Empower Your Vulnerability and Exposure Management Program With Nucleus Security

By Justin Boyer, Senior Validation Analyst
Omdia

OCTOBER 2025

Contents

Introduction 3

Background 3

Nucleus Security 5

Enterprise Strategy Group Technical Validation 6

A Unified View 6

Enterprise Strategy Group Analysis 6

Visibility Into Risk and Exposure 8

Enterprise Strategy Group Analysis 8

Automating a Vulnerability Management Program 10

Enterprise Strategy Group Analysis 10

Conclusion 12

Introduction

This Technical Validation by Enterprise Strategy Group details the evaluation of Nucleus Security. We validated how Nucleus Security helps organizations reduce risk by automating and maturing their vulnerability management and exposure management program.

Background

Modern enterprises operate sprawling, constantly changing attack surfaces across code, containers, cloud accounts, endpoints, networks, SaaS, and third-party services. A variety of security tools and teams regularly discover vulnerabilities, misconfigurations, leaked secrets, and risky identities. However, the challenge isn't finding security issues; it's the fragmentation of signals, context, and ownership. Many organizations are stuck in a siloed approach that makes it hard to see real exposures and effectively mitigate them before they are breached.

Organizations are investing in solutions to help overcome these challenges. Taking application security as an example, Enterprise Strategy Group research shows that 98% of research survey respondents are planning to invest in security solutions to modernize their approach to application security, including 57% who indicated that they will heavily invest in such solutions.[1] There are several factors that make it difficult to create and mature a vulnerability and exposure management program:

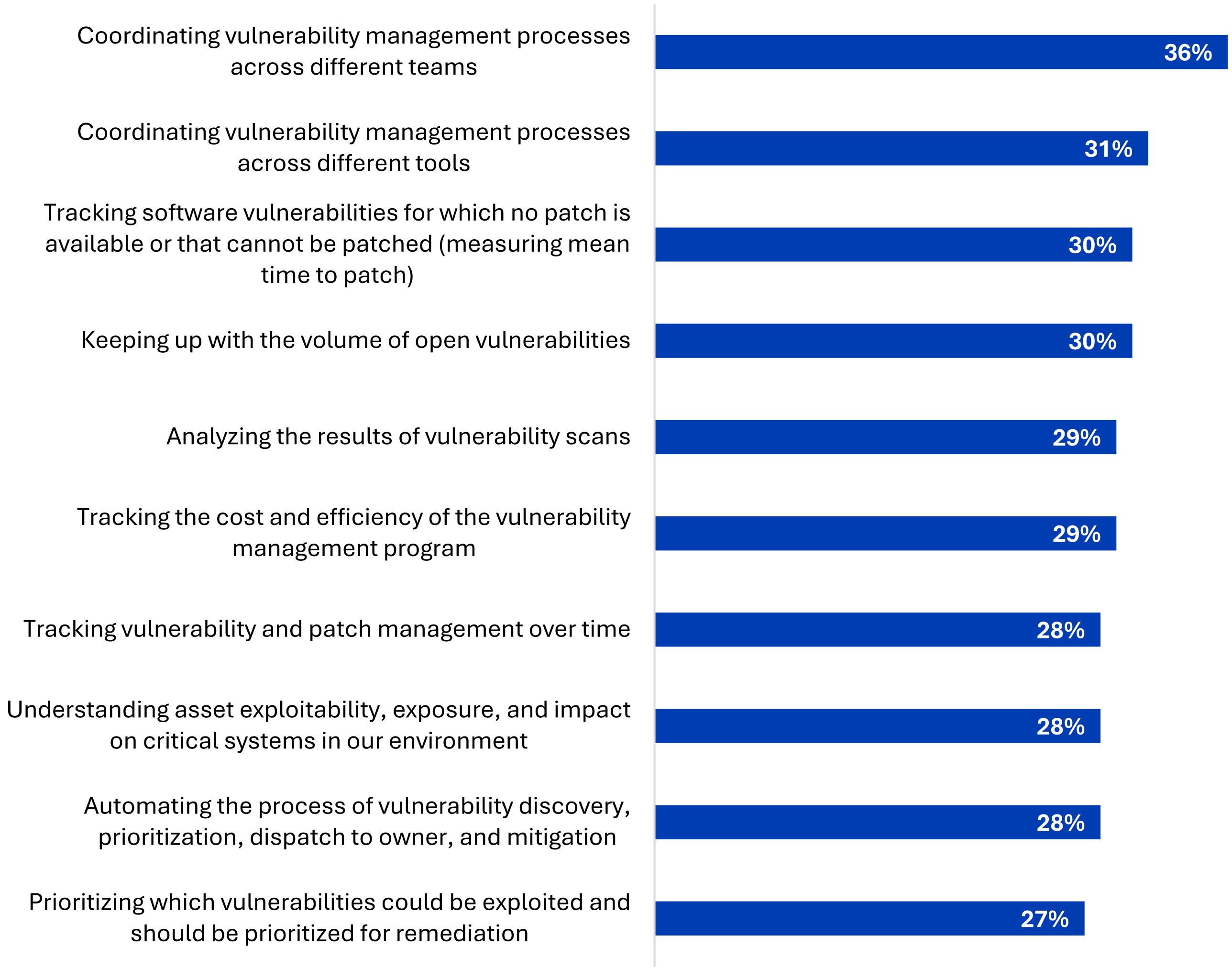
- **Data Overload**
  - A plethora of scanning tools that operate in silos leads to increased complexity and overhead.
  - Thousands to potentially millions of vulnerabilities overwhelm security, IT, and development teams alike.
  - It becomes more difficult to effectively communicate and coordinate with all stakeholders using manual processes.
- **Manual Processes**
  - Analysis, triage, and remediation tasking are still manual processes in many organizations.
  - These manual efforts slow down fixes and lead to some vulnerabilities being missed or ignored.
  - Manual tracking and reporting are time consuming and unreliable, leading to potential data errors creeping into vulnerability reports.
- **Poor Visibility**
  - Many organizations don't have a complete view of their overall risk posture, making it hard for leadership to understand exposure.
  - A lack of visibility leads to poor and ineffective metrics and KPIs.
  - Unclear responsibilities within teams further slow remediation and erode trust.

