TANIUM

The cybersecurity fail-safe:

Converged Endpoint Management (XEM)

The future of endpoint security is XEM – It's time to converge security and operations.

The cybersecurity fail-safe: Converged Endpoint Management (XEM)

The future of endpoint security is XEM - It's time to converge security and operations.

Contents

The chances are that your IT security budget has increased in the past year. Average spend has increased 60% globally, according to a recent report.[1] With the increase in hybrid working, CIOs and CISOs have re-evaluated security policies and are looking to bolster endpoint security.

It's turned out to be a bigger project than expected. In one recent survey, 82% of CISOs said that they were overhauling endpoint security, but were faced with endpoints that were either unprotected, or were overloaded with conflicting software agents. As many as one in five endpoints were discovered to be vulnerable to attack.

Organisations are experiencing more attacks than ever before. Cybersecurity Ventures expects a ransomware attack on a business to occur every 11 seconds by the end of 2022. All the while, businesses experienced a 50% increase in weekly cyberattacks in 2021.

Cybercriminals are also becoming more targeted in their attacks. Microsoft's recent 'Digital Defence Report' stated that threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot, and which threaten even the most seasoned IT security teams. Nation-state actors are now engaging in reconnaissance techniques to increase the chances of compromising high-value targets. Criminal groups have moved infrastructure to the cloud, where they can hide among legitimate cloud services. And attackers have developed new ways to scan the internet for systems vulnerable to ransomware.

This massive growth in the number and complexity of attacks, combined with a global shortage of IT security professionals, is a big problem for businesses. In the UK, the cybersecurity workforce shrank[2] by 65,000 last year, leaving a shortage of 33,000 people. Two-fifths (39%) of businesses reported experiencing cyberattacks or data breaches in 2021, according to the government.[3]

Something needs to change

Tanium believes there is a fundamental problem in how most organisations approach IT security management. As the number of IT security threats increases exponentially, companies often respond by buying another point solution. In the past year, 90% of organisations have bought at least one new IT security point solution. Almost half (45%) have bought at least four new products, according to The Foundry 'Security Priorities Study.'

> **A typical enterprise now has 43 separate IT security and security management tools in its infrastructure.**

This approach simply isn't sustainable. When businesses add more tools to their infrastructure, they don't necessarily increase protection, because the pace with which new threats emerge is faster than most organisations can keep up with. This is especially true in today's highly distributed organisations. There's also some evidence that the effectiveness of some point solutions is falling; according to one recent report in the New York Times, the first detection rates of some antivirus tools has fallen below five percent.

Then there's the issue of keeping up with a proliferation of point solutions, each with its own data, interface and owner. Perhaps one tool is managed by IT operations and reports into one data silo daily, but another is managed by compliance and reports quarterly into another data silo. If that scenario is repeated 40 times, CIOs and CISOs face a monumental data headache.

This patchwork approach cannot provide complete protection, and it can be actively harmful to corporate security efforts. If an organisation has multiple security tools sitting in multiple silos, CIOs can't get a clear overview of how many endpoints there are, much less how effectively they are protected, and what changes need to be made.

In many ways, security is a big data problem. When an organisation is running dozens of systems, and dozens of IT security solutions, each generating huge volumes of data at different rates, how is that data being integrated and understood? Simply put, companies can't protect what they can't see.

Today's security decision-makers need help. They need a platform that helps them to keep up with a proliferation of endpoints, and to understand exactly how each one is performing, the threats posed to it, and how it can be protected. This information needs to be available in one place, and in real-time. Only then can CIOs create a single view of security that is needed to deliver effective protection and create a strategy that prioritises the right things at the right time.

What's needed is a converged solution.

Just how bad are things?

Tanium spoke with hundreds of IT security decision makers, who said they want a way to reduce and simplify IT security management.

Key challenges they face include siloed teams – especially in IT operations and security – which aren't able to share security data quickly or effectively. Despite this, many business leaders feel a false sense of confidence about their protection. Second, poor visibility of security data leaves networks vulnerable to attack.

> **Some 64% of businesses expect to experience a cyberattack in the next 12 months.**

Third, businesses are concerned that cyberattacks can impact brand reputation and lead to heavy non-compliance fines.

This lack of visibility and convergence puts companies at risk of financial losses, downtime, damaged brand reputation and potential heavy fines for non-compliance. This is a huge concern given that 20.4% of vulnerabilities that are discovered within businesses are classed as high or critical risk. It also takes an average of 61.4 days to remediate a critical risk, according to Edgescan. And an average of 247 days to identify and contain a breach.[4] That is a huge security risk to organisations.

