

The Opware Network

The Opware Network for Opware Network Automation System (NAS) is a new, optional subscription offering that provides customers with additional functionality to maximize their return on investment in their network automation solution. It leverages the extensible NAS automation platform to deliver new automation capabilities on an ongoing basis.

The service will initially provide the following capabilities:

- 1. Receive actionable security alerts** – The Opware Network for NAS provides a one-of-a-kind security service that delivers network security vulnerabilities. Unlike traditional alerts that are typically delivered via email and therefore very hard and very time consuming to act on, these alerts are delivered as actionable NAS compliance policies that allow customers to quickly identify all vulnerable devices on their network and rapidly remediate them before any hackers can compromise their security
- 2. Leverage new automation capabilities on an ongoing basis** – The Opware Network for NAS leverages the extensible NAS automation platform to deliver new automation capabilities on a weekly basis. These capabilities include deeper automation scripts for specific technology areas, NAS product extensions and integration with commonly used network analysis utilities. They are delivered in the form of Solution, Extension and Integration packs. Examples of automation packs that could be included are Dynamic Groups, Voice over IP (VoIP) management, Advanced ACL management and Multiprotocol Label Switching (MPLS) management.

Since The Opware Network for NAS is a subscription service, it allows customers to leverage new automation capabilities as and when they are available. Customers access The Opware Network for NAS by logging on to a secure, password-protected website via the Internet.

Security Alert Service

Traditionally, vendors have delivered security vulnerability alerts via email making them very hard and very time consuming to act on. In today's highly networked environments, hackers attack customer networks and compromise their security often within minutes or days of a vulnerability announcement. Consequently, the most pressing concerns facing customers today are the time-to-resolution on breaking vulnerabilities and the assurance that all vulnerable devices on their network have been remediated. Furthermore, customers want to know that their network won't be prone to future attacks of known vulnerabilities as a result of any

Key Benefits

Security Alert Service

Automatically delivers network vulnerability alerts as actionable policies to enable rapid identification and remediation of all vulnerable devices on the network

New Automation Packs

Leverages the extensible NAS automation platform to deliver new automation capabilities every week in the form of Solution, Extension and Integration packs

Opware Community

Provides an online forum for sharing of automation content and best practices with other customers

regression in their existing environment or because a new device with a known vulnerability was added to their network. Unfortunately, today's vulnerability management solutions don't effectively address these concerns.

In response to these challenges, The Opsware Network for NAS delivers a unique Security Alert Service that provides customers with actionable alerts on new vulnerabilities. This allows customers to quickly identify all vulnerable devices on their network and rapidly remediate them. The