Figure 1 outlines the top 10 vulnerability management (VM) challenges as indicated by survey respondents.[2] Several themes immediately present themselves, illustrating the hurdles any solution must overcome to enable organizations to turn their vulnerability and exposure management program into a business asset.

[1] Source: Enterprise Strategy Group Research Report, *Modernizing Application Security to Scale for Cloud-native Development*, October 2024.
[2] Source: Enterprise Strategy Group Research Report, *Cyber-risk Management Best Practices*, December 2024. All Enterprise Strategy Group research references and charts in this technical validation are from this report unless otherwise noted.

Figure 1. Top 10 Vulnerability Management Challenges

Which of the following are the biggest challenges associated with vulnerability management at your organization? (Percent of respondents, N=375, multiple responses accepted)



Source: Omdia

Organizations are concerned about coordinating VM efforts across teams. These could include communicating and coordinating with stakeholders and development teams, especially assigning the right owners when it comes to remediation efforts. Other top themes include managing many tools, dealing with the amount of vulnerabilities, tracking the cost and efficiency of a VM program, and automation of critical VM processes, such as discovery, prioritization, dispatch to owners, and mitigation. Organizations are turning to solutions that enable them to build comprehensive vulnerability and exposure management programs that help teams communicate well, manage data overload, and eliminate manual processes.

Nucleus Security

Nucleus Security is a comprehensive vulnerability and exposure management platform built to enable organizations to build, automate, and scale their risk-based programs. Nucleus Security focuses on broad tool integration and dynamic automation, along with powerful analytical capabilities, to help organizations gain a view of their vulnerabilities and overall security posture and remediate high-risk vulnerabilities.

Nucleus has built its solution based on three core tenets:

