White Paper

Converged Endpoint Management Delivers the Goods: Risk Reduction, Productivity Gains, Licensing Fee Savings, and Improved Employee Experiences

Sponsored by: Tanium

Michael Suby Phil Hochmuth

April 2023

IDC OPINION

Although organizations recognize the inherent value of a prevention-first approach to security, it is not easy. Endpoint security and management teams have not always found common ground. Although both share the goal of reducing risk, they often work in a segregated fashion. Consequently, they choose technology products that support their individual functions rather than products that support both, missing opportunities to serve the greater organization better by structurally reducing risk, increasing internal productivity, reducing software licensing costs, and improving end-user experiences. IDC's research has found that these benefits are being realized by organizations that have shifted their technology approach from a portfolio of independent products to a converged endpoint management (XEM) platform.

THE CONVERGENCE OF ENDPOINT DEVICE MANAGEMENT AND SECURITY

The management of endpoints in professional IT environments has traditionally been a separate function from endpoint device security. The former involves device deployment, OS and application distribution/updating, and overall software/hardware life-cycle management. Ongoing support and help desk tasks are often associated tasks. The latter involves the deployment of endpoint security technologies. The ongoing management of the security environment, including policy enforcement, threat monitoring, and incident response are also associated duties.

These two domains always overlap. Policy enforcement spans both OS configuration and security controls. Installation of endpoint security software itself is an IT operations function. The boundaries become even more blurred when considering responsibility for vulnerability management (detection and patching) and compliance.

Most global IT teams are still separate on this front, but there are indications that these teams are starting to converge. In a global survey of 1,524 IT decision makers at enterprises and midsize businesses, IDC asked respondents about their approach to end-user device management and security and the intersection of these functions with regard to the concept of converged endpoint management, which unifies teams and tools to more coherently manage and secure endpoints.

In addition to the survey, IDC conducted in-depth interviews with four IT security and management professionals from organizations that are partially or fully using Tanium's platform of endpoint management and security tools. The following sections highlight the benefits and challenges of XEM and Tanium's own XEM approach.

THE BENEFITS OF CONVERGED ENDPOINT MANAGEMENT

Reducing Risk and Complexity

Endpoint device management and security teams have come a long way in terms of integrating functions, tools, and processes, but many groups are still hamstrung by complexity. One of the primary tasks shared between endpoint management and security operations teams is the continuous identification of new threats and vulnerability patching. Groups often use separate but similar tools to create alerts, produce logs, and extract risk data from the endpoint environment. Actions are often uncoordinated, redundant, and at worst, counterproductive.

Analytics to Reduce Audits and Data Sprawl

Any team responsible for managing and securing corporate endpoint devices has a vested interest in reducing the scope of audits or at least streamlining the compliance process. Such tasks often straddle management and security duties, as mandates can cover areas from endpoint operating systems and device configurations to location of sensitive data and the presence of specific security tools and functions (e.g., endpoint antimalware and encryption.).

The monitoring and discovery of threats is important, but endpoints can also potentially store sensitive or confidential information. If certain types of regulated or sensitive data are stored inadvertently on endpoints, companies may face major compliance violations and regulatory fines.

An example of addressing sensitive data sprawl using an XEM approach came from a large Asia/Pacific-based eldercare management firm IDC interviewed for this white paper. Part of the organization's mission is to check on elderly or mobility-challenged patients in their homes, requiring field workers to travel and collect data on mobile computers. The particular challenge the firm faces

comes from the heightened requirements for collecting and verifying digital COVID-19 vaccination certificates of employees and home visitors. The certificates contain confidential health information, which is not supposed to be stored on just any endpoint.

"The question [we needed to answer] was, where do we have COVID vaccination certificates within our environment?" said the firm's head of cybersecurity, risk, and compliance (CRC). "With the Tanium platform, we could scan across our entire landscape to find every instance of these certificates present on endpoint devices," which enabled the firm to meet the new requirements and remain in compliance.

Real-Time Vulnerability and Threat Awareness

Enterprise IT operations and security teams need quick answers to questions about vulnerabilities as well as the overall state and status of a deployed fleet of endpoints. When new vulnerabilities come up in vendor-alert bulletins, the tech press, or online forums, companies need to know their exposure without tasking ops teams with lengthy audits and evaluations of every system on the network. According to the IDC survey, real-time visibility into the endpoint state was a top-desired feature from an XEM-centric platform, with 58% of firms saying it was a requirement.

