2025

NOPSEC

OUTCOMES OVER OPERATIONS:

Is a Managed Vulnerability Service Right for You?

EXECUTIVE SUMMARY

Mid-sized organizations face the same cybersecurity challenges as larger enterprises but with fewer resources. Cloud-first architectures, container adoption, and VM sprawl have expanded the attack surface, while the cybersecurity skills gap continues to grow. Despite investing in multiple scanning tools, many organizations find themselves buried in alerts with little improvement in their security posture.

This whitepaper explores why organizations should consider outsourcing vulnerability management to a Managed Vulnerability Management (MVM) provider. Rather than focusing on tool outputs, organizations can prioritize outcomes, such as reduced risk, faster remediation, and smarter use of internal talent. By reframing return on investment (ROI) in terms of time saved, risk lowered, and security improved, outsourcing becomes not just viable, but strategic.

The Current State of Security

Most medium-sized businesses operate complex production environments that mix cloud and on-premises servers, virtual machines, containers, and the systems used to deploy and manage them.

These systems introduce new risks, such as insecure cloud configurations, vulnerable container images, and untracked operating system states. At the same time, these organizations must navigate a cybersecurity landscape with limited headcount and flat budgets.

Despite best efforts, security teams are overwhelmed. Small teams manage scanning, triaging, reporting, and remediating vulnerabilities while fending off increasingly sophisticated attacks.

So what are the options?

- **BUSINESS AS USUAL:**

  Continue spending too much time managing scanning, prioritizing, and reporting, and not enough time on remediation? See continued staff burnout and turnover?

- **INCREASE BUDGET:**

  Hire more staff, consultants, or purchase more software. Can you be sure of the ROI that this will deliver?

- **TAKE AN OUTCOME-BASED APPROACH:**

  Your goal is to minimize risk and stay within budget. Strategically outsourcing routine tasks to a service provider can give your team the time they need to focus on remedying the problems and implementing controls to prevent them from happening again.

The Hidden Costs of In-House Vulnerability Management

On the surface, running your own scanning tools looks cost-effective. But in practice, in-house vulnerability management carries significant hidden costs:

- **Tool complexity:** The use of separate scanners for cloud, containers, VMs, and infrastructure adds integration and maintenance burdens. Small organizations still typically use 10-20 scanning tools to cover their attack surface area.
- **Operational overhead:** Tool configuration and optimization, as well as monitoring that scans run correctly, all consume valuable team time and attention.
- **Data normalization and manual triage:** Not every finding is valid, and tuning systems to filter out erroneous findings can be a considerable undertaking.
- **Alert fatigue:** Thousands of unprioritized findings drain focus from real threats.
- **Reporting burden:** Security teams spend time proving they scanned rather than showing how they reduced risk.

All of this diverts time from tracking and remediating high-risk issues.

Reframing ROI: From Tool Cost to Risk Reduction

Traditional ROI calculations often center on tool licensing costs. However, in cybersecurity, value lies in risk reduction, not software usage. A better way to assess ROI includes:

- **Team efficiency:** Time saved on triage and reporting
- **Exposure window:** Reduced time between detection and remediation
- **Incident avoidance:** Fewer breaches due to quicker risk mitigation
- **Cost predictability:** Fixed service pricing vs. fluctuating tool and labor costs

