TANIUM

WHITE PAPER

Confronting the largest attack surface ever with Converged Endpoint Management (XEM)

Executive summary

Ransomware attacks are one of the fastest-growing cyber threats in recent history. The number of attacks increased over 140% in Q3 of 2021 despite organizations spending over $160B on cybersecurity last year.

Do you ever wonder why this high-priority problem is getting more money and attention than ever, and yet the problem is only getting worse?

That's because the industry's approach to security is flawed.

Every IT security and management provider offers only a small piece of the solution required to protect our environments. And to further exacerbate the situation, these different tools are often deployed in silos across organizations.

CIOs and CISOs are forced to buy multiple solutions, stitch them together and make decisions based on data that is stale, inaccurate and incomplete.

To make things worse, these tools lack real-time visibility. In fact, in 94% of enterprises, their tools may be missing up to 20% of the endpoints that require protection. Point solutions create gaps that hackers can exploit and only add to the complexity of an ever-growing attack surface area.

Stop for a minute. When was the last time you asked yourself these questions?

- How many endpoints do we have?
- What applications run on them?
- Which users have unnecessary administrative access?

To answer these questions, did you have to tap into multiple point solutions, then centralize, normalize and analyze the data from each solution?

It's time to end this cycle by taking an entirely different approach: deploying a converged endpoint management platform.

A single platform that provides visibility and remediation.

A single platform that provides real-time data and has real-time impact.

This platform manages and protects every type of endpoint, from laptop to cloud containers to sensors and internet of things (IoT), enabling teams to work together by bringing data across IT operations, security and risk and compliance management. Taking this platform approach instead of assembling diverse point solutions, you'll be able to see that it's possible to interact with every endpoint in seconds regardless of network scale and complexity.

Organizations now have a converged endpoint management platform they can trust and continue to expand and extend. They can readily and systematically rip out the accumulated morass of legacy point solutions and replace them all with a single platform.

The evolution of technology and society

We're in a dynamic time, where we see changes in both technology and the greater society that impact how we work and live. Every organization is dealing with these three massive changes:

Digital transformation

Digital transformation is changing how businesses operate and deliver value in every industry to those they serve. What used to be centrally controlled by gated perimeters has evolved into a sprawling web of software services, cloud infrastructures, and decentralized application services.

Enterprises now spend $700B annually on digital transformation projects, according to research firm Futurum. The research also shows that the typical enterprise has more than 200 actively used applications, and 60% of those applications turn over every two years. That pace of digital transformation is presenting a big challenge to cybersecurity.

Work from anywhere

The rise in remote work brought on by the pandemic has created an ever-changing dynamic perimeter.

Before the pandemic, most organizations took a castle-and-moat approach to cybersecurity. Corporate firewalls protected enterprise networks, ensuring the safety of on-premises devices, systems and data.

This approach no longer works as well as it did. Many IT resources now operate outside the moat — or firewall — and are vulnerable to cyber threats of all kinds.

If organizations don't have the ability to manage the security on those devices regardless of where they are, they are opening themselves up to a large attack surface and massive risk.

Endpoint explosion

Finally, the combination of digital transformation and work from anywhere is driving an explosion in endpoint devices expanding the edge with mobile devices, IoT, cloud containers, and sensors — all of which are potential entries for attackers.

Meanwhile, increasingly sophisticated attacks such as phishing, business email compromise, ransomware and others create a far more difficult endpoint management challenge than ever before.

Responding to that pressure, IT teams continue to acquire more and more tools, and these acquisitions are all too often siloed by team. Tanium's Visibility Gap Study in 2020 revealed that the average business uses approximately 43 IT operations and security tools, though this varies widely by size of enterprise.

But despite more tools and growing security budgets, the vulnerability gap isn't improving. It's actually getting worse. Organizations are spending billions on cybersecurity. Meanwhile, 20% of endpoints are going undiscovered and unprotected, and a ransomware attack still occurs every 11 seconds.

It is harder today than ever for CIOs and CISOs to assure and safeguard operations.

More complexity, more challenges

Organizations are dealing with extraordinary circumstances. It's easy to manage endpoints when the attack surface isn't growing or lead digital transformation when it doesn't need to happen overnight.

So how do you enable new and emerging technologies and facilitate digital transformation in these challenging times?

1. Modernize your legacy platforms, approaches and environments.

2. Manage ongoing compliance and regulatory demands.

3. Better manage security threats and growing attack surface.

Make no mistake: as we become more connected, the threats become more real. With a larger surface area, the threats are becoming increasingly complex and difficult to defend. And the bad guys, who are often state-sponsored, are using these same emerging technologies to wage a highly sophisticated war against us.

We need a convergence.

Why every organization needs XEM

Converged solutions unite tools and data into one unified solution. A converged solution is a system that enables convergence: it acts as the backbone for all crucial interactions between data, tools and teams to take place. It lives at the intersection of the domains in IT Operations, Security, Risk and Compliance Management. Converged solutions appeal to a wide range of users, enabling IT leaders and employees to collaborate.