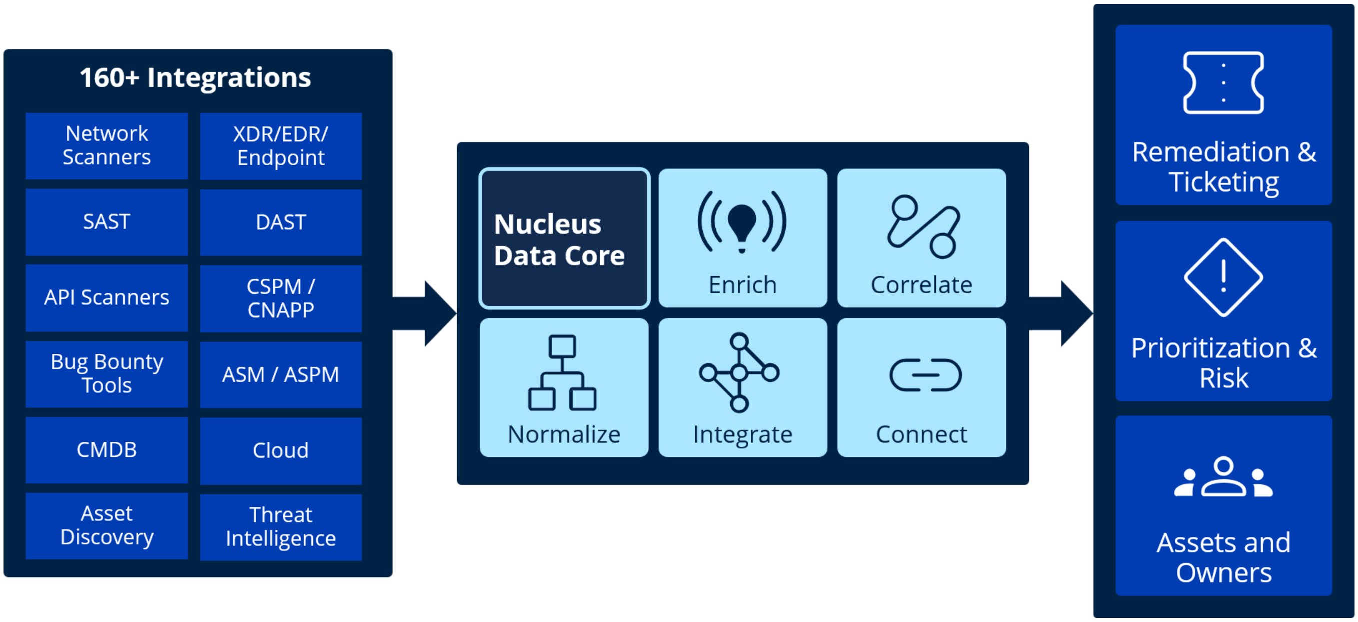
- **Unify.** Nucleus continuously pulls in, correlates, and normalizes data from all VM, asset, and threat intelligence tools. After this data ingestion, Nucleus consolidates all of it into one view, providing a single source of truth for an organization's vulnerability and exposure management program.
- **Correlate.** Nucleus organizes and enriches the incoming data and analyzes it to prioritize risk out of the box with built-in expertise.
- **Operationalize.** Nucleus offers the tools necessary to automate workflows so teams can mitigate vulnerabilities faster, with fewer resources, at scale. Nucleus enables organizations to effectively operationalize their vulnerability and exposure management program.

Nucleus Security is powered by the Nucleus Data Core, which integrates with common security tools and has over 160 connectors. It also features the FlexConnect, a universal connector schema that enables security teams to connect to tools for which a built-in integration doesn't exist.

As shown in Figure 2, the Nucleus Data Core collects and correlates all the data from VM tools and adds powerful automation capabilities to enhance an organization's vulnerability and exposure management program. Nucleus aggregates and deduplicates VM scanning tool data, identifying, consolidating, and deduplicating assets from different tools to provide a complete view of all assets. Nucleus also links identical container images across environments and repositories to enable cloud-native vulnerability management at scale, identifying the base container image used by deployments in which vulnerabilities were found.

Nucleus automates essential vulnerability and exposure management processes through Data Core's data fabric architecture, providing advanced scaling capabilities. Its customizable analytical engine automatically triages vulnerabilities from connected tools, prioritizes with threat intelligence and business context, and routes critical vulnerabilities to the right team for remediation. Nucleus also aggregates metrics and KPIs for high-level reporting, enabling security teams and management to track and measure the progress of the VM program.

Figure 2. Nucleus Security – Nucleus Data Core



Source: Omdia

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated Nucleus Security's vulnerability and exposure management solution via remote demonstration. We focused on how Nucleus delivers a unified view of an organization's assets and vulnerabilities, provides detailed and actionable insight into risk and exposure, and enables automation throughout the vulnerability and exposure management process.

A Unified View

Enterprise Strategy Group validated how Nucleus delivers a unified view of organizational assets, along with correlated vulnerability data for each.

