TANIUM

WHITEPAPER

Redefining Vulnerability Management

Transforming Legacy Approaches for Modern Cyber Resilience

CONTENTS

Introduction

Enterprise cybersecurity teams have been relying on legacy vendors, processes, and tools for too long. There has been an over-reliance on data for data's sake, with little focus on the solutions required to change the data at hand to deliver better outcomes. Businesses are being challenged by increasingly complex IT environments and hamstrung by outdated approaches to patching. For many organisations, operating with excessively high numbers of outstanding vulnerabilities has become the norm.

> **More than three-quarters (78%) of CISOs say that automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions. However, just 2% of organisations have real-time visibility into runtime vulnerabilities in containerised production environments.**

2022 Dynatrace survey of Australian CIOs[1]

As a result, businesses are throwing resources at vulnerabilities that pose immediate threats, with little capacity available to take a step back and look at the bigger picture. The cost of vulnerabilities has never been higher, the pressure from regulators has never been stronger, and customers have never been more demanding when it comes to data security and privacy.

Many businesses are struggling to keep up with the 1,500 or more newly identified vulnerabilities a month, but it does not need to be this way.

Businesses can remain competitive while delivering modern customer experiences by switching the focus from simply reporting the number of vulnerabilities to actually resolving said vulnerabilities, ensuring long-term business resilience.

Organisations need to stop patting themselves on the back for bringing vulnerabilities down by a certain percentage and transform the way they operate to ensure there are automated and reliable mechanisms in place to keep the organisation consistently protected and match fit in the face of threats.

The following whitepaper aims to outline the gold standard of endpoint vulnerability management and how traditional business models can be successfully flipped to deliver tangible business outcomes while building business resilience.

Change is overdue

Knowing the volume of risks to your business is not enough

Cybercrime is costing businesses billions of dollars each year, as well as customer loyalty, brand reputation, and operational productivity. Across ASEAN, cyberattacks, disinformation, and misinformation have been rising at such an alarming rate that last year saw the ten member states of the Association of Southeast Asian Nations open a new information-sharing and research centre specifically designed to respond to cyber threats.[2] In Singapore alone, the number of phishing attempts increased by 174% from 2021 to 2022, while in Australia, a cybercrime is reported every six minutes,[3] according to the Australian Signals Directorate (ASD) Cyber Threat Report 2022-2023.

> 70% of security professionals say their vulnerability management program is only somewhat effective,

Legacy approaches to tackling security, risks, and threats have led organisations down a path of focusing on vulnerability identification – e.g., investing time and resources into understanding where weaknesses or risks are within an organisation that cybercriminals could use to attack or access information. However, in today's era of 24/7 threats and increasingly well-funded international crime syndicates, merely identifying vulnerabilities is not enough to protect an organisation.

Organisations need to go much further to accurately understand the weaknesses and risks across all devices, how they are evolving over time, and how they can be resolved. This information should then form insights that drive immediate actions to ensure the organisation mitigates the threats of today and tomorrow. Furthermore, they need to carry out this assessment and action plan continuously to keep up with the relentless pace of bad actors.

Concerningly, while Tanium research shows 93% of security professionals say vulnerability management is "very important" or "critical,"[4] 70% of security professionals say their vulnerability management program is only somewhat effective, or worse. In Australia, part of the problem is a lack of resourcing, with 65% of cybersecurity teams feeling understaffed,[5] and 61% of cybersecurity budgets being underfunded.

Without adequate resources or tools, organisations are unable to remediate at scale. Instead, they focus only on exploitable or critical vulnerabilities, which can leave thousands of potential exploits open to attackers.

Real time data and automation can transform vulnerability management outcomes

With the mainstreaming of working from home and hybrid workforces, the volume of devices connected to a business's digital environment has grown exponentially. Tanium research found that up to 20% of endpoints are unknown in 94% of organisations,[6] leaving a significant portion of endpoints missing from the auditing process. As data is now the key target for hackers, identifying all endpoints an organisation's data is stored on must be a business priority.

