ARMIS®

WHITE PAPER

The Intelligence Revolution: Precise and Continuous Vulnerability Detection and Response

Executive Summary

For over two decades, vulnerability detection has relied on a "brute-force" architecture. This model utilizes heavy, disruptive discovery methods, including both network-wide scans and aggressive agents, that interrogate every IP address to identify assets. While this may be sufficient for the static environments of the past, this approach fails to address the complexities of modern cloud, remote work, and diverse OT and IoT ecosystems. Beyond network noise, the operational pain of deploying, configuring, and maintaining these legacy methods, as well as the "agent fatigue" caused by adding yet another permanent footprint to an asset, has created significant friction between IT and Security teams.

Adopting an intelligence-driven philosophy is essential for a modern security strategy. This white paper will explore a way forward for vulnerability detection that cuts through the noise, reduces disruption, and powers greater accuracy than ever. Establishing a foundational truth through continuous, multi-source asset intelligence is key, allowing organizations to replace outdated, reactive methods with strategic precision and irrefutable, evidence-backed intelligence in the face of today's sophisticated, AI-powered threats.

Legacy Detection is No Match for AI-Powered Threats

There is an ever-expanding wave of vulnerabilities and exposures, opening the door to more potential threats. Traditional vulnerability management processes are struggling to keep up. Legacy vulnerability detection or scanning often relies on long, static cycles that span weeks at a time. The result is slow, rigid data that simply does not reflect real-time risk. These security snapshots require a significant network footprint, where discovery and matching logic reside within the scan policy itself, creating an immense maintenance burden.

The typical detection methods consist of the following approach:

- **The Interrogation Model:** To find a vulnerability, the tool must probe an asset or run a local agent to "ask" if it is vulnerable.
- **The Plugin Cycle:** Because detection is tied to the scan, users must constantly update the tool with new plugins and run entirely new scan cycles to detect recently disclosed CVEs.
- **Operational Friction:** This creates a massive footprint of appliances and agents that require constant updates, configurations, and maintenance.

Meanwhile, cybercriminals are increasingly leveraging AI to deploy sophisticated attacks, with attackers increasingly using vulnerability exploits to gain initial access in security breaches, 34% more frequently than even a year ago.

Multi-Layered Technology Stack vs Unified Multi-Layered Detection

Visibility does not always equal situational awareness. For too long, organizations have thrown technology at the vulnerability management challenge, in hopes that a new tool would provide a pathway to resolution to the ever-expanding onslaught of vulnerabilities and costly data breaches. Over the years, this has created a compounding problem with aging technology, coverage gaps, and a "spaghetti architecture" that prevents the very thing these tools were intended to achieve: actual risk reduction.

Legacy security stacks, often comprising over 11 disjointed tools, are reactive, cluttered, and archaic, leaving in their wake vulnerability blind spots that can last weeks or months at a time. When detection is inconsistent, security teams are left ill-equipped and vulnerable, leaving the entire operation at risk. This gap, if left unchecked, will continue to expand into an unmanageable chasm between detection and protection. The industry needs a fundamental shift.

No Margin for Error:

- **20% of all breaches** are now attributed to vulnerability exploits in complex technology environments.
- **34% year-on-year increase** of attackers exploiting vulnerabilities to gain initial access in security breaches.
- **32 days** on average to progress from initial scan to eventual remediation.
- **33%** of organizations report that a tighter connection between security and IT tools would most improve their security program.

Challenges with Traditional Vulnerability Management Methodologies

Beyond the disparate technology solutions fighting for the spotlight and the complex security architectures at play, even when vulnerability detection happens, it is still leaving organizations exposed.