The XEM approach includes tools that provide quick threat detection, patching, and remediation — a critical requirement. According to the head of CRC at the eldercare firm, "The only patching we did in the past was around operating systems. Now that we can actually see what is installed, we can see what versions of third-party apps are old or out of date. We can now implement third-party application patching as well, not just [applying patches to] the Microsoft operating system" on employees' PCs.

Reacting more quickly to high-impact malware and advanced persistent threats (such as WannaCry, NotPetya, and Log4j) drove the adoption of Tanium's XEM solution for this company. Before Tanium, building reports on exposures to critical vulnerabilities or discovering dangerous malware in the environment was a glacial process. "It had taken a whole day to know what systems were vulnerable on previous platforms," said the firm's CRC head, and a full day of exposure gives threat actors more than enough time to infiltrate systems and data.

One key goal for organizations looking to converge endpoint security and management is closing the gap between detecting vulnerabilities and deploying patches to update affected software. The eldercare firm's IT team realized this benefit. According the head of CRC, "We were able to deploy patches to affected systems quickly, and compliance of those endpoints shot up from 1% to over 90% in a very short time period."

> We were able to deploy patches to affected systems quickly, and compliance of those endpoints shot up from 1% to over 90% in a very short time period."
>
> Head of CRC

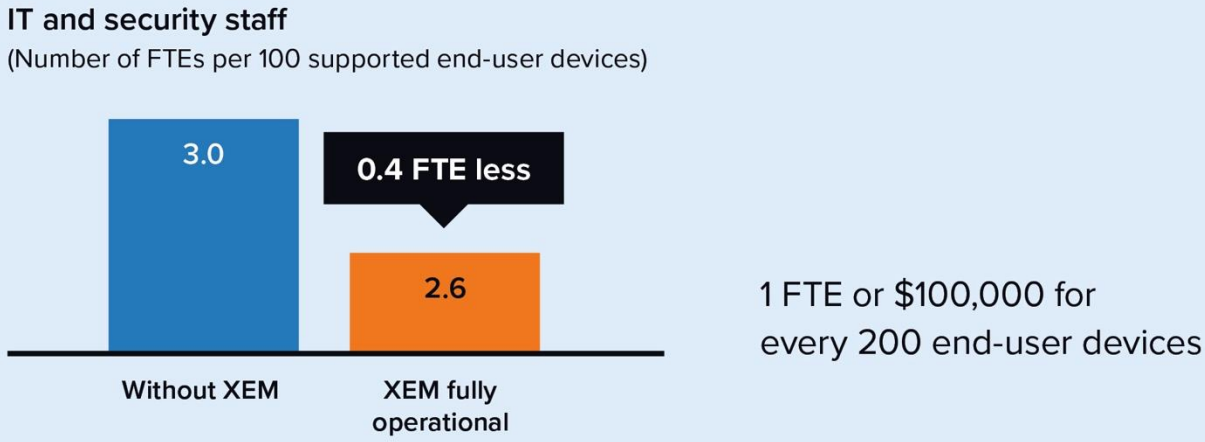
Prevention-First Security

Prevention-first security is a best practice in managing device hygiene. XEM strongly enables this approach. By elevating practices and procedures for device hygiene with management (patching and updating software, including OS and third-party apps) and security (app whitelisting, policy settings), XEM-centric firms can reduce their attack surface and overall risk and susceptibility to breaches.

Another prevention-first approach includes reducing the footprint of software running on devices. This involves reining in the number of applications and software packages. Depending on a machine's user permissions, app sprawl may stretch into the dangerous territory of unapproved apps and programs being downloaded and installed in user environments. This raises concerns about both what enterprise IT knows and doesn't know with regard to end-user software environments.

Cutting Costs

Complexity in an enterprise endpoint environment is tied closely to cost. More-complex environments are often associated with higher costs, whereas more efficient, less-complex environments are often cheaper to run and maintain. Organizations can reduce cost and complexity by reducing the number of technologies used; the greater staffing levels required to maintain and run multiple platforms helps make this approach one of the most effective cost-reduction initiatives.



Vendor and Tool Consolidation

Firms use multiple management and security tools for various reasons. According to IDC's study, more than half of U.S. firms use multiple endpoint management and security products and vendors to manage various endpoint types (e.g., Windows, Mac, Linux, mobile devices). Some security products excel or specialize in certain functions, such as endpoint protection or detection and response. At large or multinational firms, regional teams may use different tools, as certain technologies or vendors may be more well-known or only be available in certain locations.

