TANIUM

Five Steps to Uniting Your IT and Security Teams

Practical Advice From Technology Leaders on Improving Your Operational Agility and Security

Table of Contents

Your New Mandate: Unite Operations and Security

This last year has revealed a lot about endpoint security and management. It revealed which organizations were prepared for the unpredictable, and which weren't. It revealed a new wave of attack patterns, and how cybercriminals are eager to take advantage of a crisis. And, most importantly, it showed that IT and security teams need to be **ready for whatever comes next**.

This ebook will explore how IT and security teams can work together more effectively to ensure their distributed organizations are fully protected and running efficiently.

This ebook will present advice from operations and security leaders who've protected their organizations and their clients from today's biggest infrastructure-based threats by uniting their operations and security teams, and how you can do the same yourself.

To do so, it will explore:

- The new challenges organizations face that blend operations and security.
- How organizations can bring operations and security closer together.
- How Tanium gives operations and security functions a single shared platform.

Why You Must Bring Operations and Security Together

IT organizations have felt unclear about how to structure their operations and security teams for a long time, with valid arguments made by both sides.

"For the last 10 years there's been a debate about whether operations and security should work together more closely, or maybe even become one organization," says Jon Oltsik, senior principal analyst and fellow at the Enterprise Strategy Group. "Some debate that these two functions should unite, while others argue that you can't do that and you need controls, separation of duties, and things like that."

"Many organization had policies and infrastructure for supporting remote access. But they only had it for half their workforce, not 90 percent of their employees."

Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

However, this debate has become increasingly relevant over the past year, and there now appears to be a clear answer about how IT organizations must structure their two teams.

"We're realizing that there's no way around making those two functions move closer together," explains Oltsik. "We've eliminated the perimeter, workers are now remote and mobile, and the biggest security challenges we now face are all because of infrastructure."

Many technology leaders agree with Oltsik. They believe the rapid move to a large-scale work-from-home (WFH) model has increased the volume and risk of infrastructure-based threats, primarily because organizations have flooded their networks with new, unknown, remote assets.

"The biggest threat to organizations today isn't knowing about the assets that they've got — what we refer to as the 'shadow IT problem,'" explains Alissa Knight, principal analyst at Alissa Knight & Associates. "Organizations now have assets everywhere, and they have more devices that historically weren't connected and are now being connected to our infrastructure."

Knight — a former hacker — believes that these new, unknown assets give malicious actors an easy path to compromise their targets.

"Over the last two decades of my career I've hacked over a hundred networks," says Knight. "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."

To mitigate these infrastructure-based threats, security teams need to know every asset in their networks and every vulnerability those assets carry. Then, they must coordinate with operations teams to perform fundamental controls to close those vulnerabilities.

Knight believes that many breaches happen because security and operations teams commonly fail to coordinate around this fundamental task of finding and fixing these knowable vulnerabilities.

"Too many breaches are the result of an attacker exploiting a vulnerability that has a patch available for it," explains Knight. "Organizations aren't patching fast enough. They need technical controls that enable them to identify vulnerabilities that need to be patched, and to apply those patches."

"Organizations aren't patching fast enough."

Alissa Knight, Principal Analyst, Alissa Knight & Associates

These vulnerabilities have increased over the past year. Organizations have created more targets, more shadow IT, more backdoors, and a greater need to ensure their security and operations teams are collaborating to identify and close the gaps in their defenses.

"You have an entire economy of people now working from home," Knight says. "The attack surface has increased exponentially and has become a massive soft target."

It's tempting to hope these problems will go away, organizations will return to their on-premises networks and that security and operations teams will have an easier time finding and fixing their vulnerabilities. But Knight and others believe that centralization is gone for good.

"We need to get away from this idea of a central home base. A lot of organizations are going to stay in a permanent WFH architecture."

Alissa Knight, Principal Analyst,
Alissa Knight & Associates

"We need to get away from this idea of a central home base," Knight says. "A lot of organizations are going to stay in a permanent WFH architecture."