- **Vulnerability Blind Spots:** Periodic scans only provide a snapshot of security, giving attackers days or weeks of a head start, completely missing new vulnerabilities that emerge between scan cycles. This can be the difference between protection and a vulnerable state that can fester for weeks at a time.
- **Operational Friction:** The traditional scanning approach hits thousands of ports and requires authentication, resulting in a noisy, disruptive process with a high network load. This forces reliance on restrictive "scan windows" and scheduled patch days.
- **Inaccurate Risk Assessment:** Traditional methods rely on inferred data and slow, often broad public vulnerability databases. What's more, many devices simply cannot withstand traditional scans. This leads to a flood of false positives with no situational context that burn out security teams, forcing them to manually chase findings that are not actually exploitable in their environment.

A New Paradigm: Unified Vulnerability Management

In order to achieve true protection and risk reduction, organizations must shift the focus from disruptive, broad-range scanning to intelligence-driven continuous assessment that considers the entire vulnerability management lifecycle.

The Lifecycle of a Vulnerability

There is so much more to vulnerability management than just establishing an inventory. To truly tackle the “spaghetti architecture” within security teams, we must consider and bolster defenses for every stage of the vulnerability lifecycle to establish end-to-end exposure management that puts an end to uncertainty, clutter, and wasted technology spend.

- **Detect and Discover**
- **Contextualize**
- **Consolidate**
- **Validate**
- **Prioritize and Remediate**

1. Comprehensive, Low Impact Detection:

The foundation of an intelligence-driven approach to assessment begins with how the initial dataset is established. Instead of relying on multiple tools with conflicting information, what if a single solution could use multiple sources to evaluate the entire asset landscape? Every piece of technology in a modern enterprise has its own unique set of protocols and parameters and requires a bespoke assessment approach. This can happen in multiple ways.

Asset Intelligence	Active Assessment	Continuous Event-Driven Assessment
By listening to network traffic and leveraging existing technology investments and integrations, establish an authoritative asset profile of key characteristics, requirements, behaviors, and inherent risks.	Leveraged as needed, active assessment and Smart Active Queries employ a “discover-then-probe” logic. Rather than a scan of the entire network, hoping to find what you’re looking for, this takes a surgical approach to gather only the required missing information and complete the asset profile.	Instead of waiting for the next scheduled scan, organizations will instead move toward event-driven, automatic reassessment. The moment a change in the environment is detected, like new software being installed or a new device joining the network, the asset is reassessed, risks are considered and compiled, and teams are alerted to any imminent risks. This eliminates the vulnerability blind spots and detection gaps, moving the response time from weeks to minutes.

2. Deep Asset and Situational Context

Effective risk assessment must move beyond static, basic CVE lists and consider the unique context, usage, and real-world risk of every asset. Assets should be understood by more than just their IP address. By unifying multi-source telemetry, organizations can transform raw findings into a prioritized roadmap for risk reduction.

Deep Asset Intelligence	Augment with Vulnerability Intelligence	Evaluate the Business Context
Establish a true source of truth by compiling as much information about a technology asset as possible.	Beyond the individual asset profile, additional information can be obtained by determining whether any active advisories or early warning alerts exist for its unique asset profile and configuration.	Not every asset is viewed in the same way within an organization. Understanding the potential impact of an asset on the operational continuity of the business is essential for targeted prioritization.

3. Consolidate Results and Eliminate Noise

To evolve vulnerability management from the fragmented burden it is today into a strategic function, organizations must move beyond the restrictions of complex, overlapping tools. A mature security posture should bring all findings into a single, unified view. By centralizing data from all sources, technology systems, and third-party systems, teams can eliminate the silos and bottlenecks that prevent effective prioritization and risk reduction.

A best-practice approach both ingests, deduplicates, and contextualizes the results from disparate datasets to ensure that multiple alerts for the same issue do not inflate the perceived threat volume and waste valuable time.

4. Predictive Validation of Vulnerabilities

Safe validation of potential vulnerabilities is an unsung hero of effective vulnerability prioritization. Organizations are looking to minimize their disruption to keep sensitive assets operating safely. Predictive validation uses asset intelligence to verify the exploitability of a vulnerability without the need for risky and intrusive attack simulations.

