WHITE PAPER

NopSec Unified VRM - Security and Governance

The Measures NopSec Takes to Ensure Customer Data is Secure and Complies with Regulations

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

NopSec is a security company founded and run by experienced security professionals. We understand that a poorly designed and managed security product could just as easily become part of the problem it is designed to address. As a software-as-a-service (SaaS) vendor, we are aware of our responsibility to protect our customers' data. It is easy for a software vendor to get caught up in customer requests, sprints and production deadlines.

Our penetration testers see this on a regular basis. That is why, with our products, we have baked security into our designs and processes. Security is not a point-in-time check for us - it is a question and concern at each step of the way. We choose to consider security with each minor release, every customer onboarding, and every new feature implemented. Even if, following a proof-of-concept with our product, you do not choose us, we will make sure your data is securely deleted so you do not have to worry.

The remainder of this datasheet provides an overview of how NopSec addresses security relating to our products and the handling of customer data.

People and Policies

Experienced Security Experts

NopSec was founded by security experts and employs experienced practitioners with skills critical to ensuring the security of Unified VRM and customer data. Our developers and engineers are trained in secure coding practices and have integrated security into their workflows. As proven in many studies, addressing security as early as possible in the software development lifecycle (SDL) minimizes the cost and effort necessary to produce secure software. Our in-house services team includes experienced penetration testers that NopSec leverages to identify and fix any security issues missed earlier in the development lifecycle

Unified VRM Design and Architecture

Unified VRM leverages the Django web framework and benefits from its excellent integrated security features. The customer-facing components of Unified VRM run in AWS, leveraging many of the available high availability, security, key management and monitoring products in Amazon's public cloud.

Unified VRM leverages a Linux-based appliance to perform internal scans, integrate with on-premises data sources (e.g. Jira, Tenable Security Center) and perform vulnerability validations with our E3 Engine. This appliance communicates with the cloud instances of Unified VRM via an HTTPS tunnel and a REST-based API endpoint. This appliance can be configured to use an internal proxy, if necessary for outbound HTTPS communication. The appliance is pre-hardened and is managed, patched and updated automatically.

Meet Django

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of Web development, so you can focus on writing your app without needing to reinvent the wheel. It’s free and open source.

Ridiculously Fast

Django was designed to help developers take applications from concept to completion as quickly as possible.

Reassuringly Secure

Django takes security seriously and helps developers avoid many common security mistakes.

Exceedingly Scalable

Some of the busiest sites on the Web leverage Django's ability to quickly and flexibly scale.

Data Security

Customer Data and Third-Party Data Requests

The Personally Identifiable Information (PII) used by Unified VRM is limited to what is necessary for customers to use the product. The accounts and roles are defined within the product based on customer need to analyze the results of scans, gauge risk exposure and prioritize remediation. The only PII collected includes the names, email addresses, and departments of individuals with access to Unified VRM.

In addition to PII, NopSec may also collect and store customer vulnerability data, asset configuration data, patch information, service tickets and other proprietary IT asset information depending on integrations used by customers.

NopSec will not disclose customer data to a third party (including law enforcement, other government entity, or civil litigant) except as directed by the customer or required by law. Should a third party contact NopSec with a demand for customer data, NopSec will redirect the request to the customer. Publicly listed contact information will be provided unless separate contact information is provided specifically for this purpose. If required

by law to disclose customer data to a third party, NopSec will attempt to notify the customer in advance unless legally prohibited from doing so.

Outside of the aforementioned legal scenarios, customer data is never shared with third parties or partners without explicit permission.

Data at Rest

Unified VRM encrypts customer data on a per customer basis. Customer data is protected by symmetric encryption using AES with 256-bit key sizes. During the onboarding process, a customer-specific secret key is generated and stored. When the customer logs into Unified VRM, the key is decrypted and stored in memory only. Each database query must be decrypted using this key.

Row-level encryption is used in the database to protect customer data. Fields encrypted include customer PII, vulnerability data, IP addresses and host information.

Authentication

Unified VRM leverages the authentication and password management features built into Django (https://docs.djangoproject.com/en/2.1/topics/auth/passwords/). Strong passwords are enforced using the widely-used Cracklib library to test them (https://github.com/cracklib/cracklib). Integrations use either API keys or credentials, both of which are encrypted and stored in the database.

Key Management

Unique keys are created for each customer. Keys are created and stored in a Gemalto (SafeNet) HSM. There is no direct human access to the secret key at any point in time. It

is a split-key system with one key in the HSM and the other decrypted and loaded into memory from a different location. Processes exist to rekey customer data if a compromise is suspected or if requested by customers. The process used to do this is available upon request.

Data in Motion

All communication is encrypted using HTTPS. Currently, Unified VRM supports only TLS 1.2 with the following ciphers (listed in server-preferred order).
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) TLS_RSA_WITH_AES_256_CBC_SHA (0x35)
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)

Data Lifecycle

NopSec secures customer data throughout the entire lifecycle, starting with the first customer-unique encryption key that is created during onboarding. When the relationship with a customer comes to an end, we ensure customer data is securely deleted.

Availability & Resilience

NopSec utilizes AWS products and features to make Unified VRM highly scalable. Load balancers and auto-scaling application servers provide speed on the front-end, while a multi-tenant architecture with a redundant, scalable database round out the back-end. AWS CloudWatch is used to monitor instance availability.

Security Operations

In addition to the previously mentioned preventative security features, controls, and processes, NopSec is prepared to detect and respond to attacks as well. Incapsula's WAF (web application firewall) service addresses application-layer attacks and threats. AlienVault USM is used to detect and respond to network-based attacks and threats. AWS CloudWatch enables NopSec to monitor for cloud-native anomalies and threats.

Incident Response and Vulnerability Disclosure

NopSec employs experienced incident handlers and follows a tested and proven methodology.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com