NEW UNIFIED VRM
Converging Machine Learning and Offensive Security for Intelligent Prioritization
NopSec empowers organizations to make more informed risk decisions.

Unified VRM consolidates and prioritizes risks, putting an end to vulnerability fatigue. Integration with IT products improves communication and workflow between IT and Security teams. The result? Dramatically reduced remediation times, reducing exposure to critical vulnerabilities.

For more information, email us at hello@nopsec.com.
Unified VRM
See more. Prioritize. Fix faster.

Have questions about your vulnerabilities? NopSec has answers. Unified VRM can analyze massive amounts of vulnerability data and zero in on the few issues that represent real risk for your organization. This allows you to quickly identify and address major risks, while safely postponing less important issues.

STREAMLINED PEACE OF MIND

**Prioritization:** Before an analyst ever lays eyes on the data, Unified VRM analyzes imported vulnerabilities, removes false positives and prioritizes the results.

**Automated Assignments:** In many organizations, the task of assigning vulnerabilities to asset owners is a manual process. Unified VRM handles this process automatically - reducing manual, repetitive tasks.

**Our Innovations; Your Workflow:** Our strategic integrations mean that Unified VRM extends beyond simply making sense of vulnerabilities. Thanks to ITSM integrations, tasks can be assigned in industry-standard ticketing systems like Jira, ServiceNow and Remedy. Unified VRM can also select the correct patches and queue them up in patch management solutions like Microsoft SCCM.

**Reduced Noise:** Unified VRM automatically deduplicates vulnerability data and is intelligent enough to create a single ticket (rather than hundreds or thousands of duplicates) when a single vulnerability spans multiple assets controlled by a single owner.

**Powerful Search and Filtering:** Unified VRM makes it easy for analysts to find what they’re looking for.

**Flexible Reporting:** Report on data by group or owner - vulnerability or host. Export raw data for import into other tools or export PDFs for more formal uses.

VISIBILITY · SPEED · AUTOMATION
Our third party integrations are strategically focused to automate the most repetitive and time-consuming tasks related to vulnerability management. These currently include ticketing and patch management.

**Ticketing Automation**
Unified VRM can automatically create tickets, assign them to the correct parties and validate remediation work when tickets are closed in external systems. In many organizations, a full-time resource is often dedicated to this task. Not with Unified VRM.

**Patching Automation**
Unified VRM can identify and isolate the specific patches related to a vulnerability, download them and create deployment packages. All that’s left is for the patch administrator to deploy the packages - we do everything else.

**E3 ENGINE**
Systems report that patches have been applied, but is that really true? Perhaps the issue really has been fixed, or perhaps it is still vulnerable, because the patch only takes effect after a reboot. E3 Engine can provide a ‘second opinion’ by directly validating that the vulnerability no longer exists. It does this by safely simulating attacks against the affected resources. This makes it possible to drastically reduce false positives and further facilitates prioritization.

**AUTOMATED WORKFLOW**

**GOOD**

**YOUR OVERALL RISK IS:**

34 / 100 POINTS

AUG 8, 2018