Furthermore, the growing number of business endpoints is creating a larger threat landscape. Ongoing issues with human error and poor security hygiene become increasingly challenging when managing larger numbers of endpoints and employees with limited cybersecurity skill sets.

A purely people-powered approach cannot address every vulnerability within a business on a regular and daily basis. Consequently, many organisations settle for scanning only a fraction of their environment — predominantly servers — rather than workstations or devices, where the most risk lies.

Time is of the essence

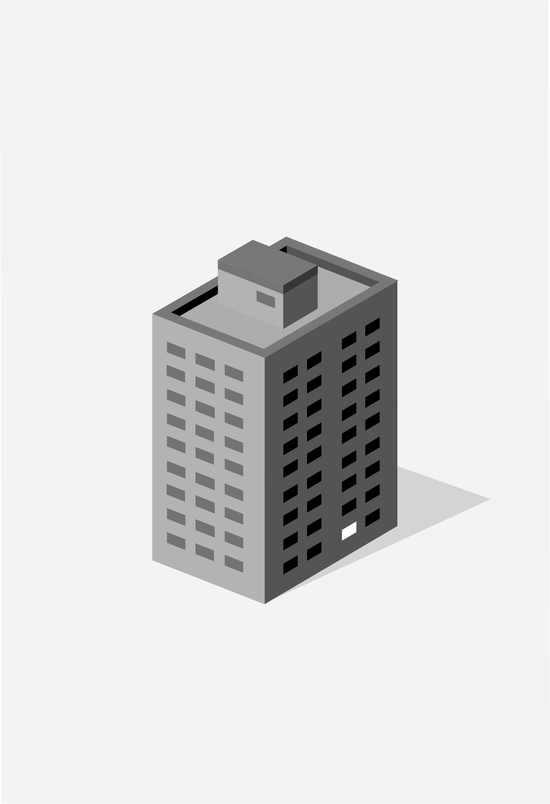
This is where real-time data coupled with automated workflows can play an important role. While traditional vulnerability management solutions overly focus on just identification, organisations are left to fend for themselves to manually remediate without resources, support, or resolutions for the vulnerabilities that are identified.

What's the point in knowing your danger points without having an effective way to fix them?

If you see your business with vulnerabilities being like a house with windows, enterprises these days can have hundreds of thousands of windows, and they need to check that each window is closed and locked every day. For an attacker, just one window needs to be unlocked for them to get in. The resources required to keep track of every window and its status far outweigh the effort involved in finding and climbing through one window.

The longer a window is open, the easier it is for someone to exploit it.

This thinking is demonstrated in data. In 2023, the average cost of a data breach was $4.45 million,[7] the highest ever reported. Organisations that were slow to react paid the price, with breach cycles longer than 200 days costing 23% more than breaches resolved within 200 days. In Australia, the first quarter of 2024 saw 1.8 million Australian account details leaked,[8] a colossal 388% increase on the previous quarter.



Organisations are overdue for a change in how they rely on vulnerability-related data. For too long, executives have been told they have a certain number of risks with almost no way to remediate them all, and everyone simply moves on. The consequences are too serious, and this cannot continue. Organisations should be aiming for automated proactive remediation and eventual elimination.

Reactive vs. proactive vulnerability management

The urgency to patch major vulnerabilities has been called out by the federal government on various occasions.[9] Meanwhile, according to the Australian Signals Directorate (ASD)'s annual cyber threat report for 2022-2023, half of vulnerabilities were exploited within two weeks of a patch or of mitigation advice being released.[10] Despite this known and ever-present threat, organisations continue to live with excessively high vulnerability counts and continue to be compromised.

So how did we get here?

Due to the increasing size, complexity, and diversity of computing environments in the modern world, approaches to managing those environments that worked decades ago no longer produce the desired outcomes today. The deficiencies have forced organisations to compensate and promote what should be a secondary line of defence, vulnerability scanning, as the pivotal component in ensuring that necessary patches are installed. Let's explore this further by breaking down and understanding some of the main areas of concern.