Meanwhile, successful vendor consolidation involves retiring single-purpose tools used for vulnerability management, asset management, compliance, file integrity monitoring, security configuration management, and threat response. Consolidated reporting features that incorporate all the aforementioned functions is also a benefit.

With many firms mired in multiproduct complexity, 60% of IT decision makers want to reduce the number of vendors and tools they use in both endpoint management and security. Reducing costs/complexity and unlocking advanced features are some of the top drivers here.

of IT decision makers want to reduce the number of vendors and tools they use in both endpoint management and security.

Embedded XEM Features Replace Whole Products

One global logistics company said consolidating multiple security tools cut their software licensing costs and subscription fees in half, saving hundreds of thousands of dollars annually. The company had deployed Tanium XEM for asset management and discovery but then discovered modules and functionality in the XEM platform that allowed them to replace tools in other areas, such as file integrity monitoring. This initial consolidation cut spending significantly. The cost savings were enough to convince them to replace their previous product with Tanium XEM.

"People don't want to change what they know. I've seen it time and again," said the logistics firm's technical director. However, the significant savings as a result of consolidating with Tanium changed their minds quickly. "We saved so much money that nobody could defend wanting to keep what was near and dear to them" simply because it was familiar.

Using Tanium to consolidate security and management functions also allowed the logistics firm to eliminate many manual processes. "In the past, there was more of a spreadsheet sort of approach to keeping track of assets and applications," according to the technical director. The firm now deploys the Tanium XEM platform for asset discovery and inventory to get a more accurate and automated view of its entire IT estate. This additional level of automation and improved efficiency came as a byproduct of the firm's larger Tanium solution deployment. The company increased simplicity and quality of asset management with no incremental cost while simultaneously lowering overall IT spend.

One large U.S. healthcare firm estimated their XEM deployment saved them over $1 million annually. When IT staff discovered that the Tanium solution had a native asset-tracking function that the company was paying for from another vendor, they quickly stopped double paying.

By choosing XEM, the firm was able to “replace multiple products” and “steal functionality from other products, [thereby reducing the] need to spend as much on those products compared to before,” said the company’s endpoint management director.

.

Consolidation and Feature Extension

Cost savings drives the adoption of XEM in many enterprises. In North America, 87% of IT decision makers in IDC's study said their organization plans to consolidate multiple endpoint management products to a single-vendor solution in the next 18 months. More than half of firms are on an even faster pace, looking to consolidate in the next 6 to12 months.

The goal is to do more with less – cover more functions, features, and capabilities from a single software product or platform. XEM’s ability to extend functionality of one platform to multiple teams was invaluable to the global logistics company as its IT team saw requirements grow around governance, risk, and compliance.

"When we learned that we needed to deal with SOX [Sarbanes-Oxley Act] and then HIPPA [Health Insurance Portability and Accountability Act] as well as all these other regulatory requirements, the GRC [governance, risk, and compliance] team grew faster than the team that manages overall PC deployments,” said the technical director of the logistics firm. As the GRC team grew, it acquired multiple compliance software products and tools. This drove up IT spending at an alarming rate.

To help the logistics firm expand and gain new business, their GRC team leveraged the Tanium XEM platform to complete its accreditation and compliance checks, which helped communicate to partners and customers that its IT environment was secure and trustworthy, a critical requirement for ongoing operators.

Spawning Greater Collaboration

Organizations recognize that to maximize the benefits of XEM, they must instill a higher degree of collaboration among their operational teams. However, forcing cross-team collaboration is not a winning approach. Fostering organic collaboration is superior, as it allows teams to discover new avenues of collaboration and take ownership of the results.

They also need a place where collaboration can be discovered and nurtured, which is where XEM shines. As one large U.S. healthcare organization said, “Our endpoint management and endpoint security teams did not collaborate well previously, but with …Tanium XEM [we are] in the same sandbox, and from that sandbox, greater collaboration has unfolded.”

At times, collaboration is driven by necessity. In the case of a global software company, mandatory downsizing in 2023 trimmed the IT and security operations teams by four full-time employees (nearly 30%). This company had previously migrated to the Tanium XEM platform, and because the IT and security teams were unified on Tanium and could work together in real time from the same data sets, the firm was able to absorb the headcount reduction and continue its IT and security modernization.