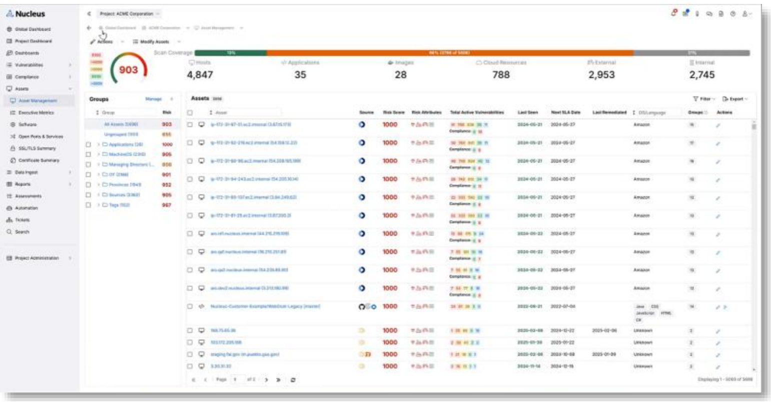
Enterprise Strategy Group Analysis

As organizations scale, the attack surface expands across in-house applications, SaaS platforms, cloud services, virtual machines, and distributed endpoints. Security teams are overwhelmed by vulnerability overload, with siloed tools generating fragmented visibility and duplicative data. This sprawl of technologies and disconnected sources creates operational friction, making it nearly impossible to see the full picture of organizational risk and to drive timely, coordinated remediation at enterprise scale.

Nucleus Security delivers a powerful integration capability that helps organizations consolidate their security tools' data to build a successful vulnerability and exposure management program. Nucleus integrates with 160+ tools, including security scanners, asset management tools, threat intelligence, penetration test results, and other data sources, and normalizes 195 asset types, including 135+ cloud asset types, into one searchable inventory. Data can be pulled from the sources or pushed to Nucleus via triggers. Nucleus ingests both structured and unstructured data while merging, deduplicating, and normalizing the data to create a single timeline and view of risk.

Nucleus correlates and deduplicates data at the metadata, core asset, and vulnerability levels. It also supports correlation of cloud assets across the continuous integration/continuous delivery (CI/CD) pipeline from code to container to cloud runtime. Nucleus Adaptive Contexts preserve code-to-container-to-cloud lineage, including base image relationships, enabling one fix to remediate vulnerabilities across environments. This unified asset inventory enables organizations to group assets based on function and organizational hierarchy while having a flattened and searchable view of core asset metadata. For example, organizations can search for vulnerabilities of a certain type or severity based on the value of certain attributes. These metadata attributes can be used for searching, reporting, automation, and prioritization (see Figure 3).

Figure 3. Consolidated Assets in One View



Source: Omdia

At the time of this writing, Nucleus supports 195 asset types, from virtual machines to hosts, OT/IoT, container images, repositories, and over 135 cloud asset types. Nucleus's sizable asset library and subsequent deduplication capabilities can detect duplicates across multiple scanning tools and generate consistent asset IDs. Using this unified view of all assets, organizations can have a solid foundation on which to build their vulnerability and exposure management programs. Nucleus also provides business context and groups applications and asset hierarchies based on teams, supervisors, and departments to provide visibility for each user or team across their assets and risks.

Why This Matters

The ever-growing attack surface of many organizations has led to increased risk and scrutiny regarding vulnerability management. However, the sheer number of findings and assets in use can make vulnerability and exposure management overwhelming for many. According to Enterprise Strategy Group research, surveyed organizations indicated that improving integration of vulnerability management tools with other IT technologies, gaining increased insight into asset exposure, and improving their ability to update their attack surface inventory and asset details would improve their vulnerability management programs. A unified view of all of their assets, along with necessary details and asset ownership, is vital to a successful program.

Enterprise Strategy Group validated that Nucleus Security helps organizations build a strong foundation on which to stabilize and enhance their vulnerability and exposure management program. Nucleus integrates with over 160 tools across security scanners, CMDBs, cloud services, and CI/CD pipelines, ingesting their asset and vulnerability data into the Nucleus Data Core. Nucleus then deduplicates the asset data, providing a single, clean record for each asset it can then use to aggregate vulnerability data along with key metrics and KPIs. Nucleus maintains strong business context, including asset criticality, data sensitivity, internet exposure and compliance scope, as well as assigning assets to the correct organizational units to maintain accountability.

