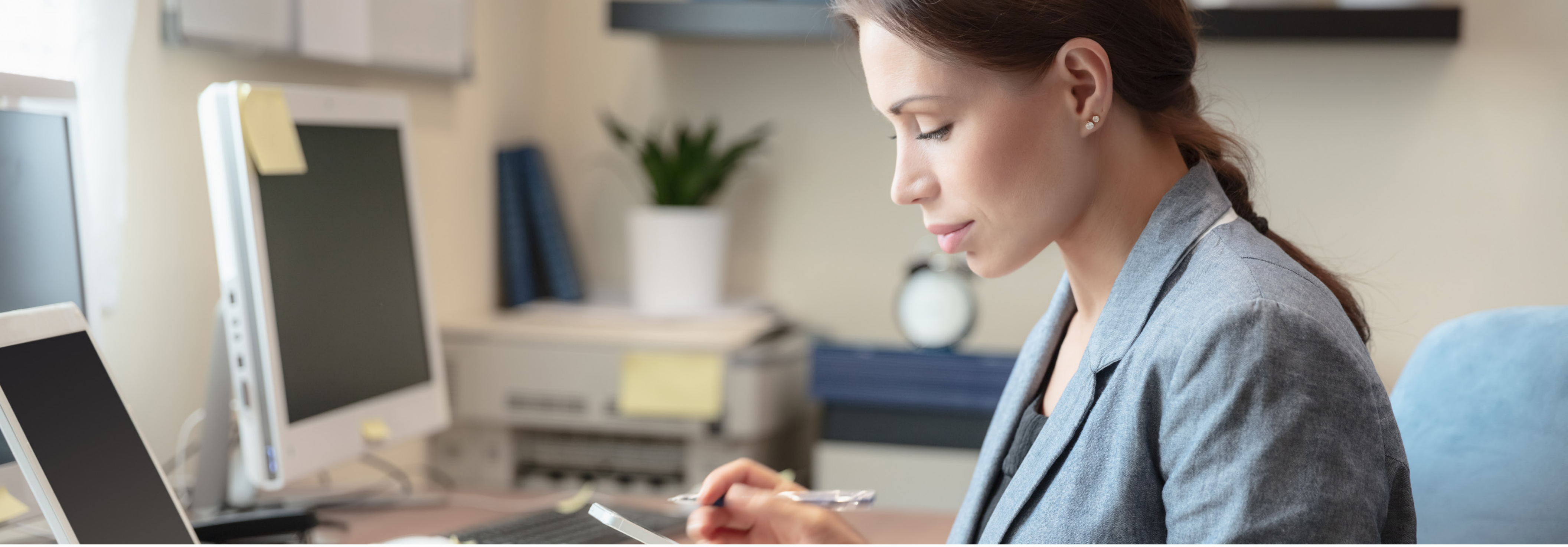
Tanium runs from a single instance that pushes data instrumentation to the endpoint and scales effortlessly alongside the environment. Tanium use a single agent that consolidates a wide breadth of endpoint security and management capabilities within a single platform that provides operators and decision makers with a comprehensive view through a single pane of glass.

Through this architecture, Tanium uses the intrinsic speed of low-latency LAN traffic, reducing inefficiencies caused by bloated databases, overloaded connections, and heavy traffic across WAN segments. Doing so allows Tanium to deliver fast, scalable, extensible endpoint visibility and control within distributed networks. And the Tanium Zone Server allows you to seamlessly and securely help manage remote endpoints to scale without needing to tax VPN connections.

Multiple federal agencies use Tanium, including multiple branches of the U.S. Armed Forces. Over the past year, the Department of Defense used Tanium to maintain effective security over their networks, even as their networks rapidly evolved to accommodate the overnight move to remote operations. By using Tanium, they maintained visibility, control and the ability to remediate and take action at scale across their enterprise in real time.