Improving the Employee Experience

Employee experiences, partly derived from their use of devices that the endpoint security and management teams oversee, is of critical importance. Bad employee experiences degrade productivity and negatively color user perceptions of how the organization values their contributions.

Endpoint security and management functions should exert a near-transparent touch to minimize the interruption in employee activities. Minimal impact, however, should be just the starting gate for XEM aspirations. With deep and near-real-time visibility into employee devices, XEM should also detect the warning signs of impending user-impacting circumstances and resolve them before the user has a negative experience. IDC's research uncovered evidence of both minimal impact and averting bad employee experiences among firms that adopted XEM.

Hands-off, Accelerated Updating and Patching

When comparing organizations with fully operationalized XEM platforms and those without, IDC survey results show that the fully operational XEM organizations improved their security posture by deploying Windows patches, updates, and upgrades 22% more often. Staff productivity also improved as fully operational XEM organizations had shorter deployment times and more often automatically deployed updates upon their release.

IDC also heard from a subset of Tanium customers that before Tanium, deploying new applications on employee devices was a manual process that lengthened the time users were out of service; in some instances, employees had to be directly involved in the deployment. After Tanium, new software applications were installed in a self-service manner. Not only did self-service deliver a better user experience, it also saved time for endpoint management staff and sped up software rollouts.

Eliminate Under-Performing Equipment

The adage "You cannot protect what you can't see" was cited by several Tanium customers; respondents also shared, "You cannot equip employees for success if you don't know what they've got." In other words, some organizations did not know that users were running required business applications on old, underpowered PCs, nor did they have the means to detect software-hardware mismatches. Concerned about the potential of "quiet quitting," one Tanium customer used the data gathered from the XEM platform to locate mismatches and prioritize older PC replacements. This effort sent a reaffirming message that employee experiences are taken seriously by IT.

Decrease Help Desk Tickets Through Proactive Monitoring

IT help desk tickets are a double resource burden on organizations. First, by virtue of being initiated by an employee, a ticket signals that a user's work routine and productivity have been adversely affected and they are unhappy. Second, IT must devote time and resources to investigate and resolve the ticket. The bottom line: Help desk tickets are a cost to the business, and it is only prudent to manage them downward.

With the XEM platform, an analytics engine can be tuned to detect emerging performance issues. In a similar vein, the same curated mechanisms that endpoint security and management teams use to take action on endpoints can remediate performance-impacting events. The end result helps avoid a negative employee experience and countless help desk tickets. XEM allows IT personnel to operate from a platform they are already familiar with and, most importantly, it facilitates the transformation of employee performance management and help desk ticketing from a costly, reactive operation to a proactive one that helps ensure employee routines remain routine.

TANIUM'S XEM VALUE REALIZED

Building upon its foundational and distinctive architecture and its ability to unify real-time data, analytics, and workflows onto a single platform (whether in the cloud or on premises), Tanium is well positioned to deliver the benefits of XEM to its customers.

The comprehensiveness and confidence in the Tanium platform was often cited by XEM adopters during IDC's in-depth interviews. Considering the dynamic nature and complexity of IT footprints and the uncertainty of what cyberthreats lurk around the corner, organizations that lack comprehensive and current visibility across their entire IT estates are handicapped, unsure if their IT and security actions will match their intentions.

In addition, both IDC survey and in-depth interviews confirmed the importance of a prevention-first security approach, the need to reduce software licensing fees without sacrificing outcomes, and the desire to elevate cross-team collaboration through vendor consolidation. Separate and isolated data stores and technologies may have been justifiable in the past but are less suitable now. Organizations are looking for a platform approach with broad capabilities from a trusted partner.

This platform approach, the means for organizations to realize XEM benefits, can't be created overnight. Rather, it is progressively built and refined to incrementally address the evolving needs of organizations. It is also built on capabilities that are native to the Tanium XEM platform:

- **Risk and compliance management.** Teams can monitor file and registry changes and ensure compliance with privacy regulations and practices.
- **Client management.** All systems can be kept running and up to date with **automated patching** and minimal downtime.
- **Threat hunting.** In a proactive approach, **threat hunters** sleuth through systems looking for forensic evidence of compromise, identifying risks, and rooting out attackers before they can do damage.
- **Asset discovery and inventory.** Converged platforms make it easier to get a **complete inventory** of hardware and software assets.
- **Sensitive data monitoring. Sensitive data is tracked and managed** to help protect it from attackers.
- **Service management.** IT teams can better support employees and resolve help desk tickets. Teams can create a streamlined help desk workflow using accurate, real-time data.

