TANIUM

WHITEPAPER

Redefining Cyber Resilience Through Proactive Vulnerability Reduction

CONTENTS

Executive Summary

In today's rapidly evolving threat landscape, traditional vulnerability management approaches are no longer sufficient. Legacy tools and reactive processes have left enterprises overwhelmed by an ever-growing backlog of vulnerabilities, fragmented visibility, and ineffective remediation cycles. The result? Increased exposure to cyber threats, regulatory pressure, and operational inefficiencies.

This white paper presents a compelling case for a paradigm shift—from reactive vulnerability "management" to proactive vulnerability *"reduction".* It outlines how organisations can move beyond identifying risks to systematically eliminating them through real-time visibility, automation, and unified endpoint control.

Key insights for IT and security leaders

- **The problem with the status quo:** Most organisations rely on outdated, siloed tools that focus on identifying vulnerabilities rather than resolving them. This leads to inefficiencies, misalignment between security and operations teams, and persistent risk exposure.
- **The cost of inaction:** With over 1,500 new vulnerabilities emerging monthly and 50% exploited within two weeks, the reactive model is unsustainable. Cybercrime is costing Australian businesses billions annually, with a breach reported every six minutes.
- **The case for change:** The paper introduces a gold standard for vulnerability reduction built on:
  - Comprehensive asset discovery and real-time endpoint visibility
  - Autonomous Endpoint Management (AEM) to automate patching, policy enforcement, and application updates
  - Confidence scoring and deployment rings to ensure safe, phased rollouts
  - Proactive remediation that neutralises vulnerabilities before they're even detected by scanners
- **Strategic outcomes:**
  - Reduced attack surface and operational risk
  - Streamlined IT operations and reduced manual effort
  - Enhanced compliance posture and audit readiness
  - Improved collaboration between security and IT operations

Proactive Vulnerability "Reduction" vs Reactive Vulnerability "Management"

The urgency to patch major vulnerabilities has been called out by the federal government on various occasions.[1] Meanwhile, according to the Australian Signals Directorate (ASD)'s annual cyber threat report for 2022-2023, 50% of vulnerabilities were exploited within two weeks of a patch or of mitigation advice being released.[2] Despite this known and ever-present threat, organisations continue to live with excessively high vulnerability counts and continue to be compromised. But why?

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, applications updated, and that the environment is configured and secured appropriately. 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, vulnerability and other management 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 and endpoint management tools typically provide support only 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, application and policy deployment. Legacy tooling that requires onerous configuration and administrative overhead to adequately cater to those requirements consumes time and exposes gaps.

Automation immaturity: A lack of guardrails and oversight within traditional endpoint management tooling inhibit the ability to automate patch and update activities. The risk to the business is often deemed too high and consequently those activities remain resource intensive.

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.

1 https://www.afr.com/technology/fix-software-bugs-now-urgent-appeal-to-business-20231027-p5efnf
2 https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

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 endpoint management 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 own tools (patching, software distribution, policy enforcement)
3. Operations team attempts to install the relevant patches or updates 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 and update processes 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.

The result

We have now identified the two primary sides to the vulnerability challenge:

1. endpoint management tooling that is unable to adequately drive its own function in a complete and timely manner, resulting in outstanding patches, outdated applications, and insecure policy on the network.
2. a dependency on vulnerability management tools that are built to identify and report on as many vulnerabilities as possible, which are used to feed the above endpoint management tools.

So, what's the problem? Well, there are several:

- the legacy endpoint management tools in question are still deficient and despite the tasks they need to perform being explicitly driven by the results of vulnerability scanning, they are unable to complete those tasks effectively.
- there are simply too many vulnerabilities to address – note that each patch or software release may remediate dozens of vulnerabilities, which when multiplied out by the number of affected endpoints often translates into incredibly large numbers and overwhelms organisational processes and resources.
- the lack of alignment between tools and teams slows and frustrates the process even further.
- the reactive cycle of scan for vulnerabilities first, remediate second, ensures that vulnerabilities remain on the network while the process plays itself out, creating significant risk for the organisation.

