TANIUM™

Defending Your Remote Endpoints in 5 Steps

Practical Advice From Security Leaders on How to Address the New Remote Work Reality

Table of Contents

The Mandate: Secure Your New Operating Environment

2020 transformed your business network. Overnight you were forced to send your workers home. This created a diverse, dynamic and distributed operating environment.

And life is not likely going back to “normal” anytime soon — if ever. The lesson from the pandemic? Digital enterprises need to be ready for whatever comes next.

“People need to adapt to this new environment,” says Charles Ross, Chief Customer Officer at Tanium. “No one’s going to flip a switch and bring everything back to the old ways.”

Some leaders have adapted and maintained secure operations. Others continue to continue on without meaningful defenses.

But both groups have learned the same hard lesson… ecurity works much differently today than it did before the upheaval of a pandemic.

This ebook will present advice from security leaders who adapted their defenses — or their clients’ — over the past year. They’ll teach you how to build solid security for your new operating environment so you are **ready for whatever comes next**.

It will explore:

- The security challenges you face.
- How you can overcome these challenges and build solid security.
- How Tanium gives you the tools to defend your environment — no matter what comes next.

New Environment, New Threats: Security Challenges Opened in 2020

Organizations transformed their security posture in several ways when they moved to new environments.

First, they dissolved their perimeters and left many security controls behind.

Security operated differently pre-pandemic. Organizations had designed their security with a single assumption in mind: Workers and their endpoints would sit and work on-premises most of the time.

With this assumption, organizations built hardened perimeters around their central networks. But this assumption didn't hold up in 2020.

Most workers left their offices to work from home. And when they did, they left the protection of their on-premises perimeters — and with them many of their defenses.

> *"Organizations had to dissolve a lot of the perimeters that contained the security controls they've relied on in the past."*
>
> Kris McConkey, Cyber-Threat Operations Lead and Partner, PwC

"Organizations had to dissolve a lot of the perimeters that contained the security controls they've relied on in the past," notes Kris McConkey, Cyber Threat Operations Lead Partner at PwC.

"You were behind layered defenses in an environment where you had physical controls — and now we've moved all that," explains Rob Vann, Chief Solutions Officer and CTO at Reliance acsn. "Now people largely subsist on their own, inside their own perimeter."

But these workers didn't secure their individual perimeters and remained unprotected.

"The bar of sophistication for adversaries was lowered," adds Alissa Knight, Principal Analyst, Alissa Knight & Associates. "You have an entire economy of people now working from home. The attack surface has increased exponentially. It's a massive soft target."

Second, organizations deprioritized security to maintain business continuity.

Most organizations could have maintained their security controls. They just needed to connect their remote endpoints to their central networks.

"A lot of CISOs had been in a situation where their technical architecture required them to connect to an HQ to perform the foundations of their control framework — things like patching, vulnerability management, identity management, and asset management," says Chris Hodson, global CISO at Tanium.

But this was easier said than done. Organizations needed a lot of bandwidth to connect to their central networks. And that bandwidth could go to security controls or line-of-business applications.

In most cases, organizations chose to maintain business continuity. While this was likely the right decision at the time, it came with significant consequences.

"Security was an afterthought when bringing systems online," recalls Ross. "In the move to work-from-home, many organizations gave malicious actors a very easy way to enter. They opened the front doors, opened the windows, and put up a big sign saying, We're defenseless."

Third, organizations opened new vulnerabilities that were unique to WFH environments.

Organizations deprioritized security at the exact moment they increased risk. They faced a wealth of new vulnerabilities they never encountered in the office.

"There were lots of vulnerabilities we had to deal with that really weren't there before," says Jon Oltsik, Senior Principal Analyst and Fellow at the Enterprise Strategy Group. "Things like people working from home on their home computers, shared with their children doing home school, and maybe a spouse who was also working from home."

These new devices carried potentially dangerous software.

"There were different applications on those systems; there were different configurations. Some were out of spec," Oltsik continues. "Some were using old, obsolete operating systems. Were they approved? Did they have open vulnerabilities?"

> *"The pandemic exponentially increased the opportunities for cybercriminals. Remote employees are a massive soft target."*
>
> Alissa Knight, Principal Analyst, Alissa Knight & Associates

And even when workers' assets were secured, their home networks may have been vulnerable.

"You had people working out of home networks. Well, what's on those networks? Security cameras, gaming systems, other tablets." says Oltsik. "Those systems are communicating with other websites, which might have been insecure and out of policy."