With Nucleus Security, organizations can run their entire vulnerability and exposure management program, including cloud, OT/IoT, application security, and risk-based vulnerability management from one platform. Organizations can use Nucleus to shift to strategic risk-driven initiatives and root cause analysis with a single view of their security posture across all asset types.

Visibility Into Risk and Exposure

Enterprise Strategy Group validated how Nucleus enables organizations to gain visibility into risk and exposure across the enterprise.

Enterprise Strategy Group Analysis

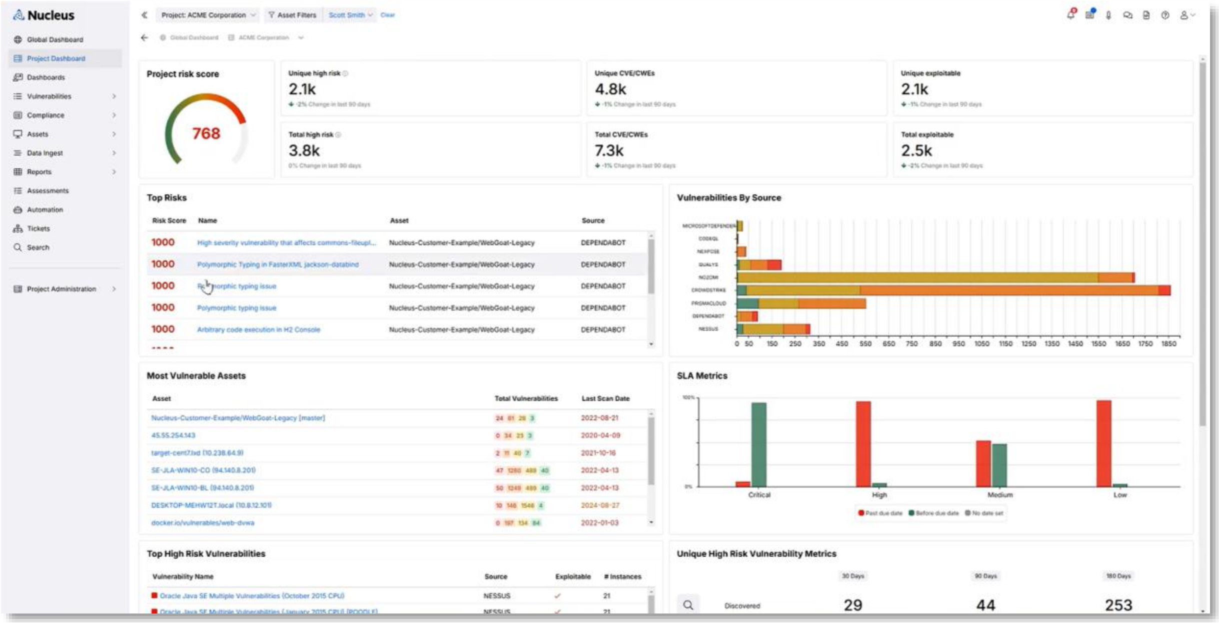
Without proper visibility into an organization's risk and exposure, security teams can't properly prioritize remediation efforts or create strategic initiatives designed to reduce risk over time. Nucleus provides the insights necessary to view, understand, and remedy vulnerabilities across the enterprise.

After Nucleus ingests data from the existing security and infrastructure tools, it aggregates and correlates security findings by asset. These findings are distinct security objects associated with an asset. They could be a vulnerability, compliance finding, misconfiguration, or penetration test result. This correlation enables groupings of findings, delivering instant visibility into which assets are affected by the same vulnerabilities. In the case of ephemeral assets, such as container images deployed as separate workload instances, Nucleus creates Adaptive Contexts to tie these instances together and deliver visibility into container-based ecosystems.

Nucleus provides visibility aligning with expedited and efficient remediation strategies, supported by the prioritized vulnerabilities view and the Fixes Page, which provides a view of total risk by fix. These views enable organizations to more efficiently reduce risk by using automation to create tickets on detection or showing which vulnerabilities can be remediated by a single update.

Nucleus brings these insights to the fore with advanced reporting capabilities. Figure 4 shows a dashboard view for a specific project. Within this view, we were able to click into a dashboard widget to view the details with data-filtering capabilities. These dashboards are customizable by each team to provide the metrics executives and team leaders want to see. Dashboards provide a unified view for a team that can then be pushed out to the team members so everyone can work from the same view of vulnerabilities and risk.