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, application and policy/configuration status), regardless of where endpoints are located. That tool must also be able to simplify the process of deploying updates into the environment itself with simplified workflows and configuration.

At this point, patching and update processes can start to drive themselves rather than be dependent on lists provided by a vulnerability management tool. The goal is to patch and update endpoints as they require it and address vulnerabilities before they even register in a vulnerability management tool in a proactive manner. So rather than "manage" vulnerabilities, we can start to "reduce" them.

Foundations to achieving the gold standard of vulnerability reduction

1. Get 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 IT 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.

2. Maximise efficacy and efficiency with confidence—automate with autonomous endpoint management (AEM)

One of the major impediments to speeding up the deployment of patches and application updates is the increased risk this poses to the business. Rounds of testing must be completed to identify any problematic software so it can be blocked from broader production deployment. There are other considerations such as complex server farms and database clusters for example, whereby logic must be applied to the order of deployment and certain criteria met for the process to continue.

To overcome these challenges while speeding up the process and increasing efficiency, a range of automation and autonomous endpoint management features must be implemented. Note that to achieve effective automation, real-time visibility of the environment is essential to inform and control the process.

Deployment Rings

The ability to split the network into discreet parts for phased deployments is critical to limit the blast radius when making changes to a production environment. Deployment rings allow predefined network separation to be leveraged quickly and seamlessly when introducing automation into the process. The progression through rings should abide by associated success criteria to ensure problematic updates are identified and contained.

Automation playbooks

To accomplish automated deployment of complex and/or multi-step patch and application deployment plus other updates require sophisticated orchestration capabilities. Defining the required steps, their order, and the rules and/or criteria for progression should be predefined and saved as playbooks to allow for repeated use. The goal is to hide the complexity and provide a simple picklist of automation packages for use. Deployment rings should be leveraged when running these playbooks to accomplish phased, controlled and automated deployment.

Confidence scoring

A key component of autonomous endpoint management, confidence scoring, leverages the experience of prior patch and software deployments from within the given network and any other organisation that has attempted deployment of the specific patches and applications. The success or failure status of those updates, plus any subsequent impacts to endpoints after deployments have completed, are analysed to inform subsequent installation. A confidence score is applied to the relevant items which can be incorporated into the criteria for automation and ring progression. This allows full automation of updates that are highly likely to succeed, while problematic updates can be held back for further investigation and testing within the environment.

3. Move from reactive to proactive patching

The reactive patching and application update 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. Modernising this approach by utilising an endpoint management tool that can identify outstanding patches, out of date applications and insecure policy, and then deploy the relevant updates 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 keep 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. Or the number of out-of-date applications installed within the environment and the time elapsed since a new version was released. There will still be vulnerabilities to be measured, but the quantity will be vastly reduced.

It's time to flip the cycle and implement a gold standard proactive vulnerability reduction approach.

Implementing the vulnerability reduction gold standard

Discover

Ensure all assets have been discovered and are under management. This also means ensuring that the endpoint management tool can communicate with the relevant services on all managed endpoints. This needs to include a self-monitoring component to ensure management integrity rather than simply assuming an endpoint is offline because the relevant services have become unreachable. This will ensure complete and ongoing management coverage of estate.

Automate

The first step is to ensure that security policy has been defined appropriately and then enforced on each endpoint in an automated and continual manner. A centralised deployment of policy without current state confirmation the policy settings have taken effect at each endpoint is insufficient. In other words, without explicit testing and confirmation that that the relevant registry settings have been applied on every endpoint will likely result in a reliance on vulnerability scanning to identify where those settings have not taken effect.

