Accelerating Digital Transformation With the American Rescue Plan

To make the most of the federal funds, SLED organizations should take stock of their IT assets and security practices now.

By Gary Buonacorsi, SLED Chief Technology Officer, Tanium

The past couple of years have been challenging both financially and logistically for state and local governments and educational organizations (SLED). Fortunately, help is on the way in the form of new funding from the federal government.

The American Rescue Plan (ARP) Act, signed into law in March 2021, promises SLED organizations new federal funds for operating budgets and investments in cybersecurity.

Getting IT operations under control now will help SLED organizations lay the foundation for the future. Two areas in particular deserve special attention:

- Endpoint management
- Cybersecurity

In this eBook, we explain why SLED organizations should reassess their capabilities for endpoint management and cybersecurity now before ARP funding arrives. (An endpoint is any internet-capable computer on a network. Endpoints include servers, desktop computers, laptops, tablets, smartphones, and Internet of Things [IoT] devices.)

Then, we offer a four-step process that SLED organizations can follow to assess their current IT assets and processes and to get a clear sense of where to invest in the future.

©2021 Tanium. All rights reserved.

Preparing for American Rescue Plan funding

Even if an organization had rigorous endpoint management in place for its on-premises operations before the pandemic, it's worth reassessing endpoint management capabilities now. Many of the most pressing trends in IT today relate directly to endpoints. These trends include:

- Transition to a remote workforce
- Increased use of cloud platforms and cloud applications
- Evolving security threats
- Increasingly strict regulatory environment

Let's take a closer look at these trends to understand why they're so important for SLED organizations and their plans for digital transformation.

Remote work is here to stay

For the foreseeable future, most government agencies and educational institutions will need to provide ongoing IT support for a hybrid workforce. The shift to Work-from-Home (WFH) policies during the pandemic has changed employee habits, expectations, and preferences. A substantial number of employees will work at home or some other remote location at least one or two days a week, indefinitely.

In a survey of 500 IT decision-makers in the U.S. and the UK in 2020, PSB Insights, a global research consultancy, found that 65% of decision-makers expect their WFH policies to continue in some way, resulting in significantly more remote workers than before the pandemic.

This shift is occurring in government agencies, not just private companies. In a survey of federal workers by *Federal News Network*, conducted at the end of 2020, nearly half reported that they would work remotely every day if they were given a choice. Almost a third reported that they would prefer to work remotely 3-4 days per week. More than half of respondents expected their agency's support for telework to increase after the pandemic was over.

It's time to focus on endpoint management and security

The switch to WFH has increased IT security challenges. Attackers take advantage of remote workers' lack of firewall protections and susceptibility to phishing attacks using popular topics such as the pandemic, political news, and the Olympics.

On average, 11% of government agency employees succumbed to phishing attacks in tests conducted in 2020. The live version of those attacks can lead to malware such as keyloggers or ransomware being installed on large numbers of endpoints.

Ransomware attacks are becoming even more numerous. Many attackers take their time now, stretching dwell times to 43 days, lurking and exploring networks to find more valuable endpoints before publicizing their attacks by encrypting data and demanding ransom.

Employees working remotely are especially vulnerable to these attacks, which can even spread to internal networks. SLED organizations must strengthen their security defenses for its endpoints, both on internal networks and remote locations such as home offices.

Find and fix endpoint problems before applying ARP funds

While it might be tempting to treat endpoint management and security as an issue to be addressed with ARP funding, a more practical approach is to rationalize endpoints and IT investments now — before ARP funds arrive.

Then organizations will be able to apply ARP funds more effectively, knowing that the endpoints used by their employees are monitored, managed, updated and secure. Faulty or unsupported endpoints have been removed. ARP funds will be applied only to endpoints that the organization is aware of and trusts.

Four steps for assessing and improving endpoint management and security

To assess and improve their capabilities in the areas of endpoint management and security, SLED organizations should follow this four-step process:

Step 1: Improve asset visibility

Discover endpoints in use, record their hardware and software configuration details, and monitor them for security and performance issues. Answer questions such as: How is the organization currently monitoring configuration drift? How quickly can patches for operating systems and third-party applications be installed in emergencies?