Tanium aligns directly to the four core principles outlined in this ebook, and makes it easy to bring them to life:

- **Tanium is built on remote, distributed architecture.** Tanium removes dozens, hundreds, or even thousands of servers with a single instance that scales effortlessly to millions of endpoints, and can perform continuous scanning and execute high-volume security controls with minimal network load.
- **Tanium performs real-time data instrumentation at the edge.** Tanium uses distributed edge computing to perform the majority of security and management tasks on the endpoints themselves, using their own computing power. Doing so allows Tanium to perform data collection across the network without moving the data, and to identify, investigate, and remediate vulnerabilities across the network in real time.
- **Tanium bifurcates data instrumentation and collection.** Tanium's architecture splits data instrumentation and collection. Tanium provides real-time endpoint visibility and control to drive real-time incident response, while providing historical data to determine how threats emerged, how they developed, and what objectives they were attempting to achieve. With integrations, Tanium can provide up to one year of telemetry to scope long-lived attacks.
- **Tanium is an easy-to-integrate platform.** Tanium provides a broad range of endpoint security and control capabilities within a single, unified platform, agent, and pane of glass. Tanium also uses an open, friendly API and has developed integrations and strategic partnerships with many leading, modern security tools. Tanium provides out-of-the-box value for these vendors and makes it easy to develop a single source of real-time truth for your ecosystem.



Federal agencies have used a wide range of Tanium's capabilities to defend their networks over the past year. They have found these solutions to be the most effective:

Asset Discovery and Inventory
Provides the ability to know what endpoints and applications are in the environment — even as new managed and unmanaged home-based agents flood the environment.

Patch, Software, and Configuration Management
Provides the ability to apply large-scale patches, software updates, installations and policy configurations to your distributed devices — quickly, efficiently and with closed-loop verification.

Incident Response
Provides the ability to perform automated threat detection across your endpoint environment, and to investigate, contain, and remediate any incident found — in real time.

The Need to Change Now: Why Agencies Must Update Their Tools

Multiple forces are pushing government agencies to make this change right now:

1. Agencies face immediate security threats. If agencies have continued to use legacy tools, their distributed networks have been a huge soft target since the shift to a distributed workforce. They may have already been compromised without knowing it, and the rate of security compromises are only increasing. Recent research suggests there will be a new incident every 11 seconds in 2021, up from every 19 seconds in 2019 and every 40 seconds in 2016.[12]
2. Agencies aren't going back to "normal." Nobody knows what the post-pandemic workforce will look like, but it likely won't return to 80% to 95% of employees working on-premises. Studies show that 54% of employees who transitioned to work from home want to continue to do so after the pandemic ends.[13] The numbers are even higher for

federal employees. Deloitte reports that 70% of federal employees who are teleworking due to COVID-19 feel they're more productive working remotely, and 80% don't feel safe returning to work.[14]

Even if agencies do return to a primarily on-premises workforce, it's possible that another unexpected forcing function will occur that upends legacy networks and defenses all over again.

3. Legacy approaches are obsolete. Even if the pandemic truly is a once-in-100-years occurrence, long-term trends are disrupting legacy tools and infrastructure on their own. Tools that worked well within an on-premises environment weren't designed to accommodate the world's accelerating technology changes. Legacy tools are already causing visibility and control issues and these issues will only increase.

   Agencies must avoid falling into the sunk-cost fallacy of clinging to a suite of tools that they invested heavily in but that can't meet today's requirements. Those investments were appropriate when they were made, but the threat landscape has changed and demands new categories of strategies, tactics, and solutions.

   To even attempt to keep up with increasing volumes of endpoints and data, agencies would have to dramatically increase their spending on legacy tools. Consider the data growth stats outlined above. If, in 2025, the world will have five times more total data than it has today, then agencies will need to spend five times as much on legacy approaches than what they're spending today — while continuing to fail to produce acceptable outcomes. A long-term investment in a modern solution will prove to be a more effective investment than a short-term, bolt-on fix to an outdated solution that's doomed to fall short of business and mission needs because of legacy design.

4. Data instrumentation is moving to the edge. Static instrumentation is failing to keep up with the velocity, volume, veracity, and variability of modern data ecosystems. Agencies have historically collected and centralized their data for storage, analysis, and action. Today, that approach leads to stale data that an agency can't act on before it loses its value, leading to inaction or ineffective action.

   Agencies must come to terms with the fact that centralized data collection is a legacy approach. It's still necessary and valuable for high-value data within certain contexts, but it can't drive real-time visibility and control within modern environments. Centralized data collection has already created a situation where agencies access only a fraction of data they collect, and this problem will only increase as data volumes expand by two orders of magnitude by 2025.[15]

Making the Change: Learn How Tanium Can Help

Agencies face a wide range of security challenges, and there isn't a single "silver bullet" solution that will resolve them. Instead, agencies must undertake a sweeping reconsideration of existing security systems, identify any tool that no longer provides value in the new network, and replace them with a modern alternative.