Figure 4. Project Dashboard



Project risk score
768

Unique high risk
2.1k
-2% Change in last 90 days

Total high risk
3.8k
0% Change in last 90 days

Unique CVE/CWEs
4.8k
-1% Change in last 90 days

Total CVE/CWEs
7.3k
-1% Change in last 90 days

Unique exploitable
2.1k
-1% Change in last 90 days

Total exploitable
2.5k
-2% Change in last 90 days

Top Risks

Risk Score	Name	Asset	Source
1000	High severity vulnerability that affects commons-fileupl...	Nucleus-Customer-Example/WebGoat-Legacy	DEPENDABOT
1000	Polymorphic Typing in FasterXML jackson-databind	Nucleus-Customer-Example/WebGoat-Legacy	DEPENDABOT
1000	Polymorphic typing issue	Nucleus-Customer-Example/WebGoat-Legacy	DEPENDABOT
1000	Polymorphic typing issue	Nucleus-Customer-Example/WebGoat-Legacy	DEPENDABOT
1000	Arbitrary code execution in H2 Console	Nucleus-Customer-Example/WebGoat-Legacy	DEPENDABOT

Vulnerabilities By Source

Most Vulnerable Assets

Asset	Total Vulnerabilities	Last Scan Date
Nucleus-Customer-Example/WebGoat-Legacy [master]	24 81 28 3	2022-08-21
45.55.254.143	0 34 23 3	2020-04-09
target-cent7.lxd (10.238.64.9)	2 11 40 7	2021-10-16
SE-JLA-WIN10-CO (94.140.8.201)	47 1280 489 40	2022-04-13
SE-JLA-WIN10-BL (94.140.8.201)	50 1249 489 40	2022-04-13
DESKTOP-MEHW12T.local (10.8.12.101)	10 146 1546 4	2024-08-27
docker.io/vulnerables/web-dvwa	0 197 134 84	2022-01-03

SLA Metrics

Top High Risk Vulnerabilities

Vulnerability Name	Source	Exploitable	# Instances
Oracle Java SE Multiple Vulnerabilities (October 2015 CPU)	NESSUS	✓	21
Oracle Java SE Multiple Vulnerabilities (January 2015 CPU) (POODLE)	NESSUS	✓	21

Unique High Risk Vulnerability Metrics

	30 Days	90 Days	180 Days
Discovered	29	44	253

Source: Omdia

The Nucleus Data Core delivers AI-powered Nucleus Insights to help organizations gain greater insight into vulnerabilities and real-world risk. Nucleus Insights uses threat intelligence, which provides the most comprehensive view into which vulnerabilities are being exploited in the wild and by which threat actors, to create a Nucleus Threat Rating for each CVE. Security teams and business owners can use the Nucleus Threat Rating to prioritize critical vulnerabilities exploited in the wild to focus remediation efforts. Additionally, Nucleus can group vulnerabilities by software fix, helping to highlight which software upgrades would remediate the most vulnerable parts of the environment.

Nucleus uses its insight into business context to deliver helpful information that can guide remediation efforts. Security teams can use the business context to understand which vulnerabilities are in assets that are accessible externally or will improve compliance when fixed. Additionally, each finding preserves the detailed context of the security tool that surfaced it. For example, findings from static application security testing (SAST) tools may include file paths or code snippets, while findings from dynamic application security testing (DAST) tools may include HTTP request/response evidence. These helpful context-based details speed up remediation efforts and further the unifying view that Nucleus delivers. For example, teams can automatically surface and route fixes for CVEs actively used in ransomware and mass-exploitation campaigns on internet-exposed assets, shrinking the blast radius before lateral movement.

Why This Matters

Gathering and deduplicating data is only the first step. Organizations can't act on the data until they have clear visibility into the risk and exposure the vulnerabilities discovered represent. Without insight into the exploitability, exposure, and impact on critical systems each finding has, security teams can't properly understand the underlying business risk and effectively prioritize remediation strategies.

