FORWARD NETWORKS



SOLUTION GUIDE

A Simple Path to BOD 23-1 Compliance

Growing Cybersecurity Requirements

Cybersecurity has been top of mind for federal agencies in the past year. From Executive Order 14028, Improving the Nation's Cybersecurity, to CISA's Binding Operational Directive, 23-1, there is increasing oversight and scrutiny on federal networks' ability to protect themselves from attack. The expectation is that leaders will be accountable for ensuring the entire hybrid, multi-cloud network is secure and in compliance with security policies.

At the same time, Gartner believes that cybersecurity professionals are losing control in a highly distributed ecosystem. This is because the sheer number of devices, vendors, and protocols in place makes it virtually impossible to document network behavior or prove that the constant changes and updates taking place within the network are not degrading compliance. Using siloed security tools or vendor-provided applications doesn't deliver an accurate assessment of the security posture. Furthermore, the process of collecting and analyzing the necessary data is cumbersome and time-consuming, requiring deep knowledge of multiple platforms and solutions. In an era plagued by a security talent shortage, this is untenable.

CISA BOD 23-1

Binding Operational Directive (BOD) 23-1 states that "continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage cybersecurity risk." Yet due to the multi-vendor nature and sheer size of agency networks, this is difficult to achieve. Most agency networks are comprised of tens of thousands of devices from dozens of vendors running billions of lines of code; understanding the complexity of these environments is beyond the scope of human comprehension.

Forward Enterprise supports all major hardware vendors, public cloud vendors, and protocols and is proven to support over 50,000 devices per instance. The result is broad deep data that helps engineering teams improve their security posture.

ALL THE VENDORS

27 Vendors | 35+ Operating Systems | 3 Clouds | 900+ OS Versions

ALL THE PROTOCOLS

MPLS | IPSec Tunnels | Segment Routing | Policy Based Routing | Multicast | FrabricPath
VRF | VXLAN| GRE | IPV6 | ARP | MAC | IPv4 Routing

COLLECTED AT FULL SCALE

500k devices and beyond!

Streamlined BOD 23-1 Compliance

The Cybersecurity and Infrastructure Security Agency (CISA) issued BOD 23-1 to enhance visibility into agency assets and vulnerabilities. This measure is intended to support CISA's efforts to effectively manage cybersecurity for the Federal Executive Branch (FECB) enterprise. CISA has stated that "comprehensive asset visibility is a basic precondition for any organization to effectively manage cybersecurity risk."

The BOD requires Federal Agencies to perform automated asset discovery every 7 days and vulnerability enumeration every 14 days. Due to technical limitations, legacy scanning tools cannot support agencies' efforts to adhere to this directive. These tools take several days to perform a scan that reaches all network endpoints. This also assumes the organization fully understands their IP address space, both IPv4 and IPv6. Also, they can allow scans through firewalls or deploy probes, if necessary, onto air-gapped environments to reach areas of the network separated by administrative boundaries.

Comprehensive Collection on Your Schedule

Forward Enterprise compliments the array of the array of security to provide several network device discovery techniques (subnet scan, CDP/LLDP, and seed device) to collect an entire network in under an hour with zero performance degradation. Discovery can be performed multiple times a day to identify missing devices and ensure they are discovered and included in future collections. Once the device list collection from the network is completed, compliance is as easy as setting a schedule. Collections can also be run on demand to meet the directive requirements. See Figure 1.

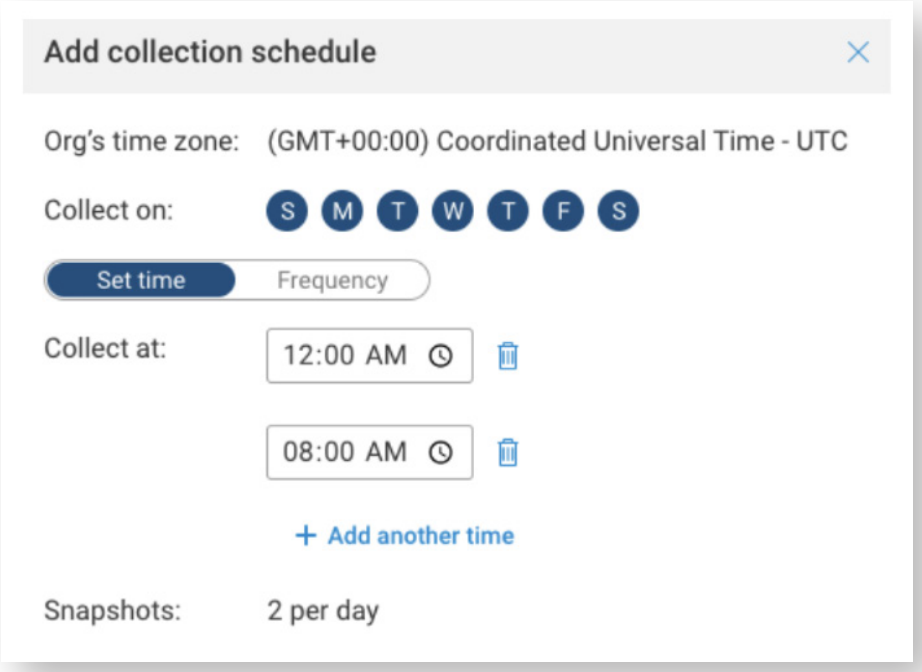


Figure 1: Setting Collection Schedules

All the information from the network devices is then extracted and presented in a vendor-agnostic, normalized view that provides full visibility into all the end points on the network. Forward Enterprise includes the ARP and MAC tables on network devices in the hosts portion of the data model. This includes all the relevant information about an end point as the network sees it, e.g. device, interface, addresses, VLANs, and gateways. The reports are customizable, built in an easy to use query language, and exportable via the UI and API. See Figures 2 and 3 for example reports.

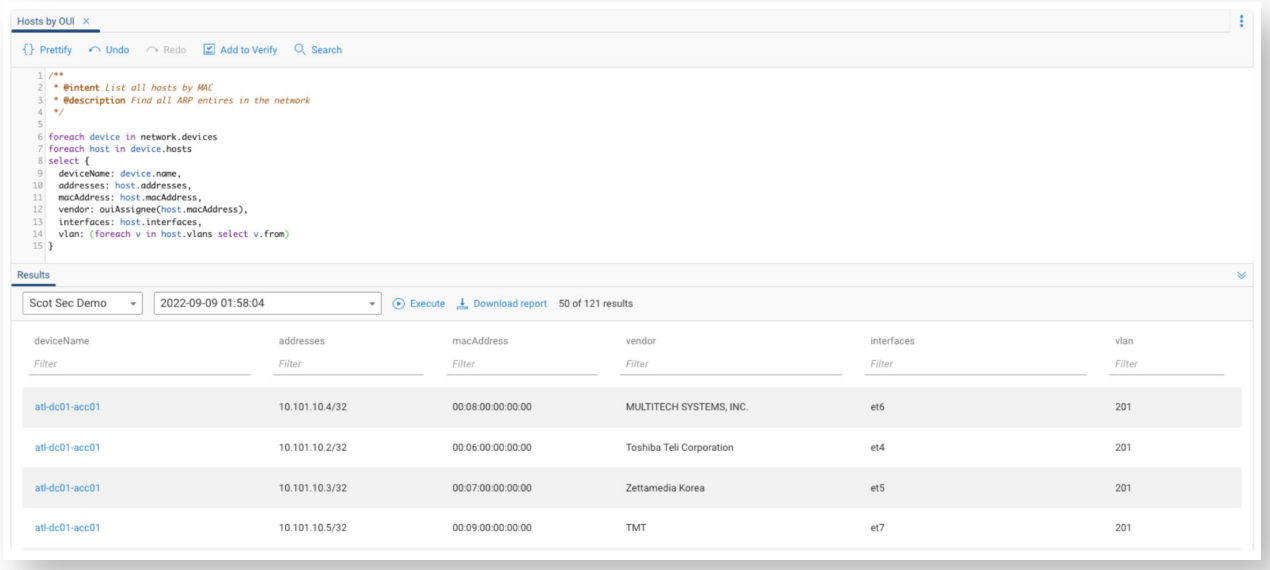


Figure 2: Example Network Visibility Report

This report can be generated for the entire network and compared to other scanning tools to ensure that the entire network is collected, including devices with IPv6 addresses.

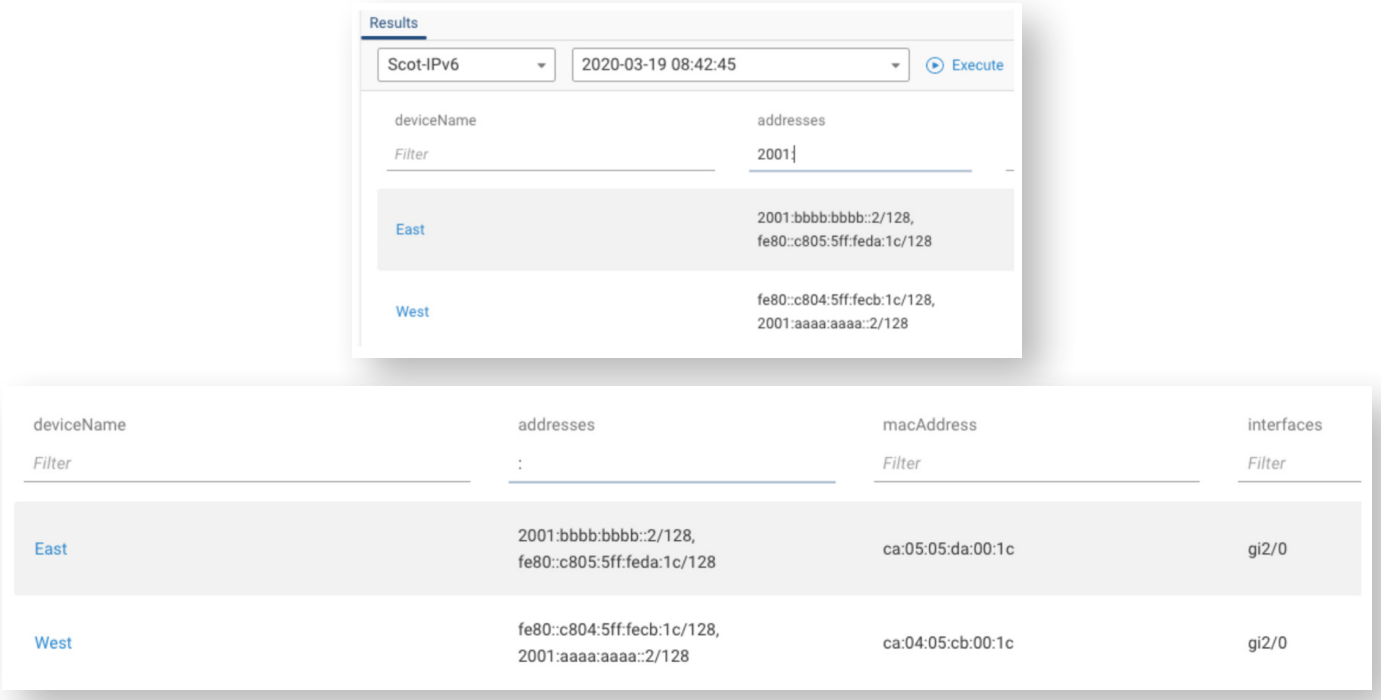


Figure 3: Example Network Visibility Report with IPv6 hosts

Enumerate Risk with NQE

The Network Query Engine (NQE) compliments vulnerability enumeration, providing an array of capabilities to delineate risk. For example, the query engine can expose any vulnerable configurations in a custom report or using the pre-built DISA STIGs (Cisco NDM STIGs). See Figures 4 and 5.

Find disallowed features that are enabled on Cisco NX-OS devices

This query locates instances of the `feature` config line in NXOS devices and extracts the named feature from these config lines. It checks the enabled features against a set of features that **should not** be enabled.

Using patternMatches

```
disallowedFeatures = ["telnet", "scp-server"];

foreach device in network.devices
where device.platform.vendor == Vendor.CISCO &&
      device.platform.os == OS.NXOS
foreach match in patternMatches(device.files.config, `feature {featureName:string}`)
let isDisallowed = match.data.featureName in disallowedFeatures
select { Device: device.name,
         Feature: match.data.featureName,
         Fix: if isDisallowed then "no feature " + match.data.featureName else "",
         violation: isDisallowed
       }
```

Figure 4: Sample STIG checks

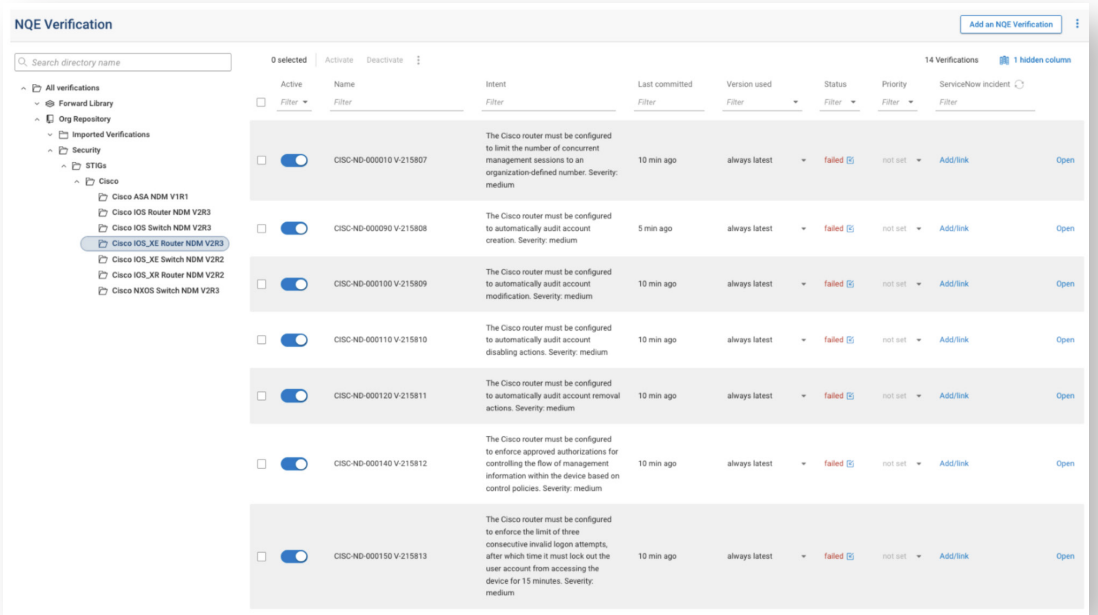


Figure 5: Sample NQE Query with failed checks

Understand CVE Exposure Based on Your Configurations

Another capability is identifying all the network devices that are exposed to a vulnerability based on version and vendor. Here Forward Enterprise reviews the vendor, version, and configurations of network devices to list all the possible vulnerabilities in the network. The CVE database can be updated daily from Forward Networks to meet the 24-hour signature update mandate. See Figure 6.

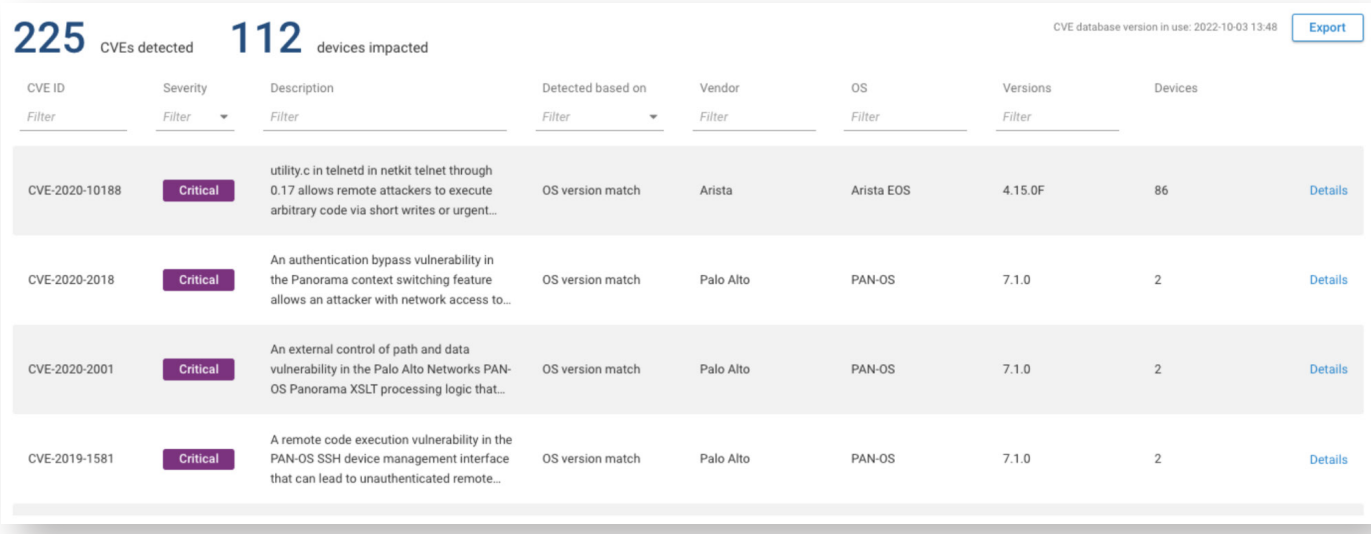


Figure 6: Sample CVE Report

Additionally, the vulnerability feature provides tremendous time savings for cyber professionals by filtering on devices that have the specific configuration bit enabled, making the device vulnerable. See Figure 7.

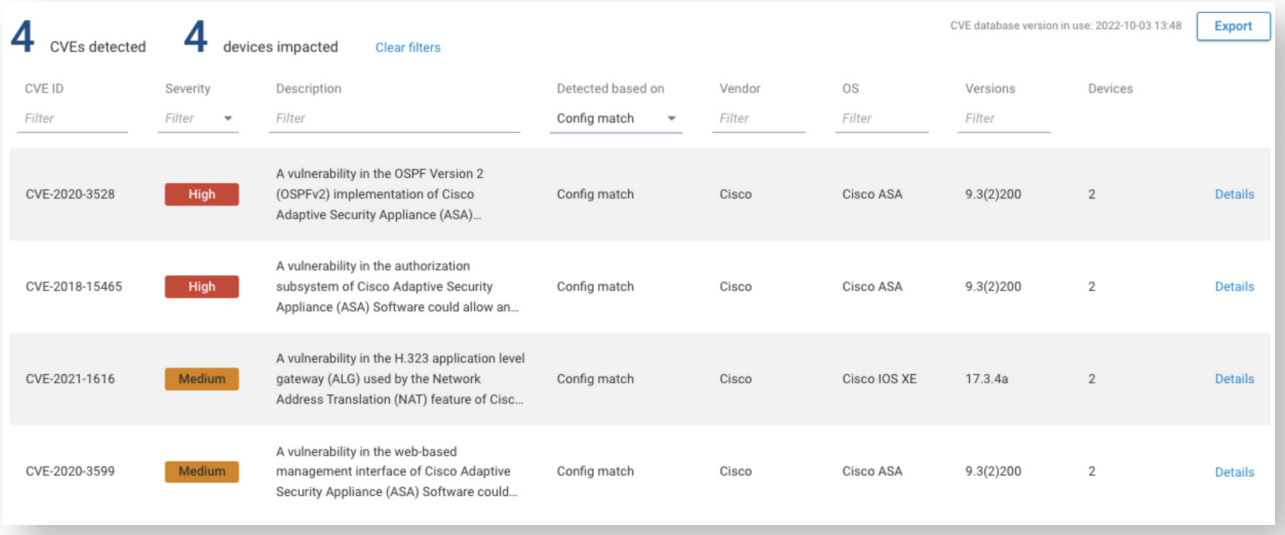


Figure 7: Devices Impacted by CVE

One Click Blast Radius Reporting

Forward Enterprise enables cyber professionals to fully understand the impact of a vulnerable host through a Blast Radius report that provides a complete list of all the possible destinations in the reachability table. This report can be generated in seconds by entering the compromised IP address and a single mouse click. See Figure 8.

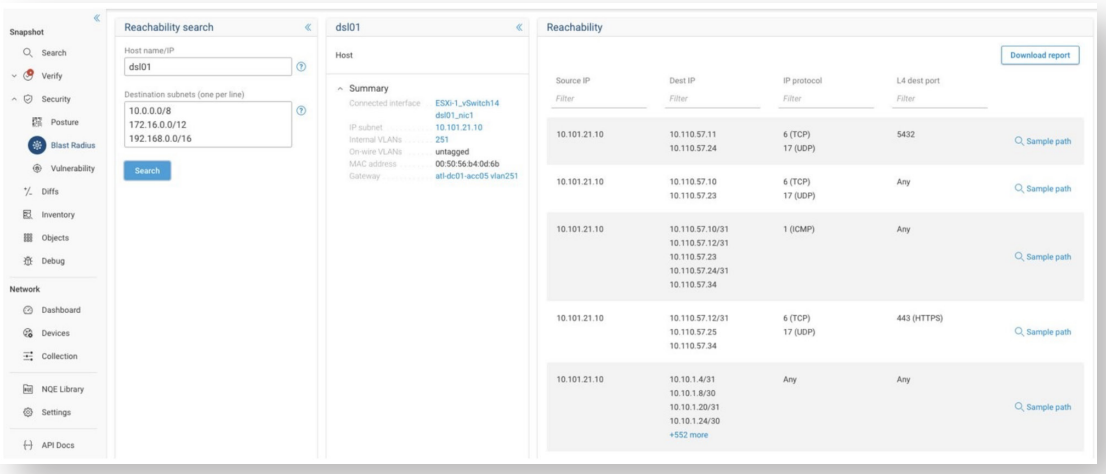


Figure 8: Blast Radius of a compromised host

Forward Enterprise also enables any cyber professional to quickly find if a host is reachable by selecting a location in the network as a FROM and searching all the possible paths in the network TO the vulnerable host. Here we can see all the possible permutations of NAT and load balancers in a path that ultimately has a host exposed to the Internet. See Figure 9.

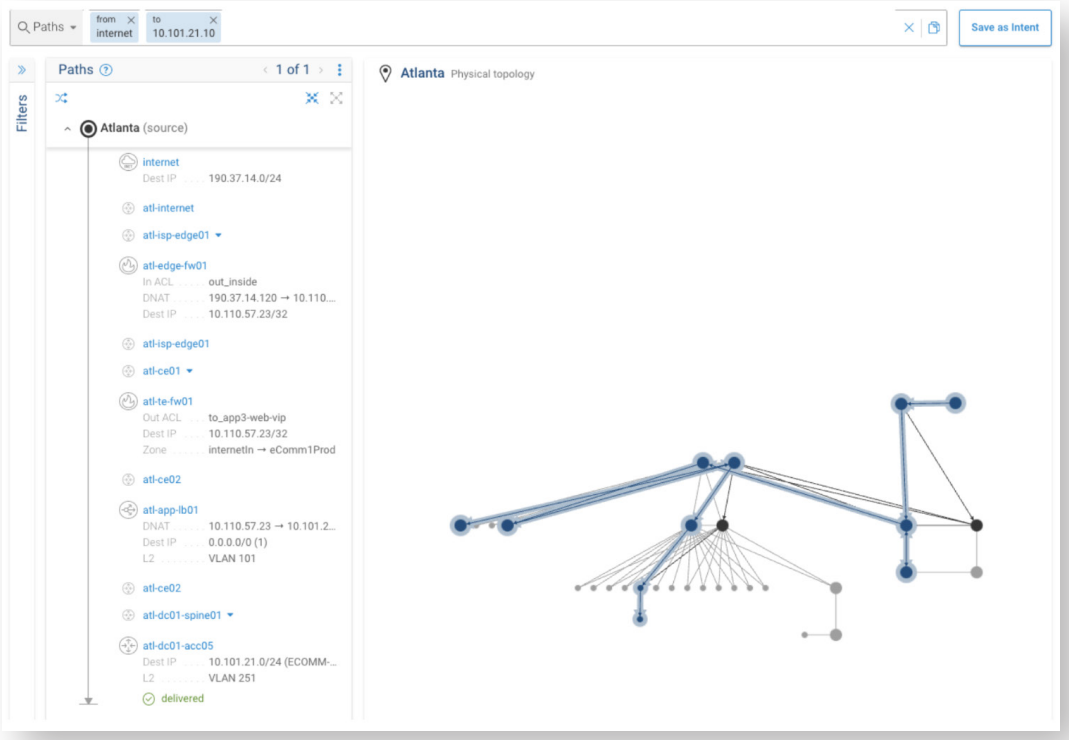


Figure 9: All potentially reachable devices from a compromised host

Integration with Rapid7 delivers the same level of insight into end-point vulnerabilities. See Figure 10.

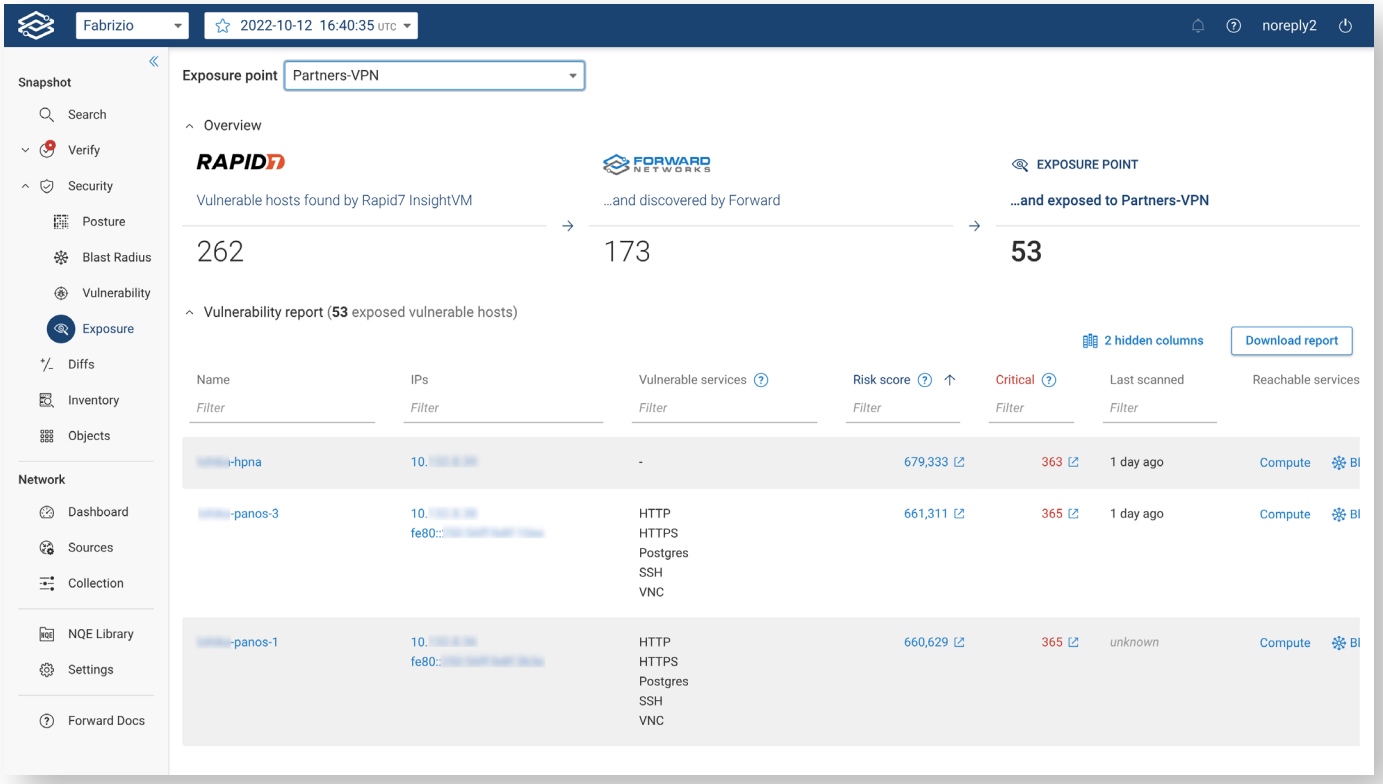


Figure 10: Rapid7 integration

ABOUT FORWARD NETWORKS

Forward Networks is revolutionizing the way large networks are managed and secured. Forward's advanced software delivers a "digital twin" of the network, enabling network operators to verify compliance, predict network behavior, and simplify network management. The platform supports devices from all major networking vendors and cloud operators, including AWS, Azure, and Google Cloud Platform.

Copyright © 2022 Forward Networks Inc. www.forwardnetworks.com