The outcome: Many organizations opened a wealth of new security challenges in 2020.

They lost their security controls just as they opened new vulnerabilities. And they've been operating at an elevated risk level for almost a year. But even though these challenges are complex their solution can — and must — be simple.

How to Defend Your Environment: Focus on Fundamentals, Not Buzzwords

In producing this ebook, we spoke with multiple security leaders, who come from different backgrounds. Some lead individual organizations. Others are security consultants or vendors who work with a wide range of organizations.

But all of them agreed on the same top-level strategy to defend today's new environments. Focus on security fundamentals — not on chasing buzzwords.

> *"So many people get excited about zero-day threats. But doing the basics well is the best form of defense. Patching. Antivirus. And then — once you've nailed the basics — you move into more advanced territory."*
>
> Alissa Knight, Principal Analyst, Alissa Knight & Associates

"What scares me is that people abandon the basics to do really advanced, clever stuff, never thinking that their doors are wide open," says Vann. "So many people get excited about zero-day threats. But doing the basics well is the best form of defense. Patching. Antivirus. And then — once you've nailed the basics — you move into more advanced territory."

According to Vann and many others, organizations must develop a few capabilities:

- They must create visibility into their endpoints.
- They must establish control over their endpoints.
- They must maintain meaningful IT hygiene at all times.

Here's why these capabilities matter and how you must be able to deploy them.

Fundamental Capability One: Endpoint Visibility

"The biggest threat to organizations today is not knowing the assets they've got," explains Knight. "What we refer to as Shadow IT — like an employee deploying an unpatched, unsecured, unhardened server into the network and accessible to the internet."

Knight — an ethical hacker — understands the threat posed by these unknown assets.

"Over the last two decades, I've hacked over a hundred networks," Knight says. "More than half of those compromises were the result of me gaining access to the network through an asset the company didn't know they had."

And over the past year, organizations have adopted a wealth of new assets they don't know they have.

"Organizations now have assets everywhere," adds Knight. "And they have more and more devices that historically weren't connected and are now being connected to their infrastructure."

To combat this threat, organizations must develop comprehensive, real-time visibility into the endpoints within their network — before malicious actors find them first.

"Every system, every user, broadens the attack surface," Ross says. "If you don't know what's in your organization, someone else will figure it out for you — someone with malicious intent."

Fundamental Capability Two: Endpoint Control

Once you establish visibility over your environment, you must be able to control what you find.

“Now that everyone’s working from home locations, you have to ensure that the controls that previously existed in the data center are available for all your workforce locally,” says Hodson

> *“A single endpoint left uncontrolled for a short period of time can lead to a global breach.”*
>
> Chris Hodson, Global CISO at Tanium

You must be able to apply these controls to the endpoints in your environment. A single endpoint left uncontrolled for a short period of time can lead to a global breach.

“It only takes one server or workstation that isn’t patched for a malicious actor to get access to the network and then move laterally across it,” warns Scott Lowe, Managing Director and Founder at EndpointX. “The ability to see and manage endpoints across the network is key.”

You don’t need to apply complex controls. You only need to perform the most fundamental security actions on your endpoints — updating them, configuring them with policy, and patching them.

“Too many breaches are the result of an attacker exploiting a vulnerability that has a patch available,” says Knight. “Organizations don’t patch fast enough. They need technical controls that enable them to identify vulnerabilities that need patching and to quickly and easily apply those patches.”

Fundamental Capability Three: IT Hygiene

Finally, you must leverage your visibility and control to maintain pristine IT hygiene.

“When we start talking about security, it doesn’t always feel relevant to talk about the operations side of things,” says Stephanie Aceves, Director of Technical Account Management at Tanium. “Things like making sure you’re updating all your systems and you have a regular patch cadence.”

But many security leaders agree on the fundamental role of IT hygiene in security.

“The first thing I always talk about with customers is IT hygiene,“ says Scott Lowe, managing director and founder, EndpointX. “There’s the perception in the press that most hacks are done by nation-states on shiny zero-day vulnerabilities. But the reality is most happen because a server hasn’t been managed or patched or there’s a vulnerability on a browser. It’s normally the most fundamental IT hygiene issues that lead to breaches.”

To prevent breaches, you must close as many of the known issues as possible.