The reason for this shift is simple. The past year didn't force organizations to do anything new — it simply accelerated the transformations they were already going through.

"What we really saw over the past year is an acceleration of digital transformations and rapid adoption of the IT infrastructure to support it," Oltsik says. "Organizations have been challenged to cope with it, but this is the future, and they have to move in this direction."

Today's distributed networks are here to stay, and so are the infrastructure-based threats that plague them. To defend against these threats, organizations must bring their security and operations teams closer together.

How to Unite Operations and Security: Lessons Learned From 2020

To produce this ebook, we spoke with multiple technology leaders. Some of them were security leaders. Others were operations leaders. All of them agreed that security and operations must work together more closely, and they all provided similar advice on how to unite the two functions:

1. Give operations and security the same comprehensive asset visibility and control.
2. Unite operations and security teams around the shared project of IT hygiene.
3. Reduce resource competition between the two functions.
4. Give operations and security teams a shared set of tools to work with.

Same Comprehensive Asset Visibility and Control

Operations and security are struggling with the same fundamental visibility and control challenges opened by the rapid, sustained move to a primarily WFH asset network.

"Speaking with both CIOs and CISOs, one of the front-and-center challenges they both face are the blind spots that have been introduced by distributed working," says Chris Hodson, chief information security officer (CISO) at Tanium. "Employees are working from their own devices, making it harder to track every device in the network, distribute appropriate security systems and updates, and maintain compliance with regulatory standards."

Organizations must close these blind spots for both teams at the same time by providing them with the same view of their asset network and access to the same suite of controls. Without this shared understanding, security and operations teams won't be able to collaborate on what vulnerabilities they must close, in what order they must close them, and whether the teams responsible for closing those vulnerabilities have done so to a sufficient degree.

Uniting Operations and Security Teams Around the Shared Project of IT Hygiene

IT hygiene — the continuous process of identifying infrastructure-based vulnerabilities and closing them — is a natural collaboration point for security and operations teams.

In most cases, security teams will identify vulnerabilities to close and security controls like patches and updates to apply. They will also establish standards for what constitutes acceptable compliance with those standards, such as patch windows and coverage. From there, operations teams will typically apply those controls to those standards.

How well an organization can perform this process of IT hygiene offers a good litmus test for how closely and effectively their security and operations teams are working together.

If they're unable to maintain near-perfect IT hygiene then that is a red flag that the two teams need to pull together more closely, or they'll continue to allow significant risk within their organization.

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

"There's this perception in the press that most hacks are done by nation-states on shiny zero-day vulnerabilities," says Scott Lowe, managing director and founder at EndpointX. "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."

At the same time, security and operations teams will naturally pull together more closely as they develop the shared capabilities necessary to maintain near-perfect IT hygiene.

Reduced Resource Competition Between the Two Functions

Over the past year, many organizations had to choose whether their operations or security teams got to do their job. These organizations lacked the computational resources and bandwidth for both teams, so they typically allowed their line-of-business operational technologies to continue to function and asked their security teams to pause their work.

> *"In the move to work from home, many organizations have given malicious actors a very easy way to enter. They opened the front door, opened the windows, and put up a sign saying they're defenseless."*
>
> Charles Ross, Chief Customer Officer, Tanium

The result of this resource competition was troubling.

"Security was an afterthought when bringing systems online," says Charles Ross, chief customer officer at Tanium. "In the move to work from home, many organizations have given malicious actors a very easy way to enter. They opened the front door, opened the windows, and put up a sign saying they're defenseless."

Organizations must find a way to reduce the resource competition between operations and security to ensure both functions can operate at the same time.

Shared Set of Tools for the Two Functions

Security and operations teams commonly use separate sets of tools. This separation contributes to — or outright causes — many of the issues that this ebook outlines above:

- Different tools produce different data sets around assets in the environment, vulnerabilities on those assets, and the potential risk they're creating, which prevents security and operations teams from seeing their challenges in the same way.
- Teams commonly use different tools to establish that visibility and to perform controls like applying patches, updates, and configurations, making it difficult or impossible to see overall coverage levels and whether new controls were applied to standards.
- Security and operations teams both use tools that consume high volumes of the same computing resources. To work, those tools consume bandwidth to connect back to the central network. Thus, they're commonly not able to be in use at the same time.