Step 2: Optimize tools and costs

Reassess the IT operations and security teams' tools to monitor and manage endpoints across different environments. Can redundant toolsets be streamlined? Would switching to a standardized toolset save time and money compared to provisioning each department with its own choice of tools?

Step 3: Help ensure data privacy

Data privacy is growing in importance for all organizations, both public and private. How is the organization measuring data privacy and regulatory compliance today? Has the organization identified the most valuable data it's protecting and how it's being accessed? Are there any data privacy risks that need to be addressed?

Step 4: Strengthen cybersecurity defenses and streamline incident response

Reassess the tools used to detect, investigate, respond to, and remediate threats, including advanced persistent threats that might have been lurking on endpoints for weeks or months. How long does it take the IT team to respond to threats? Is the organization prepared to respond to incidents as quickly and effectively as possible with increased adoption of cloud services and a continuing remote workforce? Let's examine each of these steps in turn.

©2021 Tanium. All rights reserved.

1: Improve Asset Visibility

Creating a comprehensive, up-to-date inventory of endpoints and other IT assets might seem like straightforward work, but we find that many SLED organizations have difficulty getting it done. The problem? Many endpoint management tools don't provide the comprehensive visibility they promise.

In our experience, we find that many endpoint management systems overlook anywhere from 10% to 20% of endpoint inventory, leaving SLED organizations with no way of monitoring and managing hundreds or even thousands of endpoints.

But other factors, including out-of-date records, manual data-collection processes, and the sudden displacement of so many endpoints as part of the rushed transition to a distributed model, also reduce the visibility of SLED organizations into their IT assets.

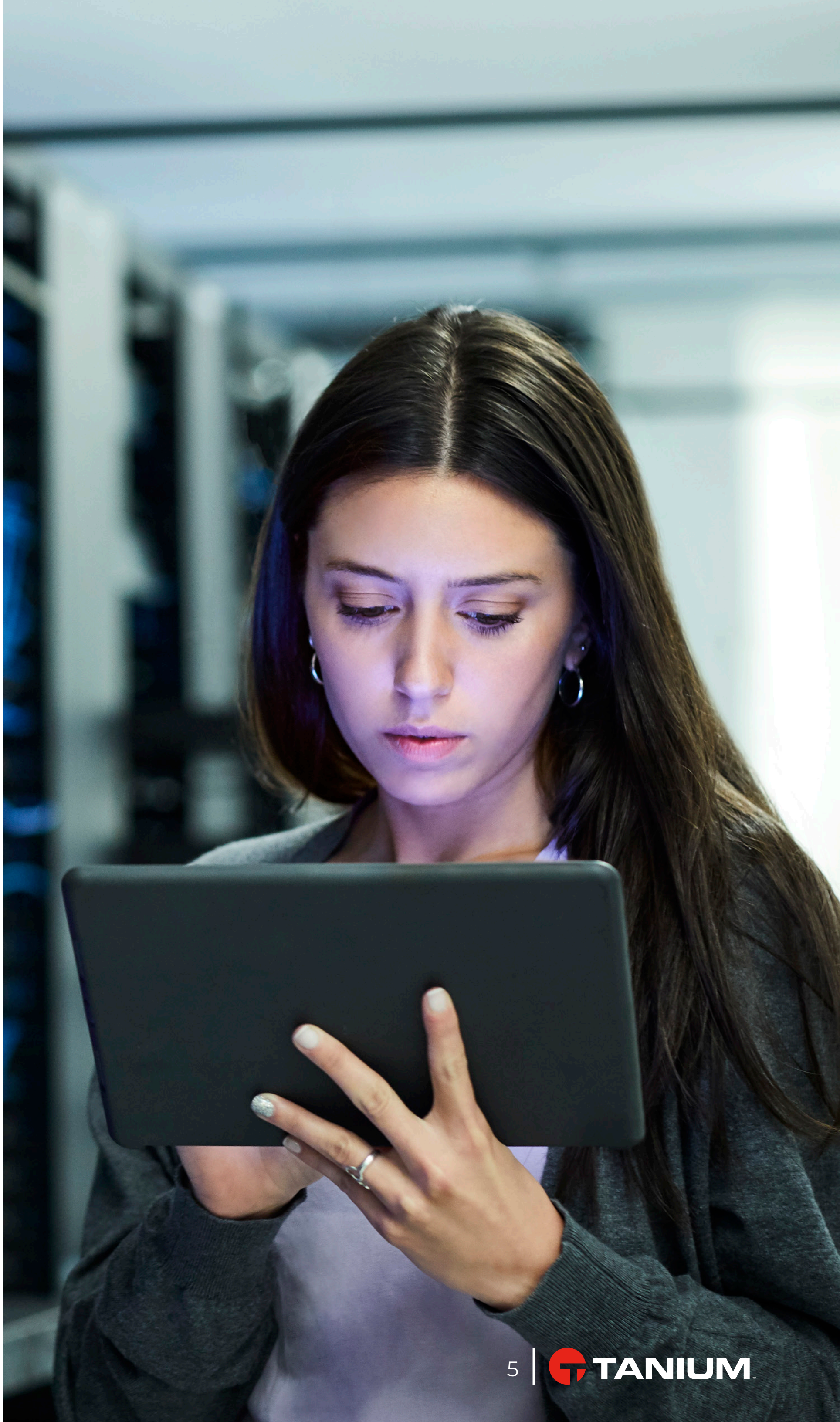
SLED organizations need to overcome these blind spots. It's critical that they know what endpoints they have, including any bring-your-own-device (BYOD) endpoints that employees use at home to access internal applications and data.