- **Anywhere effectiveness.** Converged platforms support a distributed and remote-working employee base and proactively solve IT issues before they arise.

A platform model is more than integrated capabilities; it also encompasses the relationship between the customer and the platform provider. Although customer interviews can present a biased view, the following aspects of the Tanium-customer relationship bear repeating due to the authentic substantiation that the customers provided:

- **Tangible value.** Tanium technical account managers were noted for being instrumental in driving deeper, more-effective use of the platform. As one customer zeroed in on, Tanium is a viable alternative to hiring a managed services provider.
- **Prevention first.** Vulnerabilities are inescapable in a digital world. As threat actors jump on newly found vulnerabilities, both in new and legacy software, endpoint security and management teams must rapidly develop vulnerability-scanning scripts that effectively pinpoint new threats so countermeasures can be taken. Customers appreciated Tanium's proactiveness in developing vulnerability-scanning scripts regardless of complexity, proof of a prevention-first security approach.
- **A partner rather than a vendor.** The platform model risks being leveraged by overzealous account teams attempting to increase total customer spend instead of aligning modules with actual need. The Tanium customers IDC interviewed, both large and small, appreciated the genuine effort by Tanium to find the mix of modules that best fit customer needs and timeframes, engendering a partnership rather than a transactional vendor relationship.

CHALLENGES/OPPORTUNITIES

Potential Loss of Pricing Leverage

A complex multivendor environment can be a risk to organizations, as it can introduce gaps in visibility, inhibit functionality, and raise overall costs. However, when an IT group narrows down its vendor list and consolidates functions to a few or even a single provider, they might lose leverage in pricing negotiations. A company that could once play multiple firms off each other to get the best price may find themselves stuck if they rely too much on a single source or provider. However, incremental cost savings on minor feature additions or upgrades are often offset by the overall improved efficiency and lowered costs by paring down the number of tools.

Integration Issues with Log Collection Platforms

Customers cited another potential challenge to XEM adoption: third-party system integrations, such as streaming logs for security information and event management (SIEM) platforms.

Depending on the type of vendor the organization standardizes on, another challenge may be adapting to disparate deployment technologies. On-premises, cloud-based, and hybrid models are all deployment options; in general, the industry is heading toward cloud and hybrid models.

What About Servers?

Just as the line blurs between endpoint management and security in many organizations (e.g., desktop/laptop PCs), so can the demarcation of responsibilities between server endpoints and

employee devices. Some organizations see all endpoints — servers, PCs, mobile devices, and more — as a single domain for management and/or security, where teams may share responsibilities or separately manage configuration and threats. Organizations considering an XEM approach must decide if server endpoints are part of the equation. This may already be decided in some large firms where datacenter teams handle back-end system management, security, and patching duties. In smaller or midsize organizations, and even some large enterprises, a single IT team or specialized subgroup has these responsibilities.

XEM tools and approaches can include back-end devices and systems. In the case of Tanium's XEM platform, server management and security are included capabilities. Many enterprises can benefit by extending Tanium XEM vulnerability scanning, real-time threat telemetry, and fast-patching capabilities to Windows, Linux, and Unix servers, in addition to back-end server virtualization and container management infrastructures. These use cases must be carefully accounted for and integrated into the XEM deployment plan at the start of any initiative.

CONCLUSION

IDC research has shown that organizations have realized significant benefits by shifting their endpoint security and management technology selections to an XEM platform. First, an XEM platform unifies teams to reduce cyber-risk. With a single source of truth for the organization's entire endpoint estate, the two teams can concentrate their attention and coordinate their efforts on prevention-first security, which reduces the attack surface through disciplined device hygiene and vulnerability management practices. Second, the shared experience of an XEM platform provides an environment for the teams to collaborate and increase their combined productivity. Third, vendor consolidation can produce significant cost savings that, based on Tanium's customer experiences, can materialize in the near term. Fourth, the platform approach that underlies Tanium XEM leverages existing infrastructure (endpoint agent, database, and analytics engine) to assist organizations in accomplishing additional objectives, such as improving the overall employee experience and avoiding help desk tickets.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com