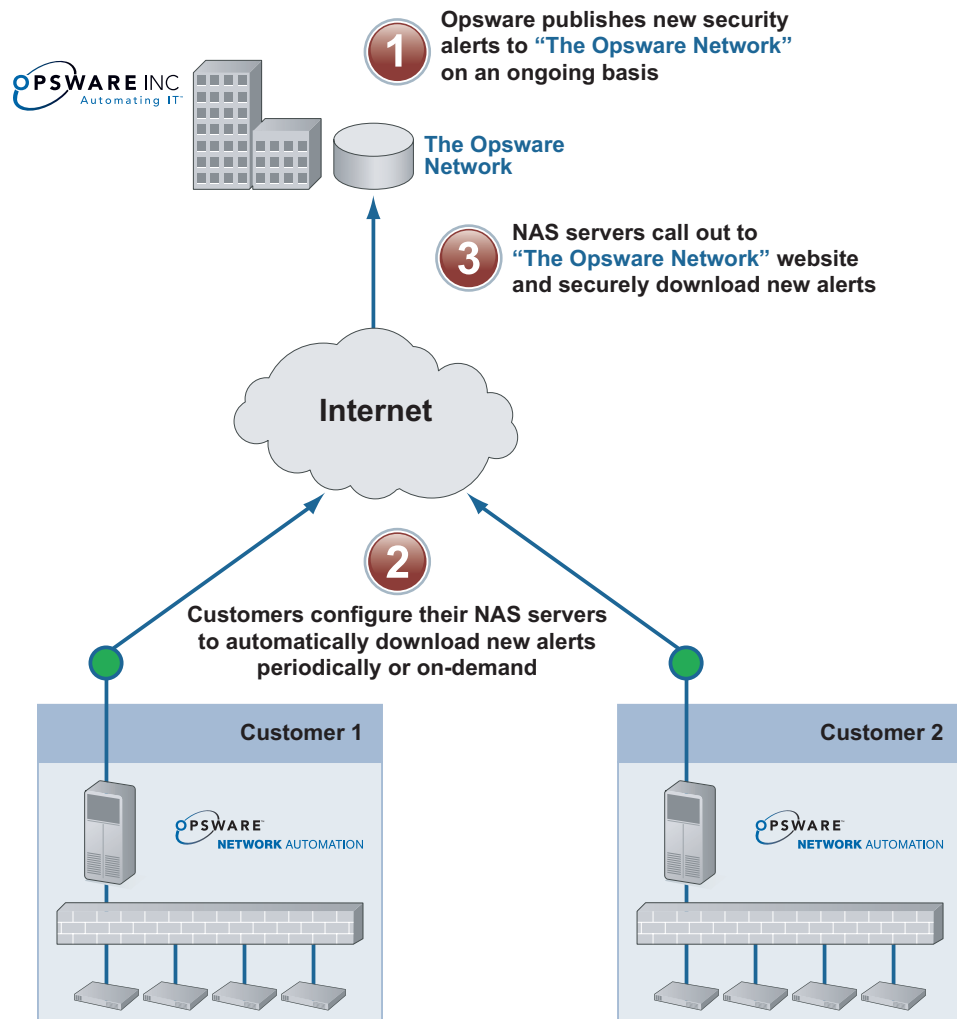


Figure 1: A high-level overview of how the Security Alert Service works

vulnerability alerts are packaged and uploaded onto The Opsware Network website in the form of NAS compliance policies. Customers configure their NAS server to either automatically download the new alerts on a periodic basis or perform the download on-demand. When the NAS server calls home to The Opsware Network, it downloads all new alerts that have been uploaded to the website since the last download. These alert policies include rich details on the vulnerabilities such as detailed descriptions, disclosure dates, severity levels and remediation solutions.

Once these alerts are downloaded onto the NAS server, customers can quickly and easily run a compliance check to identify all vulnerable devices on their network. After the vulnerable devices are identified, customers can configure NAS to remediate these devices concurrently. Typically, the remediation process involves a device software update, specific changes to configuration files or both. Besides providing alerts on new security vulnerabilities, The Opsware Network for NAS also includes historical alerts for the past 13 years across all supported vendor platforms. Since all new and historical alerts are delivered as software compliance policies, if a vulnerability is accidentally reintroduced into a customer's network in the future, NAS will immediately notify them of this event and help rapidly remediate the situation.

Anyone who has used traditional methods to identify and remediate security vulnerabilities will appreciate the inherently manual nature of this task that renders it very time-consuming, labor-intensive, expensive and unreliable. Using the Security Alert Service feature of The Opsware Network for NAS, customers can easily, reliably and rapidly remediate all vulnerable devices on their network. The Opsware Network for NAS provides an unparalleled security alert service that addresses the vulnerability management challenges of today's highly networked environments.

New Automation Capabilities

The Opsware Network for NAS leverages the extensible NAS automation platform to deliver new capabilities on a weekly basis. They are delivered in the form of Solution, Extension and Integration packs.

Solution packs are in-product automation content that leverage powerful NAS objects such as Advanced Command Scripts, Policies, Advanced Diagnostics and Event Response Rules to enable deep automation capabilities for specific technology and solution areas. Examples of solution packs could include Dynamic Groups, Cisco IOS Dynamic Syntax Checker, Voice over IP (VoIP) management, Advanced ACL management, and Multiprotocol Label Switching (MPLS) management.

Extension packs provide new capabilities by leveraging the extensible NAS platform with external add-on components. Examples could include a pack that converts NAS HTML reports to PDF format and a pack that allows configuration information to be exported from the NAS database for use in other scripts and other systems.

Integration packs enable seamless integration between NAS and well-known and commonly used network management tools. Examples of integration packs could include Cricket, Cacti and Router Audit Tool.

A new automation pack is made available each week on The Opsware Network website. Customers can download these packs and install them on their NAS server to immediately start leveraging the new functionalities. Each automation pack includes detailed instructions on its capabilities, usage and installation.

Opsware will elicit customer feedback on a regular basis on the automation packs that have been released. In addition to that, if customers have ideas for new packs, they can send an email to tonadmin@opsware.com.

THE OPSWARE NETWORK OVERVIEW

Automated download of security alerts

Configures customer's NAS server to automatically download new security vulnerabilities on a periodic basis

Automatically obtain the latest security vulnerability information rather than depending on a manual and error-prone process

Alerts delivered as actionable policies

Delivers security vulnerabilities as NAS compliance policies that automatically run vulnerability tests to identify affected network devices

Automatically identify all vulnerable devices in minutes rather than depending on a manual, error-prone and time-consuming process

Remediation of all vulnerable devices concurrently

Provides the remediation solution as part of compliance policy that can be pushed out to all vulnerable devices simultaneously

Remediate all vulnerable devices on the network concurrently by either performing software updates, making required configuration changes or both

Compliance policies are tied to the Event system

Automatically generates an alert when network devices don't comply with NAS compliance policies

Automatically alerts when a vulnerability is reintroduced either due to a regression in the existing environment or the addition of a new vulnerable device to the network

Historical alerts across all supported vendor platforms

Delivers historical alerts for the past 13 years across all supported vendor platform

Ensure that network devices aren't exposed to known historical vulnerabilities

New automation packs every week

Delivers new automation capabilities on an ongoing basis in the form of Solutions, Extensions and Integration packs

Leverage new automation capabilities every week

Provides unique sharing opportunities

Provides an online forum for sharing of automation content and best practices with other customers

Help other customers with the common pains associated with adoption of IT automation and help foster industry best practices for network automation

Field extensions shared exclusively

Delivers unique product extensions that were created in the field for other customers as new automation content

Leverage unique product extensions as new automation content



Corporate Headquarters
599 North Mathilda Avenue Sunnyvale California 94085 USA
T 408.744.7300 | F 408.744.7383 | www.opsware.com