A new class of converged endpoint platforms for a better breed of IT SecOps

The endpoint environment has transformed, but the balance between a superior user experience and effective security remains — needing better support than ever.

TANIUM

A new class of converged endpoint platforms for a better breed of IT SecOps

The endpoint environment has transformed, but the balance between a superior user experience and effective security remains — needing better support than ever.

Contents

The IT operations challenge

In the past, CIOs had to manage and secure a relatively limited number of endpoints, most of which lived on-premises within technology environments that rarely changed. Today, CIOs must manage and secure millions of dynamic, diverse, and globally distributed endpoints located across cloud and hybrid networks. Each of these endpoints introduces operational risks and security vulnerabilities, and must be monitored, managed, and secured in real-time to ensure their performance.

The IT security challenge

These endpoints also face a growing wave of cybersecurity attacks. A ransomware attack now occurs every 11 seconds, and the potential impact of a breach continues to grow as business processes become increasingly digital and interconnected.

Point solutions no longer suffice

Unfortunately, many CIOs are struggling to manage and secure their new endpoint environment. They are still using legacy point tools that were designed to work in small, static environments, and are failing in today's endpoint realities.

Balancing between IT operations and security

These tools are also creating silos between IT operations and security teams. Many of these tools are licensed and used by individual functions, teams, and employees. They give everyone a different view of the endpoint environment and make it impossible to build cohesive end-to-end endpoint management and security processes.

Worst of all, they stop IT and security from collaborating on key efforts — like applying patches and configurations — to close commonly exploited endpoint vulnerabilities. Neither team can agree on which is more important — maintaining performance even if it means leaving some security gaps open or locking everything down even if it means limiting operations — and this moment of change and conflict has reignited many long-standing questions about how these two functions should work together.

- *Should IT operations and IT security remain separate functions, or should they become one?*
- *Should IT Operations be absorbed into IT Security? Should IT Security be absorbed into IT Operations?*
- *Should either of these exist as their own standalone functions, or should they both become an embedded part of the business functions that they serve?*

Why legacy point solution tools are failing in today's environments

Most legacy endpoint tools were built to perform one task — often for just one endpoint category — and operate independently of each other. When CIOs attempt to develop a complete endpoint management and security capability using these tools, they are forced to build a stack of dozens of point solutions. And as the endpoint environment has transformed with new endpoints and new operational and security risks to mitigate, CIOs have been forced to keep adopting more and more tools.

The result? Using legacy endpoint management and security tools, organizations:

- **Face a growing visibility gap.** According to recent research, **95% of organizations have 20% of their endpoints undiscovered and unprotected.**
- **Wrestle with increased complexity.** 75% of IT operations, security, and business leaders now report too much complexity from their technology, data, and operations.
- **Can't answer basic questions.** These include "How many endpoints do I have? What applications run on them? How many have basic controls applied?"

Clearly, legacy point tools are failing to manage and secure today's endpoint environments. CIOs need new tools built around a new approach.

IT operations and security teams are struggling too

Both teams are struggling to adapt to the recent move to hybrid technology environments. IT operations is struggling to bring their new endpoints under management, while IT security is struggling to lock down as many of these new systems as possible.

Time to converge IT operations and security functions

IT operations and security must now converge. To do so, we first need to understand:

- What we mean by converge and how it differs from previous solutions.
- The first action you must take to converge these two functions.
- The reasons why now is the time to converge them.

IT operations and IT security are suffering from a visibility gap that is largely created by the two functions operating entirely separate from each other. First, we must converge IT and security around a single source of truth.

Most IT operations and security teams have their own set of point tools. Each of these tools only offers a small piece of the solution required to manage and protect endpoints, and many of these tools are redundant between the two functions. These siloed tools often collect their own data and make it difficult — if not impossible — for either CIOs or CISOs to stitch together a comprehensive picture of the environment in real time.

Despite heavy investment in new tools by both IT and security, this visibility gap isn't closing — it's growing. A recent study found that in 94% of enterprises, up to 20% of all endpoints remain undiscovered and unprotected. This visibility gap — created by IT and security operating separately — causes big problems for both functions.

- IT must manage its endpoints without being able to answer basic questions like "How many endpoints do I have" and "What applications are we running?"
- Security must protect their endpoints without knowing simple things like "Are my endpoints patched" and "Do we have proper controls on every endpoint?"
- IT and security must agree on priorities without sharing the same picture of what vulnerabilities exist in the environment and what it takes to close them.

To solve these problems — and to bring IT and security closer together as a whole — the two functions must create and converge around a single, comprehensive, and real-time picture of their environment. And now is the right time to create this single source of truth and lay the foundation for broader convergence between IT and security. Here's why.

Why organizations need IT operations and security convergence more than ever

For the most part, IT and security must now converge due to multiple long-term trends that have reached a tipping point.

Ransomware and other attacks are succeeding

Organizations spent over $160 billion on cybersecurity this year, yet ransomware attacks are still occurring every 11 seconds. Despite endpoint management and security getting more attention than ever, these problems are only getting worse.