> *“It’s normally the most fundamental IT hygiene issues that lead to breaches.”*
>
> Scott Lowe, Managing Director and Founder, EndpointX

“I talk with CISOs and CIOs who say, ‘I have 84% of my workforce’s machines patched’ or ‘92% of my devices are in-line with company policy,” offers Hodson. “Unfortunately it only takes one weak point in any organization to be compromised and used as a vector to move laterally and propagate across an organization.”

Every security leader we spoke to agreed. Effective security means applying visibility, control, and IT hygiene across distributed endpoints. Here’s how you can develop the ability to do just that.

What to Do: Five Steps to Build Solid Security in Today's Environments

Our advice is clear. Focus on the fundamentals. Develop a few of the right capabilities. And make sure you can deploy them within your new environment.

To help you, we've developed a simple five-step process you can follow to build solid security in today's environments. If you follow this process, you'll restore any security capabilities you may have deprioritized over the prior year, and you will better secure your organization against whatever threats might be coming next:

Step One: Assess your security gaps.

Step Two: Revisit your security concessions.

Step Three: Manage your new vulnerabilities.

Step Four: Decentralize your security controls.

Step Five: Re-evaluate your endpoint management and security tools.

Step One: Assess your security gaps

Ask yourself a few questions to determine how the move to your new environment may have created new security challenges for your organization, and what gaps you have left to fill.

- ✓ Did we make any short-term security concessions to allow business continuity?
- ✓ Have we revisited all of those concessions or do they remain in effect?
- ✓ Do we have visibility into the assets in our new environment — including non-work applications on work devices and non-work devices on our workers' home networks?
- ✓ How many of our security controls did we lose in the move to our new distributed environment? Have we found a way to reestablish them?
- ✓ Have we maintained our IT hygiene and kept a high barrier to entry into our network?
- ✓ Have we restored the security capabilities we lost in our transformation?
- ✓ Are we planning to return to our "normal" work environment, or are we planning for permanent changes to our operating environment — no matter what happens next?

Step Two: Revisit your security concessions.

You now have a clear picture of the potential security gaps in your new environment. To close these gaps, first list the security concessions you accepted in 2020. Don't worry if you were forced to make a lot of concessions. You were likely making the right decision at the time given the immediate context.

"When COVID hit, people thought that everyone would be back in the office in five weeks," explains Lowe. "Many machines weren't managed and remained invisible because people thought they'd be brought back to the office soon."

But chances are some of the concessions are not sustainable.

"Initially, it was a band-aid over a bullet hole," Aceves recalls. "I think a lot of people were hoping this was a temporary solution and were trying to put controls in place to properly secure what was relevant at that time, but they weren't thinking long-term."

Now it's the time to think long-term. Circle all of your short-term, unsustainable concessions, and begin to think of ways that you can either reverse them or otherwise replace them with more viable long-term trade-offs.

Step Three: Manage your new vulnerabilities.

Next, take a hard look at the risks you've incurred in your move to your new environment.

"As we switched into this new work-from-home reality, some of my top concerns were around this fundamental shift in how security works," says Michael Coates, Altitude Networks. "We've been able to make the transition and keep business going. But I don't think we have a firm grasp of the risk we've accepted."

Some risks are manageable. In the next step, you'll reestablish the capability to do so. But some risks are unmanageable. You probably can't stop workers from letting other people use their work devices. Or establish a perfect perimeter around their home networks. You certainly can't manage every device that lives on those networks. But you can establish and maintain continuous visibility into these unmanaged risks.

> *"As we switched into the new work-from-home reality, we've been able to make the transition, but I don't think we have a firm grasp of the risk we've accepted."*
>
> Michael Coates, CEO, Altitude Networks

You can map the impact if any of these unmanaged risks blow up. And you can develop a plan to intelligently provision access rights and identity management to limit the damage when one of these unmanaged devices is compromised.

Step Four: Decentralize your security controls.

"Now that everyone's working from their homes, you have to ensure the controls that previously existed in the data center are available for all your workforce locally," Hodson explains.

To do so, look at the security controls you lost in your move to a new environment. Determine how many you lost because you designed them to work on-premises only. And begin to sketch out a plan to rebuild them with a more distributed architecture.

Do this even if your organization plans to return to a "normal" environment. After all, the move to remote work didn't begin during the pandemic and won't end with it.

"We need to get away from the idea of a central home base, a central office, a central headquarters," Knight says. "A lot of organizations will stay in a permanent WFH architecture. The perimeter is gone. And new generations want to work differently. They want to work from anywhere, from any device."

