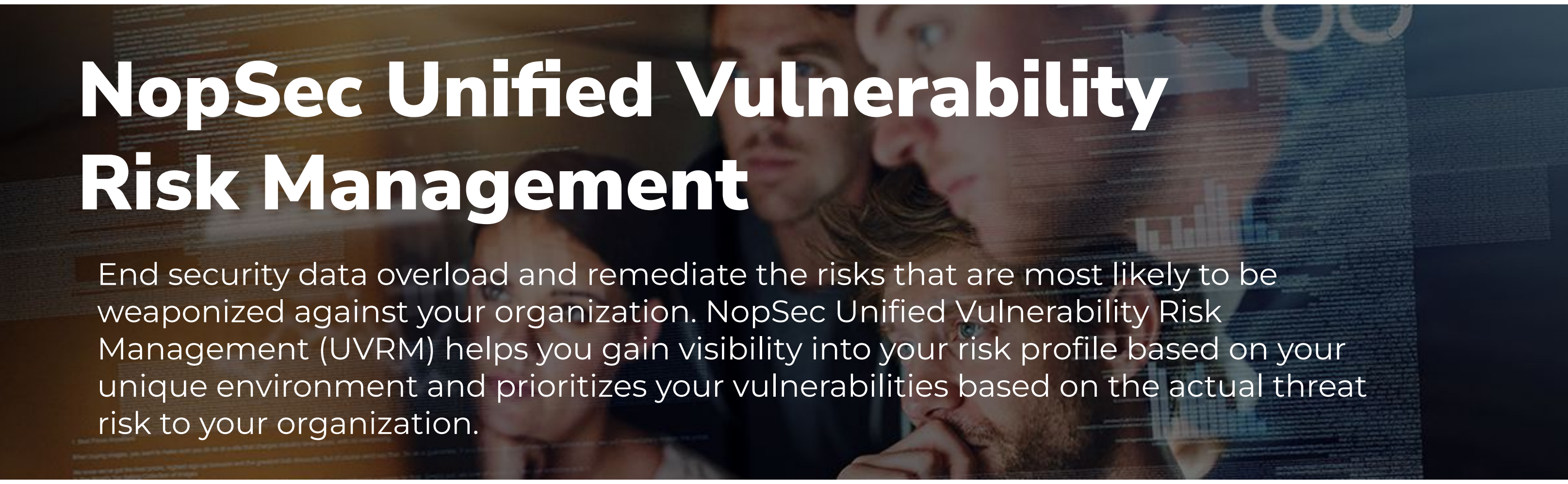
NOPSEC



NopSec Unified Vulnerability Risk Management

End security data overload and remediate the risks that are most likely to be weaponized against your organization. NopSec Unified Vulnerability Risk Management (UVRM) helps you gain visibility into your risk profile based on your unique environment and prioritizes your vulnerabilities based on the actual threat risk to your organization.

Everything You Need to Manage Your Organization’s Vulnerability, All in One Place

Traditional vulnerability assessment solutions might fulfill compliance mandates, but typically fail to deliver true strategic value through complete visibility, remediation prioritization, and overall vulnerability risk management efficiency. Vulnerability assessment solutions can also have a tendency to create data overload — making it difficult to extract actionable intelligence — and provide poor business and threat context.

Additionally, siloed processes and fragmented ownership create misaligned objectives and priorities across IT teams. This causes conflicting priorities, resulting in the creation of windows for exploitation that can result in costly breaches.

Effectively prioritizing and managing your cybersecurity exposure requires technology capable of centralizing your siloed and fragmented processes. Businesses need a unified threat solution.

Assess Exposure, Remediate Threats, Measure Progress, and More with NopSec UVRM

NopSec UVRM provides a complete end-to-end vulnerability risk management platform, from machine-learning based prioritization, to remediation automation and orchestration.

Utilizing passive analysis, active validation, and contextual enrichment, NopSec enables security teams to visually forecast threat risk and dramatically reduce the time to remediation for critical security vulnerabilities across infrastructure, endpoints, and applications, as well as provides program metrics for executive stakeholders.

NopSec UVRM Helps You Achieve More with Less

NopSec UVRM enables you to save time and resources, delivering ROI that matters.

- 25-50% Less Time Spend in Manual Data Triage
- Noise Reduction of 40-80% Post-Prioritization
- 98% Efficiency in Risk Compared to CVSS
- 60-75% Reduction in MTTR Metrics

NOPSEC

Why NopSec Unified VRM

Full-Stack Aggregation and Visibility

With a multitude of disparate data sources and systems, Security and ITOps teams struggle to get an accurate view into the state of their environment. Correlating everything you need to know across your technology stack manually is extremely difficult, if not entirely impossible. NopSec Unified VRM delivers complete visibility into your entire security technology stack, aggregating your infrastructure, cloud container, and application vulnerabilities in one, unified platform. This enables your team to view your risk in the context of your business applications or services by logical grouping. NopSec UVRM enables you to leverage your CMDB to tie all of your observed vulnerabilities across the organization and further organize them according to your business structure.

Prioritization with Context

Leveraging best-in-class machine learning algorithms, NopSec UVRM analyzes billions of pieces of information to understand attack activity and likelihood in real time. With NopSec, your vulnerability scanner risk scores will be reprioritized based on insights from 30+ threat intelligence feeds for malware, ransomware, threat actors/campaigns, public exploit databases, social media, and more. Furthermore, NopSec UVRM pulls asset criticality data from your CMDB to deliver unique context around each vulnerability in your environment. The end result is a precise and prioritized list of vulnerabilities that should be remediated first. Unlike other vulnerability risk management platforms, we don't blackbox this — you can easily view the top five factors affecting your risk score.

Vulnerability Metrics for All Stakeholders

NopSec UVRM provides full visibility into the performance of your vulnerability management program. You can track and report on KPIs such as MTTR, SLA policy compliance, and many more, all in real-time. NopSec URVM reporting uniquely provides the transparency and accountability your C-Suite needs by using common language — no technical jargon. You can report by business line, product, or platform and track trend data to indicate changes in your risk posture. Team tracking proactively identifies opportunities for improvement and role-based filters ensure your users see relevant data. Additionally, you can schedule dashboards and reports to keep all stakeholders in the loop.

Workflow Automation

Unite the efforts of your Security and ITOps teams. Relying on emailed lists or tickets created manually in your ITSM is inefficient and error-prone. NopSec enables you to design and manage vulnerability processes from identification through remediation and automatically push remediation tickets through to your orchestration systems. NopSec UVRM's workflow automation also assigns SLAs based on the NopSec risk score, alerts key stakeholders when critical SLA dates are missed, and enables you to track remediation performance by business line, product, or platform.

Security and IT leaders are being tasked to achieve more business objectives with relatively little security budget. Luckily, solving vulnerability management challenges doesn't have to break your budget or require more staff. With the right RBVM technology to support your team, you can achieve demonstrable progress in reducing your risk exposure, unite your vulnerability management efforts, and mature your security program.

Ready to see NopSec UVRM in action? Schedule a demo today.