Asset coverage: Without a thorough asset discovery process, organisations have an incomplete view of what assets exist across all the endpoints in their IT environment on their network. This results in incomplete and/or out-of-date CMDBs and no true system of record. In addition, a lack of self-discovery within patching and vulnerability tools creates skewed reporting for endpoints that may not be able to communicate with the tool but are alive and exposed on the network.

Data currency: Legacy tooling relies on legacy architectures like hub-and-spoke communication to endpoints. Using this approach is slow and requires additional tiered infrastructure to scale. The result is a weeks-old view of the state of the network due to lengthy data retrieval cycles and unnecessary technical overhead.

Domain dependencies: Traditional patching tools typically provide support for endpoints located on the core network and connected to organisation domains. Modern networks have significant numbers of endpoints that do not adhere to that antiquated notion.

Configuration complexities: Large, multi-domain organisations with business demands and constraints across many teams can create challenging processes for patch deployment. Legacy tooling that requires onerous configuration and administrative overhead to adequately cater to those requirements consumes time and exposes gaps.

Operations teams attempting to deploy all new patches released each month and striving to ensure all applications in use are updated to the latest versions have, over time, been slowly drowning in the challenges above. The result is that vulnerability counts have been steadily increasing, as has the reliance on vulnerability scanning to gain some semblance of network state visibility.

Enter vulnerability management

As the importance of resolving vulnerabilities has heightened and the number of vulnerabilities within organisations continues to rise, the practice of vulnerability management has evolved into a critical industry need. It has become the linchpin of many organisations' patching regimes, compensating for the challenges faced by patching tools and their operators. The function is typically owned by the security or risk side of the business, as they seek to understand the risk and protect the organisation from exposure to attack.

The more vulnerabilities an organisation has, the greater the need for a best-in-class vulnerability management solution becomes, with selection criteria centred around the types of devices that may be scanned and the ability to report in various ways on vast numbers of vulnerabilities. The scope of these tools, however, does not extend to resolving the vulnerabilities, which, of course, is the ultimate objective.

The remediation of vulnerabilities typically remains the responsibility of the operations team, with a cyclic process formed as follows:

1. Security team produces a list of vulnerabilities that need to be resolved and provides it to the operations team

2. Operations team attempts to reconcile the list within its patching tool

3. Operations team attempts to install the patches and hopes they are successful

4. By this time, the security team has produced another list to send, and on it goes

The above cycle defines a "reactive" vulnerability management process. The patching process can never keep up, and the organisation remains in a state of permanent vulnerability stress. It is akin to a dog chasing its own tail, never quite catching it, and becoming frustrated and exhausted over the effort expended attempting to do so.

To compound the matter, the operations and security teams are using tools sourced from separate vendors and rely on their own source of asset data. This disconnection leads to misalignment, contention, and considerable reverse workflow.

What's the alternative?

This reactive cycle that has evolved its way into organisations cannot be broken until the constraints and challenges that have caused it are addressed. That is, by leveraging a tool that can build a complete, real-time view of network state (including patch status), regardless of where endpoints are located. That tool must also be able to simplify the very process of patch deployment itself with simplified workflows and configuration.

At this point, the patching process can start to drive itself rather than be dependent on lists provided by a vulnerability management tool. The goal is to patch endpoints as they require it and address vulnerabilities before they even register in a vulnerability management tool in a proactive manner.

Getting to the gold standard of vulnerability management and reducing your risk

Getting the basics right — good cyber hygiene starts with visibility

There are two key requirements for effective visibility within the environment:

1. Get all assets under management: Presently, most organisations are unable to accurately answer this simple question: "How many assets do you have at this exact point in time?" This problem is exacerbated as the number of assets and endpoints within an organisation grows. Understanding what assets are across all your endpoints and ensuring they are being managed is the first and most fundamental step in building effective management of the estate.