IT security management must be a higher priority for business leaders. In a recent Harvard Business Review survey, 70% said they thought that leadership should be more concerned about cybersecurity.

A new approach to IT security management

It's crystal clear that businesses need a new approach to endpoint management that helps us to keep pace with tomorrow's threats.

> "Today's CIOs and CISOs are relying on a patchwork of point solutions deployed across IT operations, security, risk and compliance groups."
>
> Steve Daheb, CMO, Tanium

CIOs and CISOs are forced to buy tens of these different solutions, stitch them together themselves and make decisions based on data that is stale, inaccurate and potentially incompatible.

The reason why so many enterprises fall victim to ransomware attacks is that the tools they use are no match for the sophistication of attackers: tools are slow, unreliable and lack a common dataset to operate from. And they inherently create silos.

This approach to security isn't working. It's time to unite tools and data with a unified solution: **Converged Endpoint Management (XEM).**

Introducing Converged Endpoint Management (XEM)

Introducing Converged Endpoint Management (XEM)

Tanium takes a unified approach to IT security management. Its platform unifies multiple endpoint tools and data so that organisations can have visibility and real-time data on all endpoints, through a single interface.

> **"Unlike traditional, fragmented approaches to endpoint management, XEM maximises visibility, control and trust, and allows teams to interact with all endpoints in seconds, regardless of the scale and complexity of the IT environment," says Daheb.**

XEM provides accurate, real-time data to support end-to-end automation, so information security teams can align their efforts and protect their organisations against attacks more effectively. With a unified approach, there's no need for staff from IT operations, compliance, security and numerous other siloes to spend hours collating and sharing data. It can be viewed in a single interface, meaning IT security teams can do more with less resources.

Legacy management systems are often at the heart of problems for organisations looking to improve visibility and efficiency. Moving to a converged platform gives back countless hours of management time, allowing companies to allocate headcount elsewhere and address dangerous vulnerabilities more quickly and effectively across the whole organisation.

The case for better data

IT leaders can't make effective decisions about security without the right visibility – and that means the right data. XEM provides real-time information from every single endpoint, so that critical information isn't locked in siloes, accessed by different teams using different tools.

By converging tools into a single interface, companies can focus on actually delivering effective security. With XEM, organisations can easily see, assess and manage all their IT security data in a single view. Data can be shared, allowing for more effective collaboration and easier, more cost-effective management. Ultimately, a converged approach provides reliable, timely insight that can be used to drive better, faster decision-making. That's essential in today's fast-moving threat landscape.

Providing effective governance

IT governance is a top priority for many CIOs, but when it comes to security, it can be almost impossible to achieve. Organisations have multiple teams with responsibility for IT security, including compliance, governance, IT operations, security and risk. These teams are often working in isolation from each other, so there's no visibility of organisation-wide threats.

Without collaboration or visibility about organisation-wide risks, enterprises can develop blind spots, making both security and compliance a challenge. If you don't have visibility into all your endpoints, it's near impossible to enforce access policies and maintain control across your IT infrastructure.

The good news is that fixing these blind spots doesn't need to be a complex, time-consuming process. XEM provides a relatively quick solution that increases efficiency and effectiveness by reducing unnecessary complexity and improving visibility of IT assets.

> **"Tanium's platform approach means that everything you need – from risk and compliance to data monitoring and more – is accomplished in a single solution," Daheb adds.**

Tanium can identify where all your data is in a matter of seconds, meaning that you can deploy security tools across all endpoints, with a single control plan and common data set and taxonomy.

Making a difference

Tanium's XEM offering is the only solution that allows teams to collectively perform details and complete discovery, in-depth assessments, enterprise prioritisation, cross-platform remediation, and continuous vigilance everywhere.

XEM allows organisations to deliver convergence of IT operations and security, as well as the security infrastructures that are based on point solutions. Its platform aims to change the market and meet the twin challenges of spiralling cybersecurity threats and the rising complexity of IT security management.

Without XEM, the industry will inevitably see more breaches, more hackers, more data leaks and more problems. It's time to make a change.

See Tanium in action:

Learn more about the **benefits of XEM.**

Contact us to **schedule a demo** and see it in action.

References:

1. https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054 - Hiscox Cyber Readiness Report 2022-EN_0.pdf
2. https://www.isc2.org/Research/Workforce-Study
3. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
4. https://www.ibm.com/downloads/cas/OJDVQGRY