NOPSEC

# Managed Scanning Service

## All of the Benefits of Vulnerability Scanning, Without the Cost and Administrative Burden

For organizations looking to outsource their vulnerability management scanning, NopSec offers the Managed Scanning Service. Through our dedicated Qualys instance, NopSec delivers both scanning and asset group management customized for your environment. We can accommodate either scanner-based or agent-based vulnerability scanning and offer this across any size network whether it be a few branches with several hundred assets to an international setup with networks around the world covering hundreds of thousands of assets.

## What does the **Managed Scanning Service** include?

The Managed Scanning Service encompasses the three core areas of vulnerability scanning – infrastructure and web app scanning, asset management, and reporting. Below you'll find the specifics of what NopSec offers in each area:

### Infrastructure Scanning

- Qualys agent deployment
- Qualys scanner virtual appliances
- External network scanning
- Vulnerability reporting
- Scan configuration
- Scanning automation
- Troubleshooting

### Web App Scanning

- Scan configuration
- Scan automation

### Asset Management

- Asset group creation
- Asset group management
- Asset tagging

### Reporting

- NopSec UVRM scanning insights
- How many of your assets got scanned
- How many assets were on the network during the time of scanning
- Weekly vulnerability remediation count
- Weekly newly found vulnerability count

## Why should you outsource your vulnerability scanning?

Next is a snapshot of the benefits and return on investment when outsourcing your vulnerability scanning to NopSec's seasoned team of professionals:

### Be operational in days, not months

- The average time to operationalize a vulnerability scanner for a large well-staffed organization is between 3 and 6 months depending on complexity.
- NopSec's team of professionals will have you set up, scanning, and reporting within a matter of days.

### Fraction of the cost, the same quality of scanning

- On average, the minimum purchase price of a vulnerability scanner for any simple environment of larger than 1000 assets is $10,000. This cost can exponentially grow as environment complexity and asset count increase.
- The outsourcing of this critical security function to NopSec is usually a fraction of this price.

### Save on 2-4 full time employees (FTEs), roughly 300K per year in salaries

- Set up, management, and upkeep of a vulnerability scanner and all of the associated asset organization is no small feat. With NopSec's Managed Scanning Service you can expect to save on the following mandatory head counts necessary to run a vulnerability scanning operation:
- **1-2** Vulnerability Management Technician(s) to manage scanning configuration and asset grouping
- **1** Network Technician to oversee VM server creation, maintenance, and troubleshooting
- **1** Data Scientist /Database Administrator to handle reporting and data warehouse setup

## What is NopSec's process for managing your VM scanning?

The steps below will walk you through how NopSec will onboard your organization and get your customized vulnerability scanning underway:

- We'll start by going over your network layout and team overview. We first need to understand how your network is organized and what teams are responsible for both the management and patching of specific assets, as well as any current processes that exist.
- Then we'll recommend best practices and help your teams to create any policies they may need to help your vulnerability management.
- Next, we'll begin the scanner implementation by creating asset groups and tags based on what makes sense from both a scanning and reporting perspective (can be updated when needed).
- Following the creation of the asset groups, we'll determine what type of scanning (agent based, appliances, or hybrid) will work best for your current network layout. Once determined, we'll configure our scanner according to the entire organization's need (can be updated when needed).
- If we've chosen to go with an appliance or hybrid approach, we'll find a scanning schedule best suited to your organization based on factors like time zones, patch cycles, and reporting schedules to best optimize.
- With configuration complete, we will set up reporting for both individual teams and for leadership based on the groups we set earlier and your environment as a whole.
- Finally, after a few weeks to months, we perform a re-evaluation of the scanning setup to determine how it is performing for both your security and infrastructure teams. We'll look for opportunities to further automate functions to make your team's jobs easier.

## What will this service cost you?

Pricing varies depending on the number of assets we'll be scanning and the complexity of your environment.

To learn more about NopSec's Managed Scanning Service contact a sales representative today!

**www.nopsec.com** | **info@nopsec.com**