2. Gain real-time visibility of managed assets: Waiting days and weeks for a data retrieval cycle to complete is totally inadequate for managing and securing a network in today's world. A real-time view of the IT estate is essential to understand and standardise all software versions and their underlying components, configuration settings, applied policies, and the state/health of an endpoint. Good hygiene at this level equates to minimised attack surface and sets a strong foundation to build patching processes upon.

Patching has been reactive for too long — it's time to flip the cycle

The reactive patching cycle has become so normalised and ingrained over time that many IT organisations now structure themselves and measure operator performance based on how many vulnerabilities have been found and subsequently resolved by patching. Modernising this approach by utilising a patching tool that can identify and install patches as the endpoint requires them requires a mindset change within IT. New vulnerabilities will be resolved before they even make it to a vulnerability scanner, and the backlog of old vulnerabilities can be tackled and wiped clean.

A better approach to measuring efficacy may be to keeping track of how many patches have been installed, whether they were successfully installed or not, and how long it took from awareness of the patch to resolution. There will still be vulnerabilities to measured, but the quantity will be vastly different.

The steps to address vulnerability management and associated patching in a proactive manner are outlined in the following sections.

The gold standard:

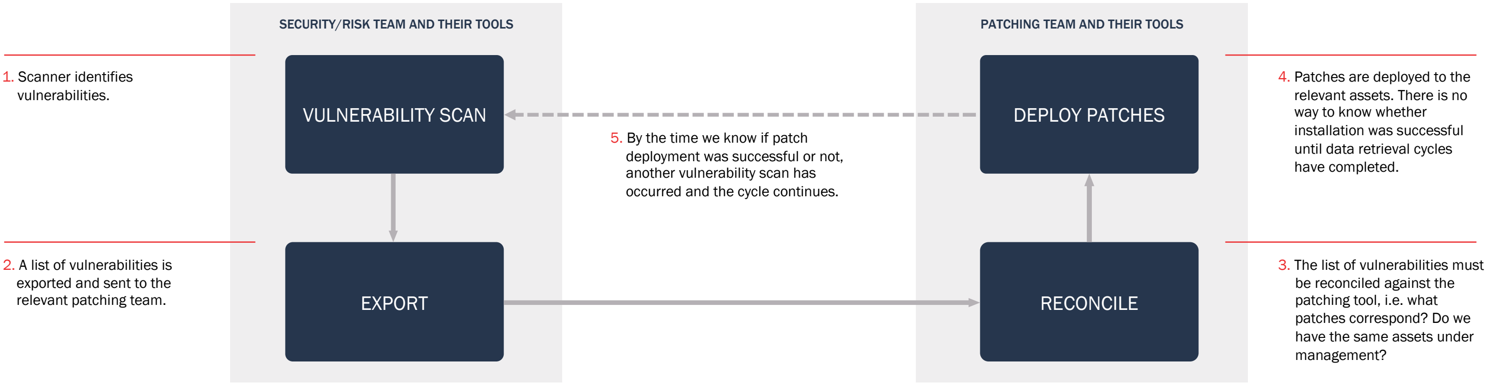
1. Ensure all assets have been discovered and are under management. This also means ensuring that the patching tool can communicate with the relevant services on all managed endpoints. **We now have complete coverage.**

2. The patching tool scans endpoints and identifies any required patches or software updates within an hour of them being published. **We now have the current status.**

3. Patch deployments can be built into reusable deployment configurations. These deployments contain a set of predefined patches or software titles and are targeted to a predefined set of endpoints. The deployments can be left running continuously, with the patches and software titles updating as they are released. Deployments can be broken into rings of endpoints to ensure a phased approach is leveraged for patching. **We now have a simplified deployment approach.**
4. Ensure that the results of patching are available immediately after the deployment has run, indicating success or failure. Causes of any failures should be stated to allow investigation and resolution of any failures (e.g., endpoint hard disk full, etc.). This will **lift patch compliance towards 100%.**
5. Report on patch compliance across all endpoints with current and accurate data.

Adopting an approach like the above will result in those vulnerabilities that have corresponding patches being addressed before a vulnerability scanner sets eyes on them. The patching process can drive patching, and vulnerability scanning can become the secondary layer it should be.