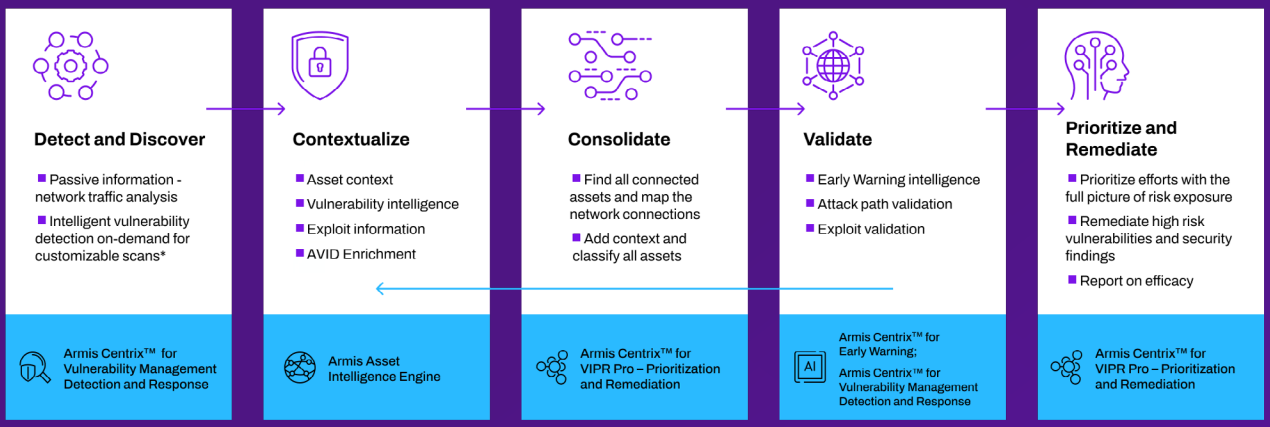
Analyzing the comprehensive asset profile, including its specific configurations, allows security teams to determine if a vulnerability is truly “reachable” and exploitable in its current environment. This intelligence-driven approach allows security teams to confirm the true risk status through precise identification rather than disruptive attack simulations. This ensures that remediation efforts are focused only on verified, high-impact threats without risking the stability of essential operations.

5. Targeted Prioritization and Informed Remediation

Every component of vulnerability management, from dynamic detection and detailed asset intelligence to situational awareness and predictive validation, informs the key step of prioritization and remediation. Risk-based prioritization allows vulnerability management teams to go beyond static scores and long lists of alerts with zero context. Strategic prioritization leaves alert fatigue behind and allows organizations to focus on the real-world threats as they appear, in the order that presents the biggest risk to the overall business.

To effectively reduce risk and strengthen cyber resilience, security leaders must be able to immediately evaluate vulnerabilities and business criticality in a single view. By analyzing real-world threat telemetry, including whether a vulnerability is currently being weaponized or exploited in the wild, organizations can isolate the critical few risks that pose the most immediate danger.

The Lifecycle of a Vulnerability



Case Study: The Power of Continuous vs Periodic Assessment

Not every scan is created equal. A traditional “point in time” scanning model leaves significant space for exposure. In this example, the traditional scanner is operating on a bi-weekly scan. If an administrative change introduces new, vulnerable software on day 1 of this cycle, the organization may be left entirely unaware until the next periodic scan begins 14 days later. This gives attackers a week-long headstart to exploit the new flaw.

It’s time to consider a new approach. If organizations adopted a continuous assessment model, this exposure window is effectively eliminated. The same new software being introduced would immediately begin an updated risk assessment, alerts, and kick off the remediation process to neutralize the potential risk nearly as quickly as it was detected. This real-time awareness allows teams to address new vulnerabilities as they appear and before attackers can exploit them. The power of continuous assessment is clearly demonstrated by transforming vulnerability management from a reactive, two-week exposure period into a proactive, real-time security function.