Change and growth must be managed

Companies need a solution that solves endpoint explosion, tool proliferation and IT modernization of every endpoint, every workflow, every team.

Given the multitude of changes impacting IT, it is critical that organizations prioritize solutions that provide visibility across all their endpoints, control of those endpoints, and confidence in the quality of the data generated. It is paramount that companies combat tool sprawl and fatigue that serve only to increase a company's risk exposure and lower employee productivity through tool consolidation. Silos within organizations can be eliminated using common tools that combine IT operations, risk & compliance and security into a converged platform.

A converged platform like the one described must cover three things:

- Every endpoint. Visibility across the whole gamut of endpoints via a single pane of glass is a must-have; whether laptop, desktop, mobile, container, sensor – all types of endpoints must be known, managed and protected.

- Every workflow. Potential to take action and build any workflow a company needs must be enabled via one platform: every module (whether IT operations, security or risk & compliance) is merely a workflow relying on the same underlying platform capabilities.

- Every team. Alignment across teams around one single source of truth, the same data, and the same set of common tools is a baseline need to break down silos.

Converged platforms address the "technology-process-people" riddle

A unified platform that allows for quicker decision-making, high-fidelity data and multiple capabilities in one location replaces tedious manual processes. Combining the reach of IT operations, security, and risk & compliance into one location achieves what multiple legacy point solutions cannot. Teams can focus on what matters, doing their job cross-functionally, productively and safely, providing the most effective response to an environment where attackers are more aggressive than ever before, and customers demand more than ever. So how do you enable new and emerging technologies and facilitate digital transformation in these challenging times?

Outcomes of XEM

This converged approach will enable customers in four critical areas:

Visibility: With complete visibility, organizations can identify risks by scanning the endpoint environment in minutes. This is vital when you think of the ever-changing perimeter where devices are coming and going, or you're adding IoT devices or sensors.

Alignment: From an alignment perspective, you can create a common language between operations, security, and risk teams — all with a common data set.

Responsiveness: Through responsiveness, you can remediate vulnerabilities and address compliance with one click, one console, in seconds.

Control: You can move the perimeter of operations, security and compliance to where the network truly begins and ends — the edge.

XEM use case: Log4j

There's no better use case of XEM than the industry's most critical vulnerability ever, Log4j. With a converged platform, customers were able to perform detailed and complete discovery in real time, in-depth assessment, prioritization, and cross platform operating system agnostic remediation.

An XEM solution can find indicators of vulnerability, detect signs of exploitation, remediate and harden the environment, and report ongoing exposures. All of these pieces working together differentiates the XEM platform from anything else on the market.

Defining capabilities

Converged platforms solve the technology problem so companies can focus on the organizational problem.

Technical solutions should transcend technology. They need to enable a business solution. By enabling better communication among teams, and by providing visibility of assets, control of those assets, and trust in the data affecting those assets, teams can make decisions more quickly and in a more informed manner. Historically, accountability has been limited due to broken tools and siloed teams — but this is not the case anymore with the advent of converged tools. Gone are the days of unreliable tools and broken processes that result in incomplete outcomes.

Converged platforms turn old-school product mentality on its head

Rather than be tool-centric, converged platforms are device-centric. Instead of applying tools to the endpoint, converged platforms consider everything the endpoint needs and make the endpoint the focus. Converged platforms solve everything needed on a device's journey or lifecycle. Product teams developing converged platforms will adopt a big-picture mindset that outlines roadmaps addressing the diverse needs of the endpoint — from an operational lens to a compliance lens to a protection lens.

Converged platforms unite tools and data into one unified solution

Several core capabilities comprise converged platforms, housed within one single pane of glass — one dashboard to see, control and trust everything happening at the endpoint. View all the data incoming from all endpoints in one place:

1. **Risk and compliance management:** Monitor file and registry changes; comply with privacy regulations and practices. Scan the network for unmanaged assets; find compliance gaps; assess computers against industry benchmarks.

2. **Client management:** Do patch deliveries consistently and quickly. Keep all systems running and up-to-date with automated patching and minimal downtime; simplify, centralize and enforce critical configurations.

3. **Threat hunting:** Issue alerts on suspicious behavior and restoration of endpoints back to steady-state. Identify high-risk accounts and systems; find and fix vulnerabilities at scale; perform automated remediation through prioritized actions on endpoints.

4. **Asset discovery and inventory:** Do a complete inventory of hardware and software assets. Identify all machines on a network, including what software they have and how it's used.

5. **Sensitive data monitoring:** Track and manage sensitive data so that attackers can't. Quickly search for sensitive data and reveal its location to take action. Find unauthorized changes of events in file paths, scope for data exposure and potential risk, and index file systems.

6. **Service management:** Enable IT teams to support employees and resolve help desk tickets. Create a streamlined, help desk workflow using accurate, real-time data.

Converged platforms appeal to a wide range of users

CIOs choose converged platforms to ensure that their endpoints are patched for the latest vulnerabilities in hours and configured appropriately. CISOs choose converged platforms to serve as their last line of defense to respond to breaches. Infrastructure teams use converged platforms to scope cloud migrations in weeks, instead of months or years. Procurement teams use converged platforms to validate that they don't pay for more software than they use. Auditors use converged platforms to assess how well companies comply with a patchwork of regulatory and compliance frameworks. Data custodians use converged platforms to find and remove sensitive data at scale.

