FORWARD NETWORKS

USE CASE

CVE Vulnerability and Exposure Management

Gaining Useful Visibility into CVEs Across Agency Environments

Forward Networks meets the challenges agencies face head-on as they encounter operating system vulnerabilities across distributed, complex hybrid environments. The Forward Enterprise network digital twin offers visibility and attack intent capabilities for the entire agency network estate. The at-a-glance insight available through the platform is critical for agency environments in which the sheer number of vulnerabilities arising each day can quickly outpace IT teams' ability to respond.

The Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities, is driving progress around remediation of vulnerabilities. The Directive's CISA-managed catalog of priority known exploited vulnerabilities is a step in the right direction for helping federal civilian agencies address mandates and remediate vulnerabilities within specific timeframes.

> *Every day, our adversaries are using known vulnerabilities to target federal agencies. We are using our directive authority to drive cybersecurity efforts toward mitigation of those specific vulnerabilities that we know to be actively used by malicious cyber actors. The Directive lays out clear requirements for federal civilian agencies to take immediate actions to improve their vulnerability management practices."*
>
> **Jen Easterly, CISA Director**

CISA is helping establish critical baseline priorities; however, the escalating volume of CVE alerts is still daunting. Increasingly complex, distributed environments with tens of thousands of devices from different vendors make it even harder for federal agencies to keep up with the constant stream of CVE alerts without becoming overwhelmed. As vulnerabilities increase, assessing and remediating alerts often fall to the back burner.

While many agencies regularly run network vulnerability scans, these processes typically run only at night. It can take almost a week for the information revealed to be transferred to network engineering teams. With this difficulty in sharing prioritized and actionable information, even when the team receives the reports, they are not in actionable form. For protocol-specific alerts, engineers will still need to manually locate impacted devices within the network to evaluate risk. Without this level of detail, the process remains time-consuming and prone to human error. A more automated, efficient approach is needed to prioritize threats and achieve CVE compliance both on-premises and in the cloud.

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

There is a better way for agencies to manage CVE alerts to protect their security posture and reduce the burden on their IT staff. The OS vulnerability mitigation functionality within Forward Enterprise helps agencies prioritize and remediate CVEs for compliance with CISA BOD 22-01.

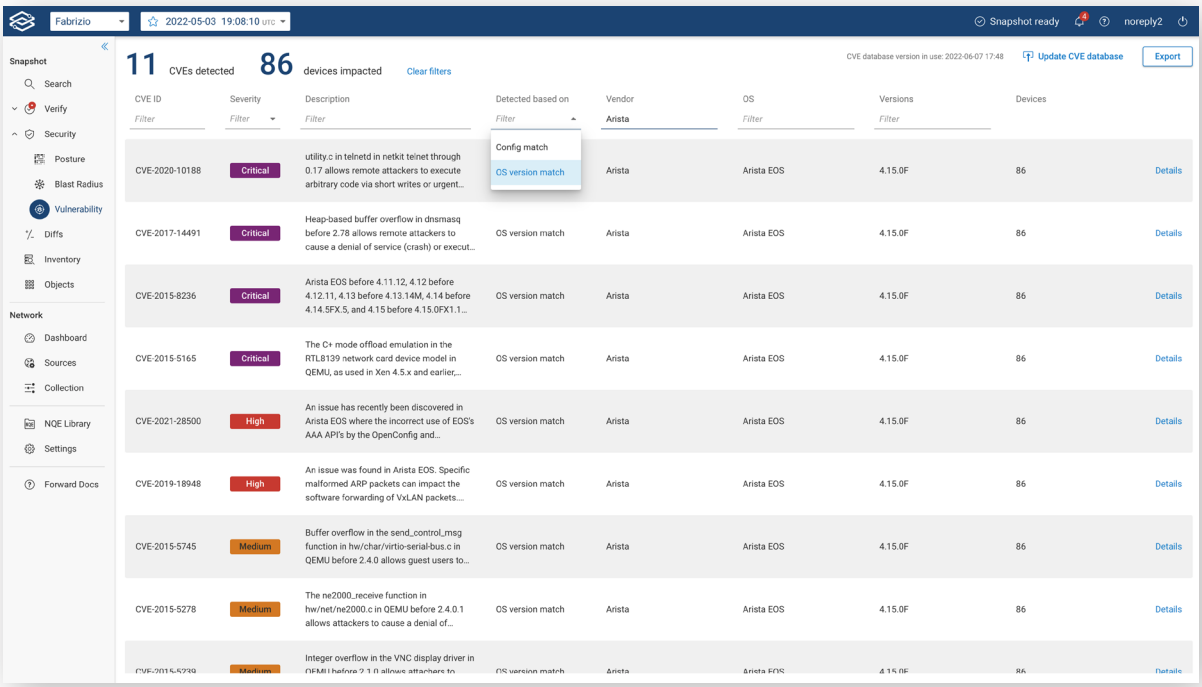
Forward Enterprise's network digital twin capability helps agencies respond to the growth of hybrid work and the need to secure collaboration and digital services within constantly evolving network boundaries. These complexities typically block understanding of network connectivity and obscure insight into whether security policies are working and which vulnerabilities pose the most significant risk.