The Power of Continuous vs Periodic Assessment

Operational and Strategic Advantages

An intelligence-driven architecture delivers benefits that legacy “brute-force” tools cannot match:

- **Eliminating Friction:** Traditional scanners often require a massive footprint of appliances and agents that must be constantly managed, updated, and configured. This ongoing maintenance burden is a primary source of friction between IT and Security teams.
- **Global Maintenance Awareness:** Rich asset context ensures scans execute only within the local, approved window of the specific asset, regardless of the time zone.
- **Reduced Infrastructure Footprint:** A single core collector acts as a multi-protocol sensor. Best practice utilizes the same collector for both passive monitoring and smart active scanning, radically simplifying resource consumption.
- **IT and Security Alignment:** By eliminating disruptive network noise and providing verified findings, the platform removes the operational tension inherent in legacy management.

Conclusion

Vulnerability management must move past the architectures of the past in order to effectively combat modern threat tactics. Legacy scanning, defined by periodic, disruptive interrogations and an overwhelming volume of false positives, imposes unacceptable costs on security teams. If we only use the old methods of vulnerability management, we will only be prepared to fight against the old ways of cyberattacks, rather than adopting a strategic approach to risk reduction and security.

This evolution of approach requires moving beyond static snapshots and toward a continuous model of asset intelligence and verified risk assessment. Organizations that prioritize accuracy and situational context over scanning everything to see what sticks will be the ones that reclaim operational efficiency and achieve the earliest possible risk protection necessary to stay ahead of advanced cyberattacks.

A unified approach to the vulnerability lifecycle that spans from dynamic detection to automated remediation will facilitate the mindset shift that is needed to go from scans to true security.

To learn more about the Armis approach to vulnerability management throughout the entire lifecycle, visit Armis.com (Armis Centrix™ for Vulnerability Management Detection and Response page)

Checklist for Intelligence-Driven Vulnerability Management

Continuous Discovery and Assessment

- Continuously and automatically detect new vulnerabilities and risks of all assets and devices.
- Continuously reassess risks based on change events, updated vulnerability disclosure, or asset behavior.
- Continuously monitor the environment without impacting performance.

Asset Inventory and Intelligence

- Maintain a real-time inventory of devices, applications, and cloud workloads.
- Classify assets based on business criticality, risk exposure, and dependencies.
- Ensure visibility into shadow IT, ephemeral, and unmanaged devices.
- Monitor network telemetry for changes in asset behavior.

Augment Vulnerability Information

- Conduct gap analysis of existing coverage and assessment.
- Deploy selective, safe, and targeted queries to obtain any missing information.
- Integrate real-time threat and vulnerability intelligence to assess exploitability.
- Predictively validate vulnerabilities to determine the probability of exploit and the potential impact on the organization. Narrow the focus to real risk and operational impact.

Unification and Prioritization

- Unify all findings from internal and external sources to a single view.
- Shift to risk-based prioritization (business impact and exploitability, not just CVSS scores).
- Correlate and collaborate with the entire technology stack to streamline operations and facilitate action.

Remediation and Risk Reduction

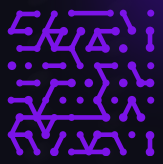
- View a verified, validated list of prioritized fixes to drive remediation processes.
- Deploy automated remediation and patching based on prioritization.
- Apply compensating controls (segmentation, firewall rules, etc.) when patching isn't feasible.
- Integrate with ITSM platforms for workflow automation.
- Align vulnerability management with incident response processes.

Validation and Monitoring

- Conduct validation testing to ensure vulnerabilities are properly remediated.
- Perform attack simulations and red teaming to test security effectiveness.
- Automate reporting for CISOs, auditors, and regulators.

Optimization and AI-Driven Automation

- Implement AI-driven adaptive risk scoring to refine prioritization.
- Leverage SOAR/SIEM playbooks as well as compensating controls from the existing security stack for faster response.
- Use predictive analytics, early warning and proactive threat hunting to identify emerging risks before they impact the environment.
- Ensure cross-platform integration to unify vulnerability management across all devices and the entire digital footprint.



ARMIS®

Go deep into the platform powering the future of security.

Explore Armis Centrix™

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com