To do so, each agency has to decide: Will it attempt to perform this sweeping innovation on its own, or will it partner deeply with the private sector? Agencies should look for an experienced partner that understands the challenges of tools rationalization and IT modernization, and that has solved them before with multiple agencies and organizations. Most important, they should look for a partner that was designed from the ground up to solve modern problems and overcome legacy challenges — a partner like Tanium.

[1] Jiblian, I., & Canales, K. (2021). "The U.S. Is Readying Sanctions Against Russia Over the Solar Winds Cyber Attack: Here's a Simple Explanation of How the Massive Attack Happened and Why It's Such a Big Deal" [Online]. Accessed via the web at https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[2] Parker, K., et al. "How the Coronavirus Outbreak Has — and Hasn't — Changed the Way Americans Work" [Online]. Accessed via the web at https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/#:~:text=Just%20one%2Din%2Dfive%20say,or%20most%20of%20the%20time

[3] Chew, B., et al. (2020). "Reimagining Government's Workforce Experience" [Online]. Accessed via the web at https://www2.deloitte.com/us/en/insights/industry/public-sector/rethinking-government-workforce-experience.html

[4] Lui, S. (2021). "Information Security: Statistics and Facts, chapter 3" [Online]. Accessed via the web at https://www.statista.com/topics/7048/endpoint-security/#dossierSummary__chapter3

[5] Coughlin, P. (2021). "Why Cybersecurity Needs an API-First Mentality" [Online]. Accessed via the web at https://thenextweb.com/neural/2021/01/28/why-cybersecurity-needs-an-api-first-mentality-syndication/

[6] MacGillivray, C., et al. (2019). "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast" [Online]. Accessed via the web at https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast

[7] Cybersecurity and Infrastructure Security Agency (2017, updated 2020). Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" [Online]. Accessed via the web at https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure#:~:text=President%20Trump%20issued%20Executive%20Order,face%20of%20intensifying%20cybersecurity%20threats

[8] Seals, T. (2021). "Executive Order Would Strengthen Cybersecurity Requirements for Federal Agencies" [Online]. Accessed via the web at https://threatpost.com/executive-order-cybersecurity-federal-agencies/165056/

[9] The Technology Modernization Fund (2017). "The Technology Modernization Fund: A New Funding Model for Federal Technology Modernization Projects" [Online]. Accessed via the web at https://tmf.cio.gov/

[10] Ostrowski, S. (2021). "CompTIA Says American Rescue Plan Act of 2021 Will Strengthen US Cybersecurity Capabilities, Advance IT Modernization" [Online]. Accessed via the web at https://www.prnewswire.com/news-releases/comptia-says-american-rescue-plan-act-of-2021-will-strengthen-us-cybersecurity-capabilities-advance-it-modernization-301246082.html

[11] Slye, J. (2020). "The FY 2021 Federal Budget Sustains Cybersecurity Funding, But Could Growth Be Slowing?" [Online]. Accessed via the web at https://iq.govwin.com/neo/marketAnalysis/view/The-FY-2021-Federal-Budget-Sustains-Cybersecurity-Funding-But-Could-Growth-Be-Slowing/3958?researchTypeId=1

[12] Morgan, S. (2020). "Cybercrime to Cost the World $10.5 Trillion Annually by 2025" [Online]. Accessed via the web at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[13] Parker, K., et al. "How the Coronavirus Outbreak Has — and Hasn't — Changed the Way Americans Work" [Online]. Accessed via the web at https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/#:~:text=Just%20one%2Din%2Dfive%20say,or%20most%20of%20the%20time

[14] Chew, B., et al. (2020). "Reimagining Government's Workforce Experience" [Online]. Accessed via the web at https://www2.deloitte.com/us/en/insights/industry/public-sector/rethinking-government-workforce-experience.html

[15] Patrizio, A. (2018). "IDC: Expect 175 Zettabytes of Data Worldwide by 2025" [Online]. Accessed via the web at https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

Schedule a free consultation and demo of Tanium.

Schedule Now

Let Tanium perform a thorough gap assessment of your current capabilities.

Get Gap Assessment

Learn more about how Tanium can help U.S. federal government agencies.

Visit Tanium Federal

TANIUM

Tanium offers an endpoint management and security platform 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.