FORWARD NETWORKS

USE CASE

OS Vulnerability and Exposure Management

Responding to Common Vulnerabilities and Exposures (CVE) alerts could easily be a full-time job for security operations professionals. Unfortunately, even though bad actors are hyper-focused on ways to exploit any security gap to gain a foothold in the enterprise network, remediating these alerts often falls to the back burner in favor of seemingly more urgent issues.

CVE remediation isn't deprioritized because security teams don't understand the value, rather it happens because network complexity is growing exponentially; the average enterprise network now hosts tens of thousands of devices from dozens of vendors running billions of lines of code. The seemingly constant stream of CVE alerts is becoming an overwhelming task for most IT organizations.

Some organizations have entire teams dedicated to tracking and remediating CVE risks, and even they have struggled to stay current because it's difficult to share prioritized, actionable information in a manner that is easy for NetOps to understand and act on.

While many organizations do regularly scan the network for vulnerabilities, they are only able to scan the network at night and it can take almost a week for the information revealed in the scan to be transferred to the network engineering team. Even when the network team receives the information, it's a raw report lacking specificity (e.g. which alerts are new). For protocol-specific alerts, engineers will still need to locate impacted devices within the network to evaluate if there is a risk. Without this level of detail, the process is still time consuming and potentially prone to human error.

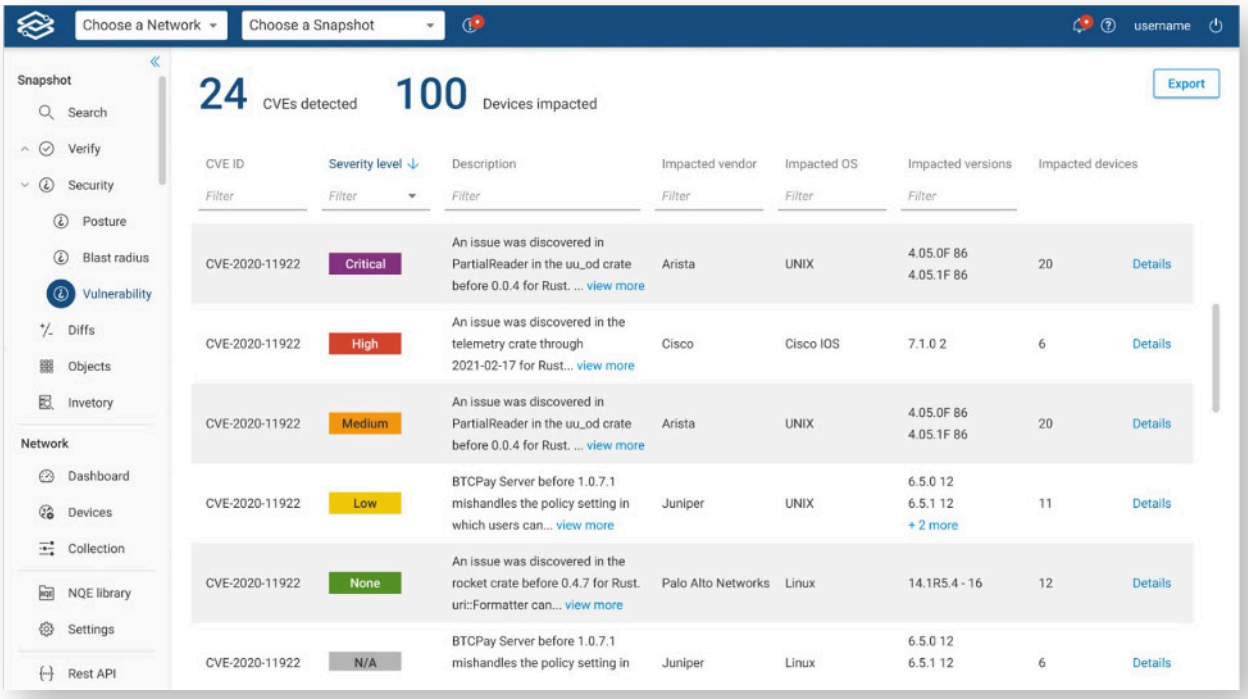
Know the What, Where, and "How Bad?" of CVE Alerts at a Glance

Forward Networks recognized that there was a better way for our customers to manage CVE alerts to protect their security posture and reduce the burden on IT staff.