www.nopsec.com

Take a Smart Approach to Outsourcing

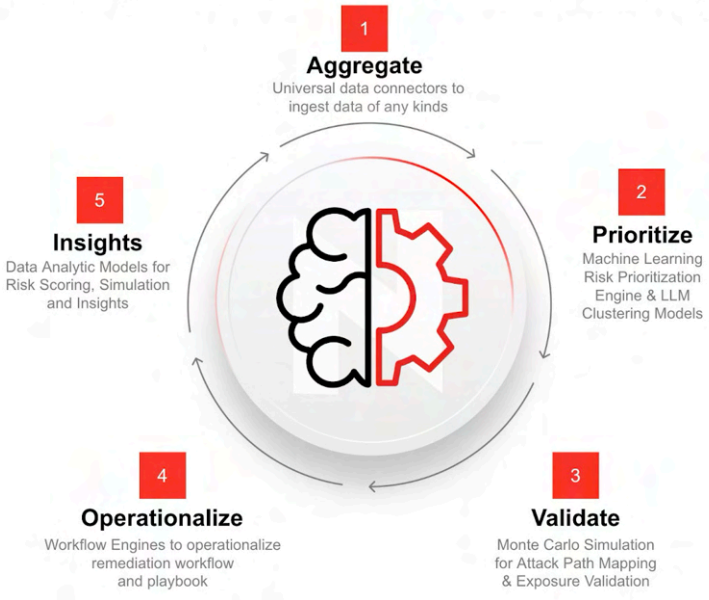
To be effective, your security team needs to aggregate data from multiple tools, sift through it to identify urgent problems, validate that the findings represent a real vulnerability in your particular configuration, and then resolve the issue as efficiently as possible. If there's time, getting actionable insights from the data can help fix root cause issues and prevent problems in the future.

Outsource: Scan Configuration, Management, and Monitoring.

Are all the right scans configured? With optimized settings? Who's keeping the tools up to date? Are the scans running correctly? An outsourced service can do these tasks much more efficiently.

Outsource: Data Aggregation and Flaw Prioritization.

Managing multiple streams of findings, deciding what to prioriti and knowing what's being activel exploited demands knowledge, tools, and time. Time that is bette spent by your team fixing the issues. Outsourcing this step to a service with experts constantly watching for the next 'celebrity vulnerability' with its headline-grabbing news and cuddly logo will keep you ahead.



Outsource: Validate

Determining if a particular vulnerability has a valid attack path (and hence represents a genuine exposure) is a complex task that requires significant manual effort or advanced simulation skills. Given the depth of expertise needed, it's another prime candidate for outsourcing.

Leverage: Operationalize

Done correctly, the first three steps will deliver high-priority, validated vulnerabilities. Now it's time to work with the outsourced service to automate the workflow so that critical flaws can be routed to the right team, accompanied by useful information so your 'local experts' can remediate them as fast as possible. By removing the toil of the preceding steps, teams are free to perform the high-value tasks of eliminating the risks before it's too late.

Outsource: Insight

Vulnerability management must be both efficient and transparent. However, tracking metrics, running what-ifs, and reporting on progress can be a frustrating distraction from the work that creates the progress in the first place. Outsourcing these tasks will not only make it easier to demonstrate progress, but it will also improve the rate of progress itself.

Choose to in-source if:	**Choose to outsource if:**
You want total control of the choice of scanning tools, configuration, integrations, and scan scheduling, and have the time to do it.	You are more focused on resolving vulnerabilities than on the mechanics of finding them.
You already have scan monitoring and management in place, and are sure scans are configured and running correctly.	You'd like to offload the burden of scan administration to an efficient managed service.
You already have a high-performing, efficient vulnerability triage process.	Your risk posture would benefit from advanced vulnerability management, prioritization, and triaging.
Your stakeholders are happy with the quality of your reporting, and you can afford the resources it requires.	You want reporting and visibility without diverting resources from reducing risk.
Your operations are efficient and effective.	You would like assistance with operationalizing your vulnerability management practice with a focus on risk reduction not operations.

Focus on Outcomes, Not Outputs

The goal is reducing exploitable risk, not managing scan findings. Outsourcing to a provider like NopSec shifts the focus to outcomes:

- **Team efficiency:** Time saved on triage and reporting
- **Prioritized remediation** aligned with business risk
- **Policy-driven workflows** for consistency and compliance
- **Meaningful metrics** like MTTR (Mean Time to Remediation), % of critical issues closed within SLA, and posture improvements

By outsourcing scan management and results processing, MVM allows internal teams to concentrate on remediating urgent vulnerabilities, setting policies, and fixing risks at source.

