

Developing operational resilience

Your guide to proactive network security with Nipper Enterprise

Tasked with operational readiness and resilience in a rapidly changing threat environment, NOC, SOC and Incident Response teams do not have the fundamental information needed to proactively secure their networks.

To address this, teams need visibility of:

- Exploitable vulnerabilities introduced by planned and/or unauthorized network changes
- Overall attack surface posture by mission critical segments
- Exposure to specific APT TTPs as a consequence of network misconfigurations and software vulnerabilities
- Indicators of compromise, including macro segmentation violations (IPs, Ports and Users)

Nipper Enterprise is designed precisely to address this, proactively and at scale.



The shift towards proactive security

The rapid expansion of the modern attack surface coupled with attack innovation and threat proliferation means the shift to proactive security is gathering pace, as organizations seek the exposure intelligence needed to close their most critical network security gaps, before they are exploited.

Network infrastructure devices - routers, switches and firewalls - are increasingly the target of state sponsored actors. Exploiting vulnerabilities in these devices on IT and OT networks allows attackers to launch and proliferate attacks ranging from advanced persistent threats (APTs) to pervasive ransomware. The network access and management controls that routers provide, for example, allow threat actors to pre-position on networks ready to strike with potentially catastrophic effect. Using this tactic of living off the land (LOTL), adversaries like Volt Typhoon can persist for many years, undetected by current assessment practices.

The rapid expansion of the modern attack surface coupled with attack innovation and threat proliferation means the shift to proactive security is gathering pace, as organizations seek the exposure intelligence needed to close their most critical network security gaps, before they are exploited.

Network infrastructure devices - routers, switches and firewalls - are increasingly the target of state sponsored actors. Exploiting vulnerabilities in these devices on IT and OT networks allows attackers to launch and proliferate attacks ranging from advanced persistent threats (APTs) to pervasive ransomware. The network access and management controls that routers provide, for example, allow threat actors to pre-position on networks ready to strike with potentially catastrophic effect. Using this tactic of living off the land (LOTL), adversaries like Volt Typhoon can persist for many years, undetected by current assessment practices.

Challenges compounded by current assessment practices

With potentially tens of thousands of these complex devices on the network, many organizations have fallen into the practice of sampling subsets of their network infrastructure or limiting assessments to just perimeter devices. The frequency of assessments also means that even these samples are left unchecked for extended periods of time.

Given the foundational role that routers, switches and firewalls play in network segmentation, current assessment practices mean that organizations simply do not have assurance that mission critical segments are being adequately protected. Bussing teams with scanning the whole network for vulnerabilities and compliance with regulatory standards and controls only compounds the problem.

Legacy preventive and reactive tools, as valuable as they remain, do not provide the answer. Which is why next-gen, risk-based, device vulnerability management (RBVM) solutions are considered a must-have component of the proactive security tech stack, for critical parts of the network.

With potentially tens of thousands of these complex devices on the network, many organizations have fallen into the practice of sampling subsets of their network infrastructure or limiting assessments to just perimeter devices. The frequency of assessments also means that even these samples are left unchecked for extended periods of time.

Given the foundational role that routers, switches and firewalls play in network segmentation, current assessment practices mean that organizations simply do not have assurance that mission critical segments are being adequately protected. Busying teams with scanning the whole network for vulnerabilities and compliance with regulatory standards and controls only compounds the problem.

Legacy preventive and reactive tools, as valuable as they remain, do not provide the answer. Which is why next-gen, risk-based, device vulnerability management (RBVM) solutions are considered a must-have component of the proactive security tech stack, for critical parts of the network.

Next-gen RBVM solutions must be capable of giving:

NOC teams up to date CMDBs and near real-time visibility of network changes to:

- Investigate and compare actual, planned and unauthorized network changes
- Manage 'configuration as code' to (i) test pre-production config changes (ii) expedite disaster recovery from operational incidents and (iii) perform root cause analysis of changes that may have caused the incident
- Assure that 'tested configuration changes' when implemented in the live environment have been successful and the device maintains a secure state.

SOC teams near real-time visibility of:

- Overall attack surface posture by mission critical segments
- Exposure to APTs' specific tactics, techniques and procedures (TTPs) as a consequence of network misconfigurations and software vulnerabilities
- Systematic exploitable vulnerabilities that require a remediation strategy

Incident Response/Hunt teams visibility of:

- Current and historic attack surface postures to inform scope and focus of response
- Critical indicators of compromise (IOCs) not visible to traffic monitoring solutions.

The screenshot shows the Mitrade Attack Navigator interface. At the top, there's a search bar for threat intelligence and labels. Below, a section titled 'T1562 - Impair Defenses' provides a summary of vulnerabilities. The summary shows 9 devices, 76 DISA STIGs, 24 CAT I vulnerabilities, 52 CAT II vulnerabilities, and 0 CAT III vulnerabilities. A table below lists specific vulnerabilities, including CVE-2019-00110, CVE-2020-007, and CVE-2020-017, with their respective severity levels (Critical) and affected systems (ASA). The table also includes columns for the repository, DISA STIG title, DISA STIG value, NESA comments, OS, OS version, labels, found at, and report.

NOC teams up to date CMDBs and near real-time visibility of network changes to:

- Investigate and compare actual, planned and unauthorized network changes
- Manage 'configuration as code' to (i) test pre-production config changes (ii) expedite disaster recovery from operational incidents and (iii) perform root cause analysis of changes that may have caused the incident
- Assure that 'tested configuration changes' when implemented in the live environment have been successful and the device maintains a secure state.

SOC teams near real-time visibility of:

- Overall attack surface posture by mission critical segments
- Exposure to APTs' specific tactics, techniques and procedures (TTPs) as a consequence of network misconfigurations and software vulnerabilities
- Systematic exploitable vulnerabilities that require a remediation strategy

Incident Response/Hunt teams visibility of:

- Current and historic attack surface postures to inform scope and focus of response
- Critical indicators of compromise (IOCs) not visible to traffic monitoring solutions.

Dashboard
Mitig Attack Navigator
Full Screen Share Close Reset

Last 7 Days Refresh

Schedule Any	Labels Any	ExecutionID Any
--------------	------------	-----------------

T1562 - Impair Defenses

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This rule involves inspecting preventative defenses, such as **firewall** and **sensors**, but the detection capabilities that adversaries can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users or administrators.

Devices
9

DISA STIGs
76

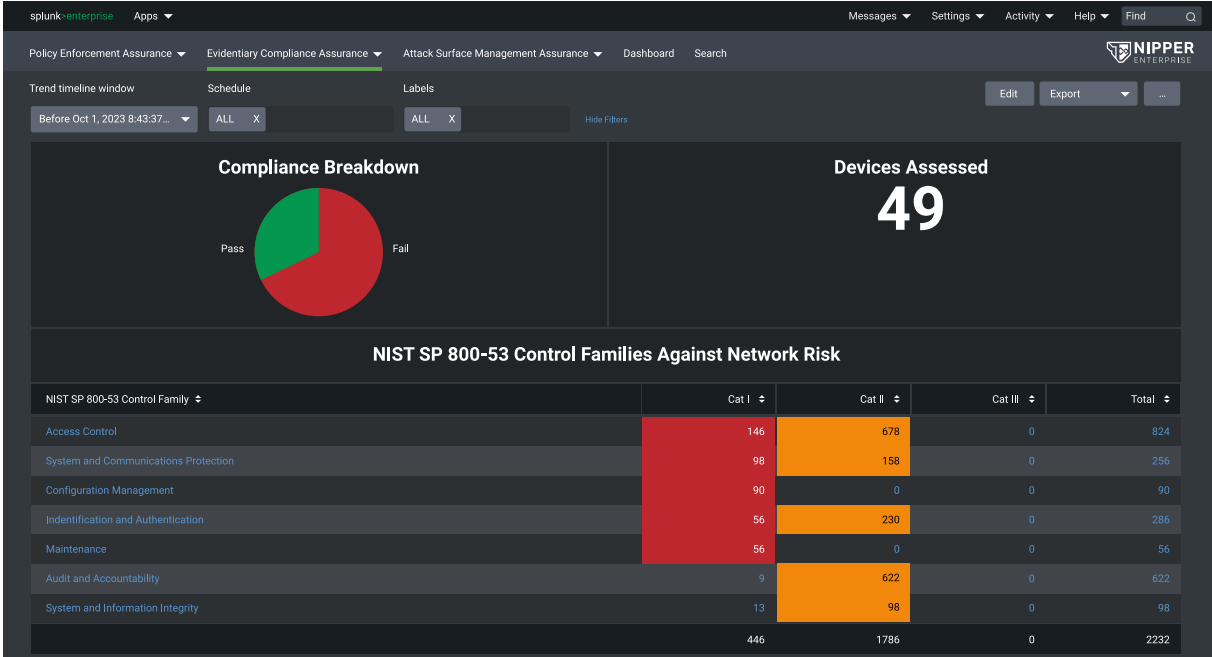
CAT I
24

CAT II
52

CAT III
—

	Repository	DISA STIG Title	NISA Controls	CAT	OS	OS Version	Labels	Found at	Report
	disco-NSARules-v2.txt	CASB-ND-QD1310 V=29940	—	CAT I	ASA	9.8(1)	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:26.694	Link
	disco-IProuter-5.txt	CBSO-ND-QS1200 V=22067	—	CAT I	ASA	15.0	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:25.696	Link
	disco-OSsmn-sns.txt	CPSO-ND-QD1310 V=22017	—	CAT I	ASA	15.0	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:25.395	Link
	disco-IDSsmn-txs.txt	CBSO-ND-QD1300 V=22067	—	CAT I	ASA	15.0	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:25.395	Link
	disco-IDSsmn-k.txt	CBSO-ND-QD1310 V=22017	—	CAT I	ASA	15.0	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:25.395	Link
	disco-IPSrouter-3.txt	CBSO-ND-QD1300 V=22067	—	CAT I	ASA	15.0	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:25.395	Link
	disco-IPSrouter-3.txt	CBSO-ND-QD1310 V=22017	—	CAT I	ASA	15.0	(USAF SFRP) Joint Base San Antonio	Nov 9, 2023 @ 11:28:25.395	Link

Dashboard prioritizing exploitable STIG vulnerabilities



Aggregated NIST SP 800-53 assessment data visualized in Splunk.

Designed to proactively minimize network exposure

Nipper Enterprise has been designed to free up and focus an organization’s scarce human cyber resource on business critical attack surface readiness and resilience. Building on Nipper’s vulnerability impact assessment accuracy and risk prioritized remediation know-how, Nipper Enterprise augments network risk visibility with macro segmentation violation and attack exposure analysis. Thereby providing the proactive security capabilities needed to:

- Maintain a continuously updated and segmented CMDB for operational resilience and disaster recovery
- Compare planned versus unplanned configuration changes to identify unauthorized and/or ineffective operational changes
- Assess all network device configurations to determine security and/or compliance posture baselines
- Automatically execute near real-time impact assessments of all new/changed configurations
- Expedite risk-prioritized vulnerability remediation with device-specific guidance and proactively confirm hardening activities have been enacted

“Nipper Enterprise assesses for configuration drift as it occurs, without the need for direct, credentialed device access, thereby delivering foundational zero trust capabilities.”

Omdia

- Test pre-production configuration changes, as well as configurations from live devices, offline
- Proactively monitor for configuration drift and known exploited vulnerabilities (KEVs) and associated exposure to active attack vectors using MITRE ATT&CK TTPs
- Identify devices with potential critical Zero Trust (ZT) segmentation violations, including blacklisted IPs, ports and user accounts
- Forensically analyze current and historic attack surface postures, informing focus and scope of incident response.

Nipper Enterprise delivers two key next-gen RBVM capabilities:

1. Enterprise-wide posture assessments

Increase the coverage and cadence of assessments for up to 250,000+ devices per day, to improve attack surface management by supporting ZT segmentation and policy enforcement, determining adherence to operational readiness and resilience standards (e.g. CORA and DORA), and automatically reporting pass/fail compliance with:

- PCI DSS 4.0
- NIST
- STIGs
- CIS Benchmarks

2. Near-real time exposure monitoring

Key to minimizing the attack surface and developing operational resilience, Nipper Enterprise proactively monitors configuration drift, providing visibility of ZT macro segmentation violations and vulnerabilities, automatically mapped to specific MITRE ATT&CK TTPs and KEVs, to inform business critical incident response and remediation strategies.

Near real-time config drift visibility, even in air-gapped environments

If this is an operational challenge, the configuration collection layer within Nipper Enterprise can be enacted to auto-populate and maintain the organization’s configuration repository. Enacting the configuration collection layer also provides the additional benefit of allowing users to manage ‘configurations as code’.

Nipper Enterprise detects network infrastructure device changes on the target network before securely extracting and storing live device configurations in the provisioned configuration repository. Git-based repositories also allow digital twin environments to be generated, which can be synced with Nipper Enterprise to test pre-production configuration changes ahead of deploying them to live devices. Changes made to the live configuration are then proactively re-checked to assure the device maintains a secure state.

All major device vendors are supported, including:



Architected for the enterprise

Nipper Enterprise has been architected to support internal and external use cases, via multi-tenanted deployments. A horizontally scalable, agentless web-based application, the solution is accessible through modern web browsers. Rest APIs and JSON outputs provide integration with trusted 2FA, CMDB/Git repository, SIEM, SOAR, GRC and trouble-ticketing solutions, to ensure full integration within the proactive security tech stack.

Flexible deployment options include:

- On-premise – deployed on a server; either a physical machine or using a virtualization platform (e.g. VMware ESXi with an Open Virtual Appliance);
- Virtual Private Cloud (VPC) – deployed using an Amazon Machine Image (AMI);
- Flyaway Kit – installed on a physical or virtual laptop.

Automating an inside-out view of vulnerabilities across network infrastructure, Nipper Enterprise enables risk-prioritized remediation to shut down attack vectors that pose real-world threats to the organization.

Key Features



Risk exposure visualizations – layer risk-prioritized vulnerability findings onto dashboards to detect privilege escalation and lateral movement exposure or report TTPs for specific APTs and ransomware.



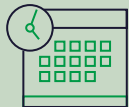
Proactive re-assessments – Nipper Enterprise proactively fetches running configurations to assess new and changed configurations in near-real time.



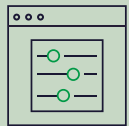
Obscured segmentation data – segmentation labels and metadata are automatically inherited, but only configuration identifiers are reported to ensure device locations remain obfuscated.



Digital twin syncing – synch provisioned config repositories, along with any digital twins, to manage ‘configuration as code’ and allow pre-production changes to be tested offline, from live devices.



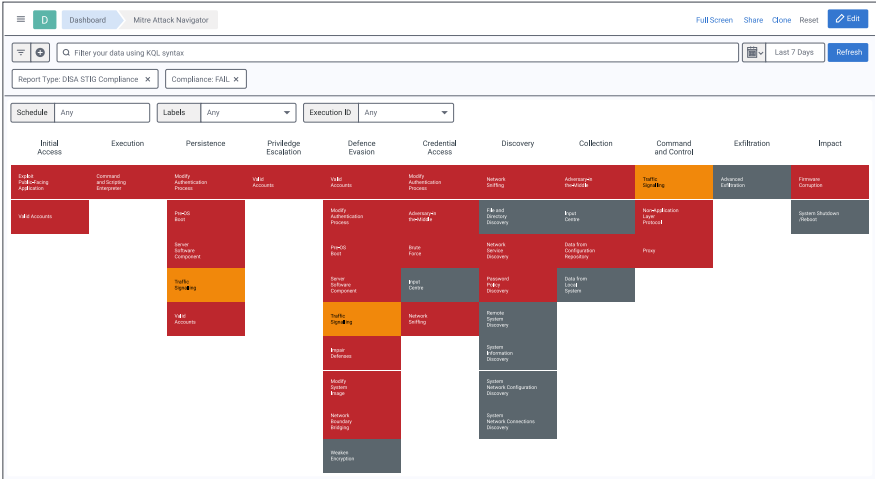
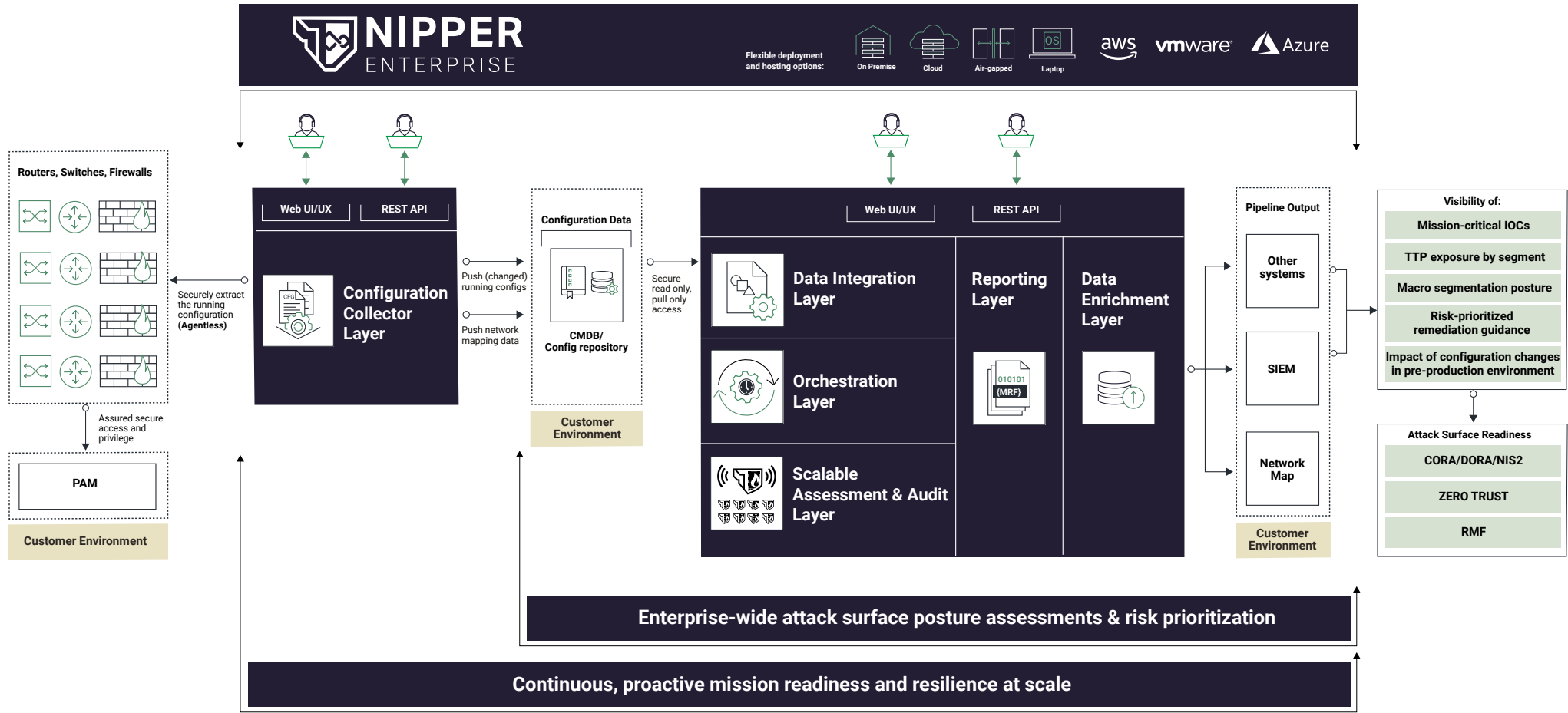
Customizable audit schedules – audit network segments according to device labels, such as network criticality, geographic location, manufacturer, device type etc.




Configurable check parameters – ensure network infrastructure assessments reflect the organization’s policies and risk profile by configuring check parameters to specific security requirements.



Aggregated data analysis – machine-readable report outputs and an agnostic data pipeline enable integrations with SIEM, SOAR, GRC and trouble-ticketing tools.



Dashboard showing heat map of exposure to TTPs from STIG compliance failures



“Nipper Enterprise adds a level of proactive security risk assessment and vulnerability management, which complements nicely the kind of server-centric vulnerability assessment enabled by the likes of Qualys and Tenable.”

Omdia

Why Titania

For more than a decade, elite cyber teams have relied on Titania's accurate network configuration assessment software, Nipper, to determine whether their routers, switches and firewalls leave their networks open to attack due to misconfigurations and exploitable vulnerabilities. Nipper helps organizations close these security gaps by automatically prioritizing