The Reactive Patching Cycle


SECURITY/RISK TEAM AND THEIR TOOLS
VULNERABILITY SCAN
EXPORT
PATCHING TEAM AND THEIR TOOLS
DEPLOY PATCHES
RECONCILE

1. Scanner identifies vulnerabilities.

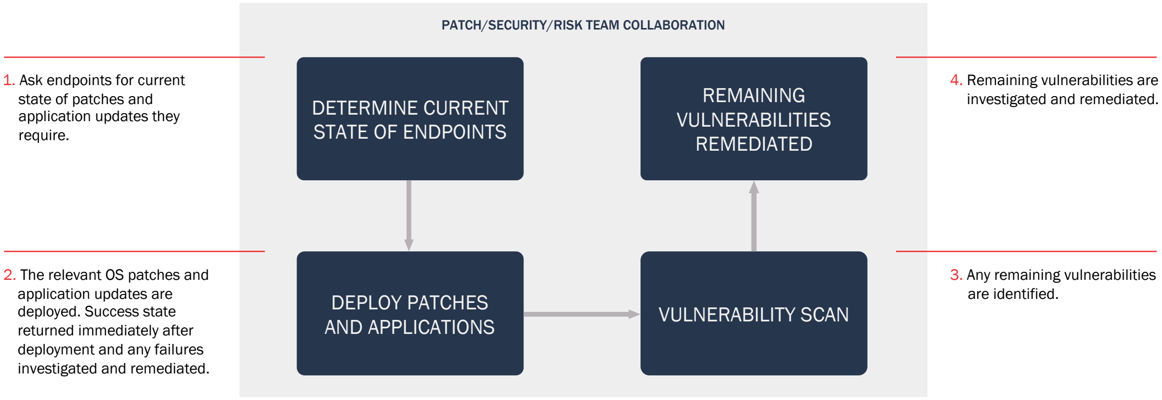
2. A list of vulnerabilities is exported and sent to the relevant patching team.

3. The list of vulnerabilities must be reconciled against the patching tool, i.e. what patches correspond? Do we have the same assets under management?

4. Patches are deployed to the relevant assets. There is no way to know whether installation was successful until data retrieval cycles have completed.

5. By the time we know if patch deployment was successful or not, another vulnerability scan has occurred and the cycle continues.

The Proactive Patching Cycle


PATCH/SECURITY/RISK TEAM COLLABORATION
DETERMINE CURRENT STATE OF ENDPOINTS
DEPLOY PATCHES AND APPLICATIONS
VULNERABILITY SCAN
REMAINING VULNERABILITIES REMEDIATED

1. Ask endpoints for current state of patches and application updates they require.

2. The relevant OS patches and application updates are deployed. Success state returned immediately after deployment and any failures investigated and remediated.

3. Any remaining vulnerabilities are identified.

4. Remaining vulnerabilities are investigated and remediated.

Vulnerability management as it should be

At this point, we have dealt with many vulnerabilities within the patching process and removed a great deal of emphasis on the vulnerability management solution. However, these solutions are still required to identify any vulnerabilities that may not have a corresponding patch (e.g., related to a configuration or policy setting) or those that do not yet have a vendor patch available.

Ideally, the vulnerability scanning leveraged for managed assets should be agent-based rather than network-based. The reasons are as follows:

- The network load can be minimised
- Less load allows more frequent scanning
- To avoid offline endpoints missing the scan windows, scheduling can be based on the endpoint's knowledge of the time since it was last scanned rather than a time-based cycle

The remaining vulnerabilities to note are zero-day threats. These are the threats that have been identified and published that do not yet have a vendor patch available or a vulnerability definition. Again, real-time visibility into the estate will provide the opportunity to quickly scope exposure to these types of threats, and the ability to perform actions and remediate across the estate will allow published mitigation steps to be accomplished.