Clearly, converged platforms enable IT leaders and employees — across a range of functions — to manage and secure all their assets.

Looking ahead

Trends shaping today's IT world will only continue to accelerate

Remote work trends are here to stay. The need to manage and secure all types of endpoints (in and out of network) isn't going away. According to a Gartner survey, 48% of employees will work remotely at least partially after the pandemic ends; a Pew Research Center survey revealed that 54% of U.S. employees prefer remote work once the pandemic is over, and a Gallup report showed 6 in 10 managers plan to allow employees to work remotely more frequently than pre-pandemic. From these statistics, it is clear that a future distributed workforce means IT teams will continue managing and protecting endpoints physically outside corporate firewalls. Converged platforms like Tanium that yield visibility, control and trustworthy data to IT teams will continue to be paramount in a hybrid work environment.

Second, cloud migration will also continue to evolve, exposing sensitive data to risk of being accessed and mishandled. In 2022 alone, end-user spending on cloud services is projected to rise by 22%, according to Gartner. And Cloud is popular: The annual State of the Cloud Report found that 90% of organizations will rely on some form of hybrid cloud solution by the end of 2022. Longer term, by 2026, Gartner forecasts cloud spending will total at least 45% of all enterprise IT spending. Thus, companies will need solutions like Tanium that are cloud-friendly and that enable safe, secure operations as they migrate from on-premises solutions.

Third, artificial intelligence (AI) and machine learning-based algorithms (ML) will only become more crucial in the endpoint world. Adapting security policies and roles to individual users in real-time based on device type, device configuration, patterns of when and where they attempt to log in and other variables will be critical. Tanium can enable true AI/ML to notify users of suspicious behavior and automate remediation because of the quality of the data it has access to — and the speed with which it can return this data. Companies will continue investing in solutions like Tanium that automate, adapt and learn from threats constantly.

Tanium's converged endpoint management platform is positioned to capitalize on these future trends

With Tanium, customers have a converged set of modules for everything needed on a device to live and perform. Converging tools across the IT operations, security and risk & compliance space brings teams together: one platform to give them visibility, control and trust in their IT infrastructure.

Tanium is consciously building its platform with the mindset of what's needed to enable IT teams (operations and security) to do their jobs. Amid an ever-expanding attack surface, IT leaders can shift from reactive problem-solving to being proactive. Their teams are better able to communicate with one another, while referencing the same dataset and tools; no additional training is needed among teams; and it's simple to add more modules because each one is simply a workflow built on the same underlying platform. Teams need to manage fewer apps and tools, while experiencing a positive impact on business outcomes through increased collaboration.

At its core, Tanium is a data company that helps IT scale by converging the world of IT operations, security, and risk & compliance into one unified solution. That's the power of certainty.

References

https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

https://venturebeat.com/2021/09/26/digital-transformation-spending-is-up-to-700b-per-year-but-results-lag/

https://federalnewsnetwork.com/federal-insights/2021/04/what-the-pandemic-driven-increase-in-it-complexity-means-for-federal-agencies/

https://www.retaildive.com/news/76-of-cios-say-it-complexity-makes-it-impossible-to-manage-performance/516065/

https://hbr.org/2021/10/does-your-team-really-need-another-digital-tool

https://www.businesswire.com/news/home/20170918005033/en/Information-App-Overload-Hurts-Worker-Productivity-Focus

https://securityboulevard.com/2021/06/proliferation-of-devops-tools-introduces-risk/

https://www.advsyscon.com/blog/break-down-silos-in-it/

https://blog.trello.com/tips-to-improve-cross-team-collaboration

https://www.beezy.net/blog/too-many-tools

https://jfrog.com/devops-tools/what-is-devsecops/

https://www.dynatrace.com/news/blog/top-eight-devsecops-trends/

https://www.maltego.com/blog/tackling-tool-fatigue-soc-teams-need-interoperable-tools/

https://explodingtopics.com/blog/remote-work-trends

https://www.parallels.com/blogs/ras/green-it-cloud-predictions-2022/#:~:text=Gartner%20forecasts%20a%20rapid%20global,enterprise%20IT%20spending%20by%202026

https://workforceinstitute.org/workers-globally-wish-for-better-technology/

https://www.formstack.com/resources/blog-software-interoperability#:~:text=The%20term%20%E2%80%9Csoftware%20interoperability%E2%80%9D%20refers,behind%2Dthe%2Dscenes%20coding

https://www.darkreading.com/edge-articles/security-considerations-in-a-byod-culture

https://site.tanium.com/rs/790-QFJ-925/images/WP-Visibility-Gap-2020.pdf

https://www.globenewswire.com/news-release/2021/05/04/2222642/0/en/GitLab-s-Fifth-Annual-Global-DevSecOps-Survey-Reveals-2020-Was-Catalyst-for-DevOps-Tool-Adoption.html

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.