Organizations must find a way to allow their security and operations teams to work from tools that integrate well with each other or work from the same shared tools.

Five Steps to Bring IT Operations and Security Closer Together

This advice tells a simple story: Reduce competition between operations and security. Bring the teams together through a shared set of capabilities and projects. And give them tools that integrate well together or operate from the same platform.

To help you bring this advice to your organization, follow a simple five-step process to unite your security and operations teams. This process will give your security and operations teams the capabilities, projects, and tools to unite them at natural touchpoints, while giving your organization stronger security against today's most dangerous infrastructure-based threats.

These five steps to bring operations and security closer together are:

Step One: Assess your present state of operations and security.

Step Two: Develop distributed visibility and control.

Step Three: Establish and maintain near-perfect IT hygiene.

Step Four: Embrace the cloud and distributed-edge computing.

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

Step One: Assess Your Present State of Operations and Security

Ask yourself a few questions to determine how close your operations and security functions currently work and where they exist in silos when they should be working more closely.

- ✓ Have my operations and security teams competed for resources over the past year?
- ✓ Did I have to ask one team to pause their actions entirely to allow the other to function?
- ✓ Do my operations and security teams share a single source of truth for our assets?
- ✓ Do we still have blind spots in our visibility and control within our distributed network?
- ✓ How well does my operations team meet the standards set by my security team for controls like patching and updating? Are we able to even measure our compliance?
- ✓ Do my security and operations teams utilize different tools? How well do those tools integrate with each other, if they integrate with each other at all?

Step Two: Develop Comprehensive Visibility, Control, and IT Hygiene

Review your answers from step one and make a list of gaps in your visibility and control over your distributed asset networks. Even if you don't have significant gaps in your visibility and control, take a moment to ensure you have developed these capabilities to a mature degree.

Ralph Loura, CIO of Lumentum, provides a practical guideline for how mature your endpoint visibility and control must be to effectively defend yourself against modern threats.

To deploy mature endpoint visibility, you must meet these criteria.

"Having good endpoint-edge intelligence is the key to everything else," explains Loura. "I need intelligence coming off every device, all the time — what's occurring on it, what may or may not have been deployed, and what activity that is normal or abnormal that's occurring on the device — so I have the information I can use to make better decisions about how to proceed."

To deploy mature endpoint control, you must meet these criteria.

"Having good endpoint-edge intelligence is the key to everything else."

Ralph Loura, CIO, Lumentum

"I need to be able to touch every device on a moment's notice when I need to," Loura says. "When these things land, they can move very quickly. Being able to rapidly respond, isolate, and recover are key capabilities to prevent a minor issue from becoming a major issue — and ultimately potentially becoming a real significant issue in your environments."

Step Three: Establish and Maintain Near-Perfect IT Hygiene

Once you confirm or develop mature endpoint visibility and control, your security and operations teams must use these capabilities to establish and maintain pristine IT hygiene.

Both teams must collaborate to consistently identify vulnerabilities, define standards, and perform the fundamentals of patching your systems, updating your applications, and configuring your devices properly. And they must continue to move closer until they're able to perform these actions to a near-perfect degree on every asset in your networks.

"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," Hodson says. "Well, unfortunately, it only takes one weak point in any organization to be compromised and then used as a vector to move laterally and propagate across an organization."

> *"Unfortunately, it only takes one weak point in any organization to be compromised and then used as a vector to move laterally and propagate across an organization."*
>
> Chris Hodson, Global Chief Security Officer, Tanium

Step Four: Embrace the Cloud and Distributed-Edge Computing

You have two primary options to reduce any resource competition that might occur between your security and operations teams and to ensure both groups can always do their jobs. You can:

1. Reduce the amount of shared computing resources that either group needs to consume to perform their work.
2. Reduce the number of applications that need to connect back to a central headquarters and consume bandwidth to work.