The Forward Enterprise platform now features operating systems (OS) vulnerability mitigation functionality. It uses information from the NIST National Vulnerability Database and the specific device and configuration data we collect from your enterprise network to automatically analyze the network for vulnerabilities. It presents that information in a vendor-agnostic, actionable format for your security and network engineers.

The example dashboard below shows how the OS vulnerability mitigation functionality in the Forward Enterprise platform provides pertinent details about CVE alerts that apply to an organization's specific network(s) at a glance. This information includes:

- CVE IDs
- The severity level of the alerts (from critical to N/A)
- A description of each alert
- The vendors impacted by the alert
- The OSes impacted by the alert
- Which versions of software are impacted
- How many devices in the network are impacted



From this interface, security and network teams can click on “Details” to view full configuration and state information for impacted devices. Using the Network Query Engine within Forward Enterprise, engineers can run a query to locate devices running protocol-specific alerts and immediately determine their risk and begin remediating it.

With up-to-date vulnerability insights automatically curated within the Forward Networks enterprise platform, security and network teams can act fast to prioritize and fix severe vulnerabilities. Just as important, they can easily decide which CVE alerts present the least security risk, so they can ensure they’re devoting their resources to the most critical fixes first — and feel confident that they’re not putting the organization unnecessarily at risk by postponing responses to other, less-critical alerts.

API Integration with ServiceNow

Forward Networks' API integration with ServiceNow can automatically generate tickets that automate the entire process of addressing OS vulnerabilities in response to CVE alerts, further reducing the burden on IT teams. It takes only seconds to enable and configure this integration. Engineers can automatically share relevant details about network state, configuration, and behavior with everyone working to resolve a security or compliance issue. This information automatically updates within both platforms, creating a detailed and current single source of truth.

Case Study

Right before Christmas 2020, Cisco sent out a field notice that announced a major issue with many of its network devices. Due to a bug with expiring self-signed certificates on Cisco devices, many services and capabilities relying on those certificates would no longer function.

This was a critical announcement, as the services impacted included SIP connections, encrypted signaling, gateway calls using MGCP or H.323 signaling, API calls, RESTCONF, HTTPS sessions, SSL VPN sessions, IPSec connections, and much more. Essentially, chief functions of the network — including basic internet browsing — would be significantly affected. The process to identify all the affected devices could easily represent weeks of work for impacted engineers.

Forward Networks' customers received an automatic update about this field notice and turned to the Network Query Engine (NQE) in our platform to create a custom query so that they could identify the impacted Cisco devices and report them to the network security team within hours.

Analyze Network Vulnerabilities With Mathematical Certainty

Forward Networks is the industry leader in network assurance and intent-based verification. Our mathematical model creates a complete and always-current digital twin of your physical, virtual, and cloud network estate including config and state information for all devices. The digital twin provides a complete view of all network behavior, with visibility into every possible path in your network. It brings mathematical certainty to security teams' analysis of network vulnerabilities by enabling them to:

VISUALIZE network layer 2 – 4 topology and all possible traffic paths within a single-pane view for on-premises, cloud (AWS, Microsoft Azure, and Google Cloud Platform), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data.

SEARCH the network as simply as a database. Our browser-like search feature performs complete end-to-end path analyses across the network for both on-premises and cloud infrastructure. This enables you to locate devices and access detailed information on their location, configuration, and state in milliseconds.

VERIFY that the security controls in the network are working as intended by using purpose-built (custom) intent checks. Continuously audit the network and receive actionable alerts for noncompliance with your security policies.

PREDICT the effect of proposed changes, so you can deploy updates without the fear of unintended connectivity changes by using the network digital twin as a sandbox.

COMPARE network changes over time to understand their impact on the network and prevent incidents from reoccurring. The network collector frequently scans the network, taking and saving snapshots of network configurations, topology, and device state. These "snapshots" become a searchable historical record of network behavior and compliance at any point in time. And the behavior diffs feature makes it easy to quickly find and compare snapshots to identify changes that may violate your security policy.

See for yourself how the network OS vulnerability mitigation functionality in the Forward Enterprise platform can help your security and network teams collaborate more effectively on CVE alerts. Your teams can identify and fix affected devices faster, so that your network — and organization — can be more secure. Request a demo to enhance your security posture!

Getting Started With Forward Networks

Are you ready to deliver new capabilities through the network, reduce outages, enhance security, and save time?

Request a personal demo ›

FORWARD NETWORKS

www.forwardnetworks.com