Step Five: Re-evaluate your endpoint management and security tools.

Finally, take a look at your endpoint management and security tools. Divide them into two lists. In the first list, put every cloud-based tool designed for a distributed environment. These tools likely delivered value over the past year, and likely will throughout the future.

"Organizations with more of an internet-first model — who were using distributed computing for a distributed workforce — had a head start and were significantly less impacted by the pandemic from a technology perspective," says Hodson. "I predict the most successful security functions are those that re-evaluate their tooling to one of a cloud-first distributed way of working."

In the second list, put down every tool designed for an on-premise environment only. These tools probably failed over the past year and contributed to gaps in your security.

"One of the major problems with cybersecurity and IT operations tools is they were designed to work in a world where people sometimes worked from home, and sometimes worked in the office," notes Lowe. "We've had a period where machines have not come back into the office. And some of these tools have not been designed to patch them, to scan them for vulnerabilities — they just weren't designed for this fully-remote workforce."

> *"The perimeter is gone. And new generations in the workforce want to work differently. They want to work from anywhere, from any device."*
>
> Alissa Knight, Principal Analyst,
> Alissa Knight & Associates

Keep this exercise simple. Look at your list of on-premise tools. These tools are ripe for replacement with cloud-based alternatives.

Alternatives like Tanium.

Meet Tanium: Secure Your New Environment

At Tanium, we didn't see the precise security challenges of 2020 coming. We never thought organizations would have to move to distributed environments overnight. But we did know that distributed environments were the future of work and that these environments carried with them unique security challenges and requirements.

So, we had already designed our platform to establish and maintain comprehensive security controls over diverse, dynamic environments filled with distributed endpoints. And over the past year, a wide range of organizations and security leaders were able to use Tanium to protect their environments — even as they transformed overnight.

In 2020, our customers used Tanium to:

- **Maintain comprehensive visibility** into all managed and unmanaged endpoints within their environment in real time — and the applications and users on those endpoints.
- **Maintain security controls** over all of their manageable endpoints and applications allowing them to patch, update, configure, and close all their vulnerabilities.
- **Maintain strict IT hygiene** to raise the barrier of entry into their rapidly expanding and changing environments without obstructing business continuity efforts.

There are several reasons why Tanium could help these security leaders and organizations maintain effective defenses for their and their clients' new environments. Tanium:

- Uses a modern, distributed architecture with decentralized edge computing that doesn't need to connect to the central network and doesn't compete for bandwidth with line-of-business applications.
- Automatically scales and adapts to changes in endpoint environments without additional infrastructure, automatically folding new endpoints into the security team's visibility, control, and IT hygiene efforts.
- Provides a complete suite of capabilities to deliver visibility, control, and IT hygiene on entire endpoint environments — no matter where endpoints are located — in a single, unified platform.
- Can deploy new endpoint management and security capabilities in hours or days — not weeks or months — to rapidly fill gaps in the security posture of new environments.

The Tanium Platform offers critical services for defending your endpoints devices

Asset Discovery and Inventory

Know what endpoints and applications are in the environment — even as the environment rapidly floods with new managed and unmanaged home-based agents.

Patch and Software Management

Apply large-scale patches and software installation and updates to countless distributed endpoints — without consuming significant network bandwidth or threatening outages.

Vulnerability and Configuration Management

Continuously find open vulnerabilities, breaks in compliance, and policy misconfigurations — and remediate issues — within new environments.

The Road Ahead: Secure Your Environment Against Whatever Comes Next

2020 has passed. But your new environment remains. There's no way to know if it will ever go back to "normal." Odds are it won't.

This reality puts you in an uncomfortable position, with two options:

- Do nothing and hope you eventually return to on-premises operations.

OR

- Proactively build solid security that works in any environment.

The security leaders we spoke with chose option 2. And they recommend you do the same.

"Too many people are too comfortable with the pillow and the snooze alarm. They're just waiting for this to be over so they can go back to the way it used to be, says Ralph Loura, CIO of Lumentum. "And I think they'll have a lot of challenges coming up, because the world they knew isn't coming back anytime soon."

To learn if Tanium can help you prepare for the unpredictable, reach out today. Take the appropriate next step to see if Tanium is the right platform to drive your ongoing business continuity requirements.

Schedule a free consultation and demo of Tanium.

Schedule Now

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

Get Gap Assessment

Launch Tanium with our cloud-based offering, Tanium as a Service.

Try Now

TANIUM