Why Outsourcing Works

Managed services like NopSec MVM bring:

- **Specialization:** Security expertise and mature processes
- **Automation:** Advanced tooling without maintenance overhead
- **Scale:** Economies of scale reduce cost and increase coverage
- **Continuity:** No gaps due to staff turnover or bandwidth

Instead of building a team to manage tools, you gain a partner focused on delivering reduced risk.

Example: Relief from Patching Pain

Deciding what to patch and when is a constant problem. Between hypervisors, operating systems, dependencies, and applications, the list of possible patches is near-endless. Balancing security needs against operational risks, disruption, and resources for testing and implementation is challenging. NopSec managed vulnerability management can make prioritized, risk-based recommendations for patching, allowing you to tune your risk tolerance against your operational capacity.

The NopSec Approach

NopSec delivers a proven combination of platform power, expert services, and a risk-reduction mindset tailored for your organization's size. Rather than just run scans and issue reports, we provide an end-to-end Managed Vulnerability Management solution that quickly improves visibility, prioritization, and remediation workflows. This gives your people the time, visibility, and direction to be an effective risk-reduction team, not just a risk discovery function.

Implementation
Our onboarding process starts with an implementation kickoff, followed by several parallel workstreams:

Customer Environment Setup:

Environment discovery: Inventory of cloud, container, and IaC environments

Tool integration: Roll out of our managed scanning services in your environment

NopSec Platform Configuration:

Platform onboarding: Provision the NopSec SaaS platform with users and roles

Risk alignment: Custom tuning of risk scoring based on your environment and business impact

Operations Configuration:

Platform onboarding: Provision the NopSec SaaS platform with users and roles

Risk alignment: Custom tuning of risk scoring based on your environment and business impact

Most customers complete onboarding within 30 days.

Ongoing Monitoring & Management

Our platform continuously ingests, correlates, and prioritizes findings using contextual risk scoring. The platform

- Unified view across all assets and sources
- Threat intelligence enrichment
- Automated ticketing and remediation tracking
- Continuous improvement via policy-based governance

NopSec's patented exposure and remediation scoring models help teams focus on the risks that matter most.

Customer Success & Communication

Every NopSec engagement is led by a dedicated Customer Success Manager (CSM). Regular check-ins ensure:

- SLA performance is tracked and optimized
- Key metrics are reviewed, including MTTR and risk reduction progress
- Continual adjustments as environments evolve
- Executive-level reporting supports stakeholder communication
- Integration of the findings from other tools, such as code scanning or supply chain analysis, into the NopSec platform.

The NopSec Vulnerability Detection Suite

Nopsec Managed Vulnerability Management can replace most of your current tools for vulnerability detection and management.

Vulnerability Management	Continuous asset discovery across on-prem, cloud, containers, and remote endpoints with automated vulnerability scanning.
Cloud Security Assessment	Continuous monitoring and assessment of cloud infrastructure (AWS, Azure, GCP) to identify misconfigurations, exposed services, and compliance violations
Web Application Scanning	Scan web applications and APIs for OWASP Top 10 risks and other vulnerabilities.
Container Security	Scan container images for vulnerabilities in base images and open-source components.
Endpoint Detection	Extend scanning capabilities to endpoints for vulnerabilities, misconfigurations, and missing patches.
Infrastructure as Code (IaC) Scanning	Scan Terraform, CloudFormation, and Kubernetes configurations to identify security issues before deployment.

www.nopsec.com

A Better Way to Reduce Risk

Security teams should be judged by their ability to reduce exploitable risk, not by the volume of scans or length of reports. For many organizations, outsourcing vulnerability management provides a pragmatic path to enhanced security and improved operations.

Let your team focus on the work only they can do. Let NopSec handle the rest.

Is your team buried in scan results instead of fixing real problems? Contact us for a risk assessment or ROI consultation.

GET IN TOUCH

Let NopSec help you focus on what matters.

www.nopsec.com