The second and very significant component of establishing automated vulnerability reduction is patching. This includes operating system patching and application patching in the form of version updates. Autonomous endpoint management features should be leveraged to ensure a current state of the environment is understood, and then those patches and applications that are deemed safe to deploy by virtue of their confidence score should be deployed automatically via deployment rings. This will remove a significant load and allow only those potentially problematic patches and applications that require more scrutiny to be surfaced and held back for the appropriate testing.

We have now simplified and streamlined deployment while reducing the manual load and risk considerably through controlled and highly informed automation.

Assess & Revise

This is the clean-up step.

- Work through any low confidence scoring patches and applications to determine if they are safe and appropriate to deploy into the environment.
- Investigate any failed deployments that have occurred within the automated deployments and then resolve those issues. For example, there may be insufficient disk space on an endpoint, or the Windows Update feature on Windows endpoints may be corrupted or in a failed state.

This will raise the compliance ceiling towards 100%. Resolving the issues identified in this step will feed into the ongoing automation process and over time increase the efficiency and efficacy of the overall patching regime. This is also the step where vulnerability scanning running as a secondary layer can be leveraged to refine the process and ultimately minimise it's need.

Report

Now that vulnerabilities are being resolved before they are identified by a vulnerability scanner, reporting can focus on those aspects of the environment that constitute the underlying cause of vulnerabilities – that is, does the operating system running on every endpoint have all necessary patches, are all applications up to date (or indeed, need to be installed at all), is policy defined appropriately and applied on every endpoint?

Gold standard functional workflow

Vulnerability management as it should be

At this point, we have dealt with most vulnerabilities with automated processes and removed a great deal of emphasis on vulnerability "management" or scanning/collection. However, this function is still required as a secondary layer to identify any vulnerabilities that may have slipped through the net.

This remaining vulnerability scanning function will be enhanced significantly by leveraging the same management solution that performs remediation as discussed in prior sections of this document, by leveraging complete coverage of endpoints, real-time access to endpoints to understand their state, and the inherent alignment of teams responsible for the identification of vulnerabilities and those that perform the remediation.

It is worth re-emphasising that the ultimate goal we are working toward is removal of vulnerabilities from the environment, not building the best collection of them. Vulnerability "management" solutions that do not focus on and facilitate remediation of the vulnerabilities they identify are at best belying their name, and indeed, arguably only perpetuating an exaggerated reliance on themselves.

Zero Day threats

A notable category of vulnerabilities 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.

Conclusion

In an era where cyber threats are evolving with alarming velocity, the traditional approaches to vulnerability management are proving inadequate. 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.

In this paper, we've underscored the urgent need for a paradigm shift from reactive, identification-focused strategies to proactive, resolution-driven vulnerability reduction.

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 AEM 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, before a vulnerability scanner even sets eyes upon them. This proactive stance not only enhances security but also streamlines operations, reduces costs, and fortifies business resilience.

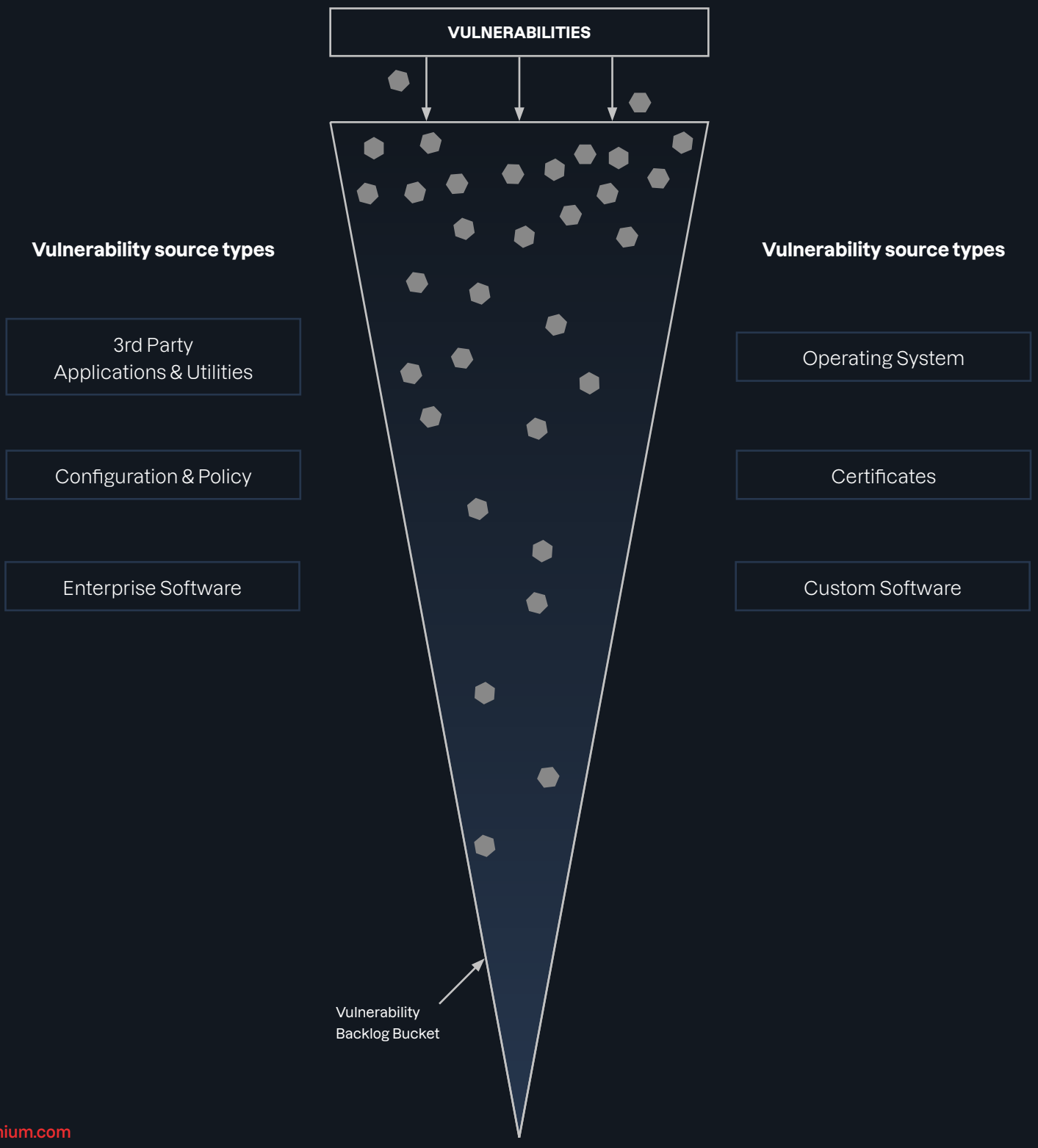
The transition to Tanium's future-ready vulnerability reduction approach is not just a strategic move; it's imperative for survival in the digital age. Organisations that choose to partner with Tanium are not only securing their present but are also paving the way for a more secure, efficient, and resilient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

Let us demonstrate how Tanium AEM can help you adopt a gold standard of vulnerability reduction: **Book a demo now** or visit to www.tanium.com/see-a-demo.

Appendix

Reactive Vulnerability Cycle

Vulnerabilities are continuously generated from various sources and identified via scanning. They can be represented in a triangular backlog or bucket due to some types being more prevalent than others. The volume quickly becomes overwhelming as reactive remediation efforts cannot keep up with the new vulnerabilities. The backlog continues to grow.



Proactive Vulnerability Cycle

Vulnerabilities are continuously generated from various sources. They can be represented in a triangular backlog or bucket due to some types being more prevalent than others. Those at the top of the bucket can be addressed in an automated manner before a vulnerability scanner even identifies them. The remaining backlog is much smaller and more manageable.