Enterprise Strategy Group validated that Nucleus Security delivers insights into the risk and exposure the various vulnerabilities discovered represent. Nucleus Insights, an AI-powered component embedded in the Nucleus Platform, uses threat intelligence to create standardized threat ratings and exploitability flags. No matter which tool originally generated the finding, Nucleus creates a singular threat rating scale based on which vulnerabilities are being actively exploited in the wild and combines it with asset context such as criticality and internet exposure to calculate the Nucleus Risk Score. Nucleus also provides security teams with project dashboards that surface key metrics and vulnerability data to executives and management, keeping them updated while providing a view with which they can drive and prioritize remediation efforts.

Nucleus delivers standardized risk scores across all findings, eliminating the wasted time and effort of comparing the conflicting risk scores from various tools. Categorized risk scores by asset group, owner, and team establish a common risk language from engineering to the board, enabling accountable, top-down remediation. By providing a unified view of security risk, Nucleus delivers visibility and insight into the overall posture, along with the prioritized contributing findings, ensuring that remediation efforts focus on the vulnerabilities that will have the greatest impact on risk reduction and compliance.

Automating a Vulnerability Management Program

Enterprise Strategy Group validated how Nucleus helps organizations automate their vulnerability and exposure management program.

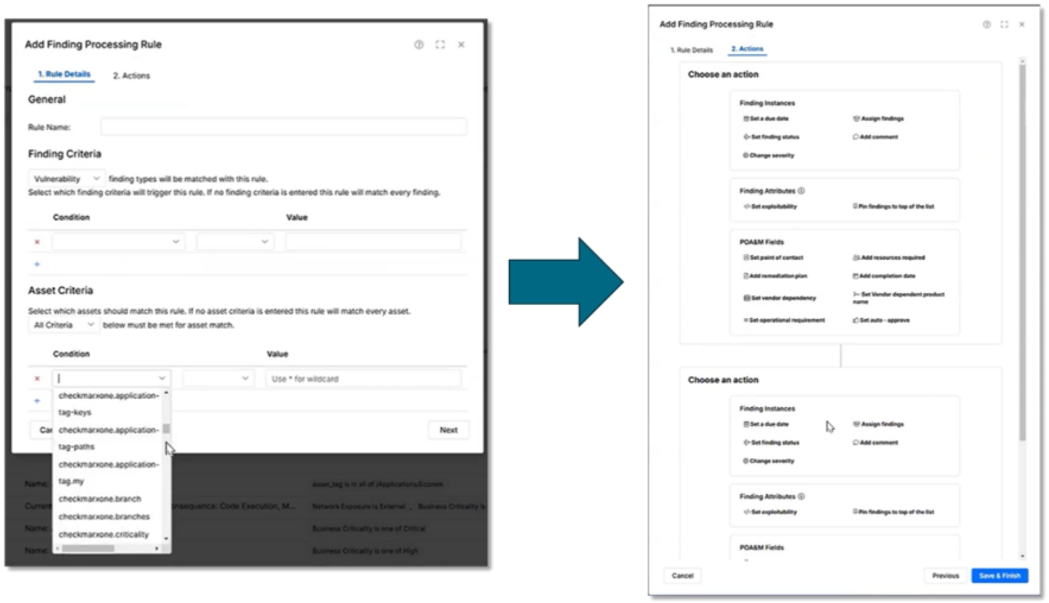
Enterprise Strategy Group Analysis

Scanning, gathering, and organizing vulnerabilities across an environment is only the beginning of the VM process. Nothing is accomplished if those vulnerabilities aren't remediated in a timely manner. However, many organizations continue to struggle to get vulnerabilities to the right people or teams to remediate them before they can be exploited. Any vulnerability and exposure management solution must help organizations automate their programs not only to triage and prioritize risks but also to eliminate unnecessary remediation delays.

Nucleus features a powerful automation engine capable of complex processing as data flows into the system. The dynamic templating language provides administrators with the power to reference variables, use regular expressions, and access arrays of data, providing maximum flexibility when processing data from various sources. Nucleus automations support quantitative and qualitative prioritization strategies (risk scores vs. SSVC) as well as expedited or efficient remediation strategies (remediate the most critical risks vs. group by risk for bulk remediation). Bi-directional ServiceNow/Jira updates, auto-applied SLAs and exceptions, and due-date/expiration controls enforce policy at enterprise scale.