To carry out either option, organizations must rethink security and operations tools with legacy hub-and-spoke architecture, and look towards more modern approaches including cloud platforms and, especially, solutions that utilize edge computing.

"Some of the more successful organizations that I've been working with are looking to the computer power of the endpoint to do more with less," Hodson says. "It's critically important that security and operations teams can conserve resources by computing as much locally on the endpoint, and only send telemetry and information that's necessary for their reporting, patch, and vulnerability management systems."

Step Five: Re-Evaluate Your Operations and Security Point Tools

Finally, when you re-evaluate your legacy hub-and-spoke tools, take a broader look at all the applications that your security and operations teams are using, and determine how well your solutions work together.

For each of your teams' tools, ask:

- Is this an isolated, single-function point solution?
- Does it take a lot of work to integrate with our other tools?
- Is it used by both our security and operations teams, or only one of them?
- Does this work from a shared data set, or provide its own view of our network?
- Gut check — does this tool bring our two teams closer together, or further apart?

No need to complicate this exercise. Take your answers and consider replacing any isolated, single-function point solution that creates distance and disagreement between your security and operations functions. When you do, consider replacing it with a platform-based solution that combines security and operations capabilities within a single pane of glass.

"You need a well-instrumented platform that you can use to run data collection and run execution and action on a wide range of devices across the globe," Loura says. "Having an effective endpoint security and management solution is really key."

An effective security and endpoint solution like Tanium.

How Tanium Gives Operations and Security a Single Platform to Share

Tanium closes the gaps between operations and security teams. Over the past year, a diverse range of organizations and security leaders have used Tanium as a unified platform to consolidate many of their endpoint management and security capabilities and give their operations and security teams a single, unified platform to work from.

With Tanium, these organizations have established a single source of truth for their operations and security teams, and a comprehensive suite of endpoint solutions that integrate natively with each other. By using Tanium, these organizations have been able to create congruence and accountability between the policies and standards that their security teams set and the delivery on those mandates by their operations teams.

Operations and security teams use Tanium together for a few reasons. Tanium:

- Delivers real-time visibility and remote control over expansive endpoint environments, making it easy to raise the barrier to entry into organizational networks and perform rapid incident investigation, response, and attacker eviction.
- Has distributed architecture and edge computing capabilities to perform complex endpoint management and security tasks at scale, all while preserving computing resources and mitigating competition for those resources.
- Offers role-based access controls that allow users from operations and security teams to safely use the Tanium Platform at the same time, providing visibility into each other's actions without allowing either team to interfere with the other or overstep their roles.
- Can deploy new endpoint management and security capabilities in hours or days — not weeks or months — which allows technology leaders to quickly spin up new capabilities, address any gaps in their tooling, and rapidly unite their operations and security teams.

While technology leaders use a wide range of Tanium's capabilities to bring their operations and security teams closer together, the table below outlines solutions that are most effective for organizations uniting these two functions.

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

Patch and Software Management
Provides the ability to apply large-scale patches and software installation and updates to countless distributed endpoints, without consuming significant network bandwidth or threatening outages.

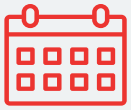
Vulnerability and Configuration Management
Provides the ability to find open vulnerabilities, compliance issues, and policy misconfigurations and to remediate problems within your rapidly changing networks.

Unite Your IT Organization and Security Teams to Be Ready for Whatever Comes Next

The future remains uncertain. You must find a way to maintain continuity and security, all without knowing what your organization will look like tomorrow or what threats you'll face.

We can't tell you the answer to those questions. Nobody can. But we do know this — you must face tomorrow's challenges as a united IT organization, and you can only do so if you bring your operations and security teams closer together. Only then will your organization be **ready for whatever comes next**.

Learn how the Tanium Platform can help make your IT and security operations more efficient and effective, helping bring far greater agility and security to your organization.



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

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.