Questions to ask

To lay the groundwork for any new IT strategy, begin by asking these questions:

- How many endpoints do we have?
- Where are they deployed?
- Which endpoints are being used and which can be decommissioned?
- Which services and applications are our endpoints running?
- Which endpoints are up-to-date with patches, and which need to be patched soon to minimize security risks?
- Which endpoints are running third-party applications with known vulnerabilities that need to be patched?
- Can we verify that our endpoints are up-to-date with both operating system patches and application patches?

Endpoints that aren't tracked can't be managed and secured. And they can't be figured into new plans for digital transformation.



©2021 Tanium. All rights reserved.

2: Optimize tools and costs

Once you've answered questions about asset visibility, you're ready to take on questions about IT tools and cost optimization.

Questions to ask

To evaluate your IT toolsets and how their costs might be optimized, ask:

- What monitoring systems do we have in place?
- How many tools do we use to see and control the endpoints across our environments?
- How do we identify our assets and measure software utilization?
- What's our strategy for patching endpoints when security incidents occur?

When you know what tools and third-party software applications you're using, you can explore questions about centralizing tools and eliminating redundancies from your IT investments:

- What are our long-term strategies for cost optimization?
- Which redundant IT investments can be standardized and streamlined?
- Are multiple departments running copies of the same software?
- Are departments using similar tools that could be standardized?
- Have we oversubscribed to certain software licenses?

We recommend centralizing and streamlining toolsets before you begin applying ARP funds. After all, there's no point in applying new purchases to redundant hardware and software.

If you've improved your asset visibility to the point where you have a comprehensive understanding of which software and hardware products employees are using, you can deprovision unused products and eliminate redundant licenses. This will give you confidence that you're saving money without jeopardizing productivity.

There's no point in embarking on bold digital transformation projects while your IT organization is hobbled by redundant tools, a lack of standardization, and slow, complicated processes that result from a "swivel chair" approach to IT management.

3: Help Ensure Data Privacy

Data privacy is important not only for fulfilling the American Rescue Plan's goals of strengthening cybersecurity; it's also important for winning the trust of constituents.

Demonstrating that you take data privacy seriously gives customers the confidence to trust the digital services you offer.

It's also important for ensuring compliance with a growing number of data privacy and data security regulations. SLED organizations may need to comply with a growing number of federal data privacy regulations, such as PCI and HIPAA. In addition, many states are passing their own data privacy laws similar to the European Union's General Data Protection Regulation (GDPR). And they need to put data privacy practices in place so they can earn and keep the trust of their constituents.