The automation pipeline in Nucleus is structured into sequential workflow stages that mirror the vulnerability management lifecycle. It begins with asset discovery and inventory, continues through vulnerability processing from multiple sources, and culminates in remediation, exception handling, and notifications. At each stage, administrators can apply rules, leverage variables, and reference contextual data to dynamically shape how findings and assets are handled under specific conditions. This flexibility enables organizations to automatically group applications by owner or business unit, assign dynamic risk or criticality scores based on asset context, and drive targeted remediation paths. Because every action and output can serve as an input for later steps, automation in Nucleus creates a seamless system that adapts in real time to new data. The result is a highly efficient, risk-aligned vulnerability management program where SLAs, exceptions, and remediation workflows are executed consistently and at scale without manual intervention (see Figure 5).

Figure 5. Creating a Processing Rule



Add Finding Processing Rule

1. Rule Details | 2. Actions

General

Rule Name:

Finding Criteria

Vulnerability finding types will be matched with this rule.
Select which finding criteria will trigger this rule. If no finding criteria is entered this rule will match every finding.

Asset Criteria

Select which assets should match this rule. If no asset criteria is entered this rule will match every asset.
All Criteria below must be met for asset match.

Name: asset_tag is in all of /Applications/Ecomm

Current ... nsequence: Code Execution, M... Network Exposure is External , Business Criticality is

Name: Business Criticality is one of Critical

Name: Business Criticality is one of High

Add Finding Processing Rule

1. Rule Details | 2. Actions

Source: Omdia

Why This Matters

According to Enterprise Strategy Group research, 30% of surveyed organizations struggled to keep up with the volume of open vulnerabilities. Another 36% struggled to coordinate vulnerability management activities across teams. As the number of applications, infrastructure, and endpoints increases, so, too, does the complexity of managing their vulnerabilities. Organizations still relying on manual processes will struggle to keep up and will inevitably increase their risk in the meantime.

Enterprise Strategy Group validated how Nucleus helps organizations build automation into their vulnerability and exposure management program. Nucleus exposes the data workflow to administrators, enabling them to perform and customize complex data processing as security findings enter the system. With its powerful templating language, administrators can process findings, automate remediation workflows, issue notifications, and generate tickets based on exploitability, criticality, or other business factors.

Increasing automation eliminates much of the manual triage, ticketing, and notification of affected teams. Once the rules are established, Nucleus enables organizations to focus on more strategic VM program management rather than operational functions.

Conclusion

The number and variety of applications businesses use to accomplish their work has increased, along with the complexity of keeping them secure. According to Enterprise Strategy Group research, 98% of survey respondents indicated that they are planning to invest in security solutions to improve their application security.[3] These investments are necessary due to the many challenges inherent in application security and vulnerability and exposure management, namely data overload, too many manual processes, and poor visibility into risk posture. These factors impede many organizations on their journeys to create a mature vulnerability and exposure management program.

Nucleus Security has developed a solution that enables organizations to build and maintain a strong and scalable vulnerability and exposure management program. Nucleus focuses on extensive tool integration and automation, along with AI-powered analytics, to unify, correlate, and operationalize vulnerability data from across the environment. The Nucleus Data Core collects, aggregates, and correlates data from over 160 common security tools and across vulnerability management, asset management, and threat intelligence. It then provides the tools necessary for rapid remediation, helping organizations focus on the important risks.

Enterprise Strategy Group validated that Nucleus creates a unified view of security and risk posture across the enterprise. We saw how data pulled from cloud services, applications, OT/IoT, CI/CD pipelines, and containers will deliver a single, risk-driven view of exposure. We also validated how the AI-powered Nucleus Insights uses threat intelligence to understand which vulnerabilities are being exploited in the wild and by which threat actors. Since Nucleus understands business and technical context, it knows which vulnerabilities exist on services exposed to the outside world. This insight helps security teams and business owners prioritize critical vulnerabilities exploited in the wild and focus remediation efforts on them. Finally, we validated Nucleus Security's powerful automation capabilities, as it gives administrators the power to process data as it comes into the system and automate ticket creation and assignment based on rules. With these tools, organizations have the power to build, automate, and enhance their vulnerability and exposure management program.

If your organization struggles to keep up with the flood of security vulnerabilities and manual processes, Enterprise Strategy Group recommends seriously considering Nucleus Security.

[3] Source: Enterprise Strategy Group Research Report, *Modernizing Application Security to Scale for Cloud-native Development*, October 2024.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the “Omdia Materials”) are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together “Informa TechTarget”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

Get in touch: www.omdia.com askananalyst@omdia.com