The attack surface is larger than ever

The pandemic and the creation of large-scale hybrid networks are only part of the problem. The global network of Internet-of-Things (IoT) devices is expected to grow to 43 billion devices by 2023, and all digital devices are becoming more integrated than ever.

Most security challenges are operational in nature

The most effective ways to close the attack surface and defend against ransomware involve coordination between IT and security, including asset management, configuration management, patch management, and application security management.

Endpoint technology has advanced

Organizations no longer need to deploy dozens of point tools to manage and secure their endpoints. They can now replace these tools with a converged endpoint management (XEM) platform that consolidates all necessary visibility and workflows.

These trends and challenges will only grow. Organizations must solve them while they are still manageable. And convergence between IT and security is the solution.

Converge, not merge

Converging IT and security is not the same thing as fully merging the teams with each other. There are a few reasons why they must maintain some independence from each other, and remain separate functions:

- While IT and security share some activities and outcomes, they will always have their own distinct goals that still need to get done.
- Organizations will always need teams and leaders who offer specialized perspectives and skills and solely focus on how a narrow domain operates.
- Neither function is "correct" all of the time — there are times IT should be the priority and times security should be — and both functions need advocates.

For these reasons and more, merging IT and security is not an option. At the same time — as we'll detail later in this article — maintaining the status quo is no longer an option. Thankfully, converging IT and security offers a best-of-both-worlds solution.

When you converge IT and security, you allow them to remain as separate functions, but you bring them closer together. To do so, you break down certain siloes between the two functions, you sync their priorities, and you create conditions where they can coordinate and collaborate on shared activities. Overall, when you converge IT and security, you help them act like one team in the moments they intersect — primarily around managing and securing endpoints.

While there are multiple ways these functions can work closer together to keep endpoints secure and operational, there is one initial area where IT and security must converge ASAP — shared visibility.

> "To fully embrace an XEM strategy, it's clear that IT and security pros can't simply invest in a tool — they must also embrace a mindset shift and start working collaboratively."
>
> **Andrew Hewitt**
> Senior Analyst, Forrester
>
> Forrester blogs, *Endpoint Management 2023: It's Back To The Basics,* November 2022.
>
> **Read more of Hewitt's thoughts on XEM and endpoint management →**

Converged endpoint management platforms

CIOs need a new technology solution that corrects the problems with legacy point tools, and overcomes the challenges of endpoint explosion, tool proliferation, and IT modernization. This solution must offer a holistic approach to endpoint management and security that unifies three core aspects of these activities. They must cover:

- **Every Endpoint:** They must create visibility across laptops, desktops, mobile devices, containers, sensors, and every other type of endpoint from one agent.
- **Every Workflow:** They must perform a full range of actions — from asset discovery, to threat hunting, to client management — all from one console.
- **Every Team:** They must use this single source of truth and a common set of tools to align cross-functional functions, teams, and individual roles.

Tanium is the only **converged endpoint management (XEM) platforms** that meets these criteria. It consolidates the functionality of dozens of point tools into a single dashboard where teams can see, control, and trust everything happening on their endpoints. By doing so, these converged platforms give CIOs and their teams:

- Real-time visibility and a single source of truth for their endpoint data
- Reduced tool sprawl and significantly less complexity to manage
- Instant and accurate answers to their most important questions

Most importantly, **converged platforms eliminate silos in endpoint management and security.** They act as the backbone for all crucial interactions between endpoint data, controls, and teams in one place, and give IT, security, risk management, and other technology functions one "home" to seamlessly collaborate from. With the right platform, you can drive most of your endpoint use cases for most roles:

- **CIOs** can patch, update and properly configure their endpoints.
- **CISOs** can investigate and respond to threats in real-time.
- **Infrastructure teams** can scope cloud migrations in weeks (not years).
- **Procurement teams** can see if they're licensing software they don't need.
- **Data custodians** can find and remove sensitive data at scale.
- **Auditors** can track if a company complies with its regulations and compliance.

In sum: With the right converged endpoint management platform, CIOs can solve most of their core operations and security challenges.

Picking the right converged endpoint management platform

When evaluating the right platform to adopt converged endpoint management, CIOs must ensure they select a solution that provides three key qualities.

- Visibility into every managed or unmanaged endpoint in real-time.
- Control across cloud, on-prem, and hybrid estates in seconds.
- Truth composed of accurate, high-fidelity data for every endpoint team.

Consider these to be table-stakes for any converged endpoint management solution you evaluate, and the key to solving most modern endpoint management and security challenges created by legacy tools.

The Tanium advantage

Tanium is the world's first converged endpoint management solution: a single platform that can identify where all your data is, patch every device you own in seconds, implement critical security control tools and do it all within a single pane of glass.

Learn how Tanium is converging tools across the IT Operations, Security and Risk Management space to bring teams together.

See Tanium in action:

Let us show you how Tanium's converged endpoint management platform gives complete visibility, control and trust in IT decision-making.

Request a demo →