Questions to ask

Here are some questions to ask when evaluating your organization's strengths and weaknesses regarding data privacy and regulatory compliance:

- How does your organization assess its data privacy risks today?
- Has your IT team identified the types of data that require protection?
- If so, has your IT team identified the data repositories and applications where that data might be found?
- Can you systematically track user access rights across devices and services, so you can limit access to sensitive data to only authorized users?
- How do you measure compliance?
- How does your organization ensure compliance with the relevant regulations and policies?
- Does your organization conduct regular audits of its regulatory compliance?
- Can your IT team generate comprehensive reports on compliance without relying on manual processes, spreadsheets and guesswork?
- If so, are those reports shared with executive leaders and the IT security team?

©2021 Tanium. All rights reserved.

- When risks appear, can you address them quickly?
- If a security attack threatens the privacy or integrity of your organization's data, how quickly can you quarantine affected endpoints and mitigate the attack?

Answer these questions, then determine what changes you should make to improve your organization's data privacy protections. For example, do you need to improve visibility into employee endpoints? Improve employee training on best practices and security threats? Monitor employee activity more closely for possible regulatory violations?

Determine what you can change and optimize now to address data privacy requirements and preserve your organization's reputation as a trusted protector of confidential data.

4: Strengthen cybersecurity defenses and streamline incident response

Cybersecurity is a key focus of the American Rescue Plan. As soon as organizations switched to a remote workforce, cyber threats increased. In a 2020 survey, 63% of chief information security officers (CISOs) reported an increase in attacks.

At the same time, 58% reported being concerned that remote employees weren't following security guidelines, and 36% reported a lack of visibility into IT assets such as employee endpoints.

Cyber threats are increasing in variety, severity, and sophistication. Targets have expanded from corporate networks to national infrastructure. In part, that's because today's threat actors include nation states and criminal syndicates with lots of money, tools, and patience.

Without visibility into employee endpoints, IT teams can't detect threats and mitigate them.

Questions to ask

Answer these questions to assess your organization's IT security strengths and weaknesses:

- Do you have comprehensive visibility into your endpoints, including the devices that remote employees are using?

- Do you have visibility into the applications and services those endpoints are connecting to in the cloud?
- Can you collect endpoint data in real time? If not, how current is your data? Is it collected once a day? Once a week? If you collect endpoint data only once a week, are you willing to endure the cybersecurity risks of having week-old data about security threats?
- Do your IT security practices depend on endpoints connecting over a local area network (LAN) or a virtual private network (VPN)? Or can they work with today's remote workforce, which is rarely on LANs and VPNs?
- When security incidents occur, can you respond quickly, stopping threats before they spread to other endpoints?
- Can you automatically scan the endpoints that employees are using, identify vulnerabilities, and patch the endpoints to help eliminate those vulnerabilities?
- What means does your organization have for detecting and cleaning up attacks that may have been active for 90 days or longer?

Answer these questions to identify the shortcomings in your current IT security practices or toolsets. Then determine what, if anything, needs to be replaced, added or optimized.

For example:

- Do you need to revise policies and processes now that you have an ongoing WFH workforce?
- Do you have the tools and procedures you need for complying with the latest government regulations?
- If you're keeping your current IT security toolset, could you easily augment that toolset with other tools to strengthen and optimize your overall security?

Reassess and optimize your IT security and data privacy practices now so that when new federal funding arrives, you'll be able to spend it productively — and be ready for the future.

SLED organizations should take the time now to evaluate their IT tools and practices for data privacy and cybersecurity. There's no point investing new federal funds in old technology and practices that aren't working as they need to be. Instead, clean out the old, optimize what you're keeping, and lay the groundwork for any new investments you identify.

Conclusion

The American Rescue Plan Act offers SLED organizations a great opportunity for embarking on bold digital transformation projects and improving services for customers and employees.

By following the four-step process outlined in this eBook, SLED organizations can take stock of their current endpoint and security capabilities, so they can make wise decisions about optimizing investments before ARP funding arrives. Then, working with a clear understanding of their current IT capabilities, they'll be able to invest ARP funding productively in new toolsets, services, and staff.

To learn how the Tanium platform can help SLED organizations monitor, manage, and secure endpoints regardless of location, visit our website.

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.

©2021 Tanium. All rights reserved.