Levelling up to automation and autonomous endpoint management

Only when strong endpoint management foundations have been built by ensuring all assets are known and managed, the asset data being leveraged is current and contextual, configuration and management flows are simplified and efficient, and teams and tool capabilities are sharing the same data plane can the benefits of employing automation be considered.

Automating incomplete and inefficient processes will only amplify the issues. It's like trying to fix a bug in code that causes excessive CPU consumption by adding more CPU. It will allow the code to run faster, which simply consumes even more CPU. When the patching and vulnerability management processes become refined, well-understood, and effective, steps may be taken to automate parts of the process and to remove those manual checkpoints.

Beyond automation, autonomous endpoint management (AEM) seeks to build further by leveraging AI in various ways to remove areas of manual effort within endpoint management where applicable while the operator maintains control over the process.

For example, a complex patching scenario may require orchestration of patch deployments across various servers in a particular order, with various activities required on the endpoints prior to and after patch installation. The intent of autonomous endpoint management may be to automatically build the orchestration playbook with all the steps in place, offer it for approval or modification, and allow it to be run.

Another example may be asking for the top ten issues an operator should focus on to secure the network, then offering solutions and fixing them.

Clearly, to take full advantage of future capabilities like autonomous endpoint management, real-time visibility of *all* assets on all endpoints and having the foundational management capabilities in place is essential.

Conclusion

In an era where cyber threats are evolving with alarming velocity, the traditional approaches to vulnerability management are proving inadequate. In this paper, we've underscored the urgent need for a paradigm shift from reactive, identification-focused strategies to proactive, resolution-driven vulnerability management. The legacy systems, with their fragmented and outdated methodologies, have left organisations grappling with an overwhelming number of vulnerabilities, exposing them to cyber risks that can have dire financial and reputational consequences.

The solution lies in embracing a future-ready approach to vulnerability management, one that leverages real-time data, automation, and comprehensive asset coverage to transform outcomes. By adopting Tanium's cutting-edge platform, organisations can gain the visibility and control needed to manage their digital environments effectively. Tanium's solution offers a unified, real-time view of all endpoints, enabling swift identification and resolution of vulnerabilities. This proactive stance not only enhances security but also streamlines operations, reduces costs, and fortifies business resilience.

Tanium embodies the gold standard of vulnerability management, which is characterised by automated, proactive remediation, and the elimination of vulnerabilities before they can be exploited. With Tanium, organisations can transcend the limitations of legacy IT, ensuring that every "window" in their digital "house" is securely "closed and locked" against cyber threats.

The transition to Tanium's future-ready vulnerability management is not just a strategic move; it's imperative for survival in the digital age. Organisations that choose to partner with Tanium are not only securing their present but are also paving the way for a more secure, efficient, and resilient future. The time for change is now, and Tanium stands ready to lead the charge toward a new era of vulnerability management excellence.

> Let us demonstrate how Tanium XEM can help you adopt a gold standard of vulnerability management: Book a demo now

References

1 https://www.securitysolutionsmedia.com/2022/06/02/research-reveals-76-of-australian-cisos-are-worried-too-many-application-vulnerabilities-leak-into-production-despite-a-multi-layered-security-approach/

2 https://www.japantimes.co.jp/news/2023/07/18/asia-pacific/asean-cyberattacks-operations-center/

3 https://www.smh.com.au/business/the-economy/australia-s-digital-economy-needs-strong-cybersecurity-to-thrive-20231213-p5er5s.html

4 https://www.tanium.com/blog/tanium-security-operations-for-servicenow-cybersecurity-solution/

5 https://australiancybersecuritymagazine.com.au/65-of-cybersecurity-teams-understaffed/

6 https://www.tanium.com/blog/why-you-need-converged-endpoint-management-xem/

7 https://www.cyberdaily.au/security/10165-report-average-cost-of-data-breaches-rises-to-us-4-5-million

8 https://www.cyberdaily.au/security/10472-australia-records-388-per-cent-quarter-on-quarter-jump-in-compromised-accounts

9 https://www.afr.com/technology/fix-software-bugs-now-urgent-appeal-to-business-20231027-p5efnf

10 https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023