Security and network engineers can manage and prioritize CVE alerts easily and confidently with Forward Networks. Visibility into on-premises, hybrid-cloud, private cloud, public cloud, and multi-cloud gives agency IT teams a 360-degree view of networks across physical and virtual environments. Teams also get a single pane of glass for end-to-end in-depth connectivity analysis and policy and security verification.

The operating systems (OS) vulnerability mitigation feature collects information from the NIST CVE database and automatically analyzes it against the device and configuration data collected by the network digital twin for an instant security data call for CVE remediation. In one dashboard, security operations teams can see all the key details about the latest CVE alerts — from the severity level of the alert to how many and which devices in an agency network are impacted – as well as what sources or subnets can reach the device to attack the vulnerability.

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 agency's specific network(s) at a glance. This information includes:

- CVE IDs
- Severity level of the alerts from critical to not applicable
- Description of each alert
- Vendors impacted by the alert
- OS impacted by the alert
- Which versions of the software are impacted
- How many devices in the network are impacted



The Forward Enterprise platform helps IT teams gain new efficiencies for vigilant CVE monitoring, making it easier to stay on top of recent vulnerabilities targeting remote workers and cloud-based communications software. With access to up-to-date, actionable vulnerability insights automatically curated within the platform, agency security and network teams can act fast to prioritize and fix severe vulnerabilities. This capability is especially important for agencies whose mission means handling sensitive information where any risk – no matter how small – is too much risk.

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

API Integration with ServiceNow

The ability to automate the monitoring of new NIST CVE alerts with detailed information for fast prioritization and remediation makes it easier for security and network teams to close those gaps before bad actors exploit them. Automated monitoring can help maintain compliance without overwhelming stretched staff.

Forward Networks' API integration with ServiceNow generates 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 updates within both platforms, creating a detailed and current single source of truth.

Case Study

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, the chief functions of the network, including basic internet browsing, would be significantly affected. Identifying all the affected devices could easily represent weeks of work for impacted engineers.

Forward Networks' users received an automatic update about this field notice. They turned to the Network Query Engine (NQE) from Forward Networks to create a custom query to identify the impacted Cisco devices and report them to the network security team within hours.

Analyze Network Vulnerabilities with Mathematical Certainty

Forward Networks' mathematical model creates a complete and always current digital twin of your physical, virtual, and multi-cloud network estate, including config and state information for all network elements and your hybrid or multi-cloud environment. The digital twin provides a comprehensive view of all network behavior, with visibility into every possible path a packet can take. It brings mathematical certainty to network security validations by enabling security operations teams to:

VISUALIZE network layer 2 – 4 topology and all possible traffic paths within a single pane of glass including on-premises, Cloud (AWS, GCP, and Microsoft Azure), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data. View the global network in a single view or drill down to a single device.

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

VERIFY that the security policies are extended to the cloud using purpose-built (custom) intent checks. Forward Enterprise offers the most advanced network segmentation tool available with support for multi-vendor on-prem, hybrid-cloud and multi-cloud environments. Continuously audit the network and receive actionable alerts for non-compliance with your security policies. Know that applications are compliant before provisioning them.

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 network configurations, topology, and device state snapshots. 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.

Get Started with Forward Networks

Are you ready to help your security and network teams collaborate more effectively on CVE alerts and reduce the time that limited resources are dedicating to meet new CVE directives? Forward Networks can help you realize cost savings and efficiencies that are hard to achieve as complexity and vulnerabilities increase across on-premises and multi-vendor clouds. Our single source of truth with automated analysis introduces a new approach to visualize, verify, search, and predict network behaviors with game-changing speed and efficiency.

See how Forward Enterprise's network OS vulnerability mitigation functionality can help your teams identify and fix vulnerabilities fast for a more proactive approach to securing mission IT. Learn more at forwardnetworks.com/network-security and contact us at forwardnetworks.com/federal.

ABOUT FORWARD NETWORKS

Forward Networks' mission is to de-risk and accelerate network operations by increasing efficiency, reducing outages, and verifying network intent. Built on a series of breakthrough algorithms, the Forward Platform provides enhanced network visibility, policy verification, and change modeling for legacy, SDN, or hybrid environments.

Forward Networks is headquartered in Santa Clara, California, and funded by top-tier investors, including Andreessen Horowitz, DFJ, A.Capital, SV Angel, and several luminaries in the networking and systems space.