CrowdStrike Store

NOPSEC

CROWDSTRIKE

Data Sheet

NOPSEC: UNIFIED VRM®

Gain visibility and prioritize vulnerabilities with vulnerability risk management (VRM)

CHALLENGES

Traditional scanners fulfill compliance mandates but fail to deliver strategic value in complete visibility, remediation prioritization and overall vulnerability risk management (VRM) program efficiency. Traditional scanners create data overload, making it difficult to extract actionable intelligence, and they provide poor business and threat context.

Siloed process ownership across the VRM lifecycle creates misaligned objectives and priorities across infrastructure, endpoint, security and application teams. This causes remediation delays and creates windows for exploitation that can result in costly breaches.

Finally, the manual processes related to data collection, analysis, prioritization and reporting waste valuable employee time and create significant inefficiencies.

SOLUTION

CrowdStrike® Falcon Spotlight™ scanless vulnerability management offers security teams a real-time assessment of vulnerability exposure on their endpoints that is always current. Built on the CrowdStrike Falcon® platform, powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight enables customers to assess vulnerabilities within a complete endpoint protection framework.

NopSec's Unified VRM® empowers CrowdStrike Falcon Spotlight by providing holistic visibility, machine learning-based prioritization and vulnerability-based analytics for risk assessment.

KEY BENEFITS

Enables machine learning-based prioritization of endpoint vulnerabilities to augment CrowdStrike Falcon Spotlight data

Offers holistic visibility of vulnerabilities across infrastructure, endpoints and applications

Provides advanced vulnerability-based analytics and reporting capabilities to accelerate remediation

There are three primary use cases for Unified VRM. The first is for delivering global, holistic visibility that aggregates vulnerability data into a single dashboard so that customers do not have to log in to multiple systems to manage their overall VRM program.

The second is for vulnerability prioritization. Unified VRM's machine learning-based prioritization provides the context and business risk associated with each vulnerability.

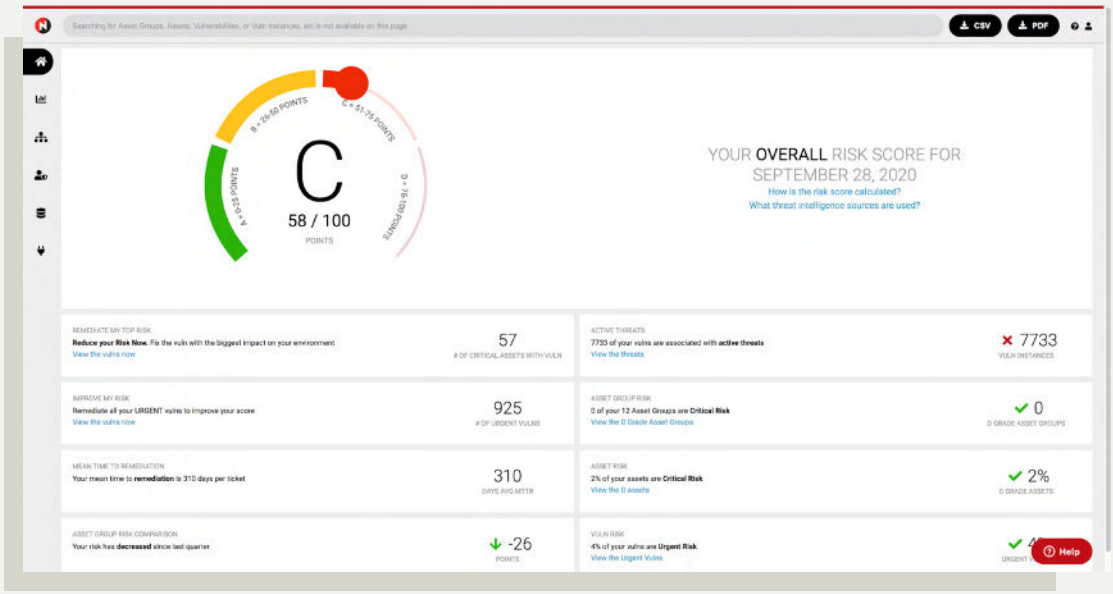
The third is for analytics and easy reporting — presenting the metrics and key performance indicators (KPIs) that matter to the VRM program. Unified VRM allows for customizable dashboards that translate vulnerability data and remediation trends into graphs and visualizations that communicate the health of the VRM program. This allows for better visibility to help customers improve the efficiency and efficacy of their VRM program. These dashboards allow you to view the processes across your VRM program and answer the question that many board members ask: Are we more secure today than we were yesterday?

BUSINESS VALUE

Use Case	Solution	Benefits
Data noise overload: Traditional vulnerability assessment (VA) scanners fulfilled compliance mandates but failed to deliver strategic value in complete visibility, remediation prioritization, and overall VRM program efficiency and effectiveness. VA scanners also create data overload and alert fatigue, making it difficult to extract actionable and timely context-rich intelligence.	**Visibility:** NopSec's Unified VRM aggregates infrastructure, endpoint and application vulnerabilities in one place with prioritized remediation based on your business and threat contexts. It dramatically reduces irrelevant data noise.	Gain holistic vulnerability visibility across infrastructure, endpoints and applications in one place.
Long time to remediate: Siloed process ownership across the VRM lifecycle creates misaligned objectives and priorities across Infrastructure, endpoint, security and application teams, and as a result, vulnerabilities take too long to remediate.	**ML-based prioritization:** Unified VRM's risk-based prioritization reduces noise and eliminates false positives and false negatives. It automates remediation workflow, orchestrates the remediation playbook, and automates patching and ticketing processes to fix critical exposures faster.	Prioritize the most important vulnerabilities to fix first across infrastructure, endpoints and applications.
Inefficient manual workflow: Manual processes using legacy tools lead to significant inefficiency and time waste in data collection analysis, prioritization and reporting.	**Analytics:** Unified VRM provides comprehensive program efficiency and effectiveness metrics, and benchmarking analysis compared to your peer organizations.	Easily assess trending metrics on your vulnerability management according to your industry's benchmarks. Access standard and custom reporting, key performance indicators (KPIs), service level agreement (SLA) metrics and more.

"The sheer volume of vulnerabilities makes it impossible to patch everything. The NopSec and CrowdStrike combination provides customers a holistic visibility of vulnerability intelligence across infrastructure and endpoints, and enables customers to prioritize remediation efforts based on risk and business contexts — giving customers world-class vulnerability program intelligence to stay ahead of the game."

Lisa Xu
Chief Executive Officer, NopSec



KEY CAPABILITIES

- **Vulnerability Risk Assessment:** NopSec analyzes billions of pieces of information to understand attacker activity in real time — what attackers are doing, how they're doing it and the tools they're using to exploit vulnerabilities in the wild. NopSec vulnerability risk is derived from hundreds of features and 30+ threat intelligence feeds for malware, ransomware, threat actors/campaigns, public exploit databases, social media and more.
- **Context and Prioritization:** Unified VRM ingests data about your environment to give context to each vulnerability. Then, the vulnerabilities found in your IT environment are reprioritized according to their risk and the criticality of the assets.
- **Data Agnostic:** Leverage the volumetric security data you already have from the investments you've already made in vulnerability scanners, endpoint data and other sources of security data. NopSec is a vendor-neutral risk management solution that is capable of ingesting and analyzing security data from a wide range of sources and transforming it into actionable intelligence.
- **Ticketing System Integrations:** Align security and IT teams around the common goal of reducing the most risk. Integration with popular ticketing systems ensures that both teams have the same level of actionable intelligence, so IT knows what to fix, how to fix it and why. Bidirectional communication and automated tracking keep security teams informed regarding progress on all tickets.
- **Full-Stack Risk Assessment:** Determine risk and prioritize remediation efforts across the organization with visibility into infrastructure, endpoint and application vulnerabilities in one place. Unified VRM provides organizations with full visibility and accurate, real-time, risk-based vulnerability prioritization across the organization's full stack.
- **Peer Benchmarking:** Make more informed decisions about your security programs by comparing your risk posture with that of your industry peers.

ABOUT NOPSEC

NopSec's Unified VRM® is an award-winning SaaS product that provides a complete end-to-end vulnerability risk management platform, from machine learning-based prioritization, to remediation automation and orchestration. Unified VRM utilizes passive analysis, active validation and contextual enrichment to enable security teams to visually forecast threat risk and dramatically reduce the time to remediation for critical security vulnerabilities across infrastructure, endpoints, and applications, and provides program metrics to executive stakeholders.

Forrester has named NopSec's Unified VRM as a leading vendor for two years in a row. Gartner frequently named NopSec as Innovator in the space. To learn more, visit **www.nopsec.com** or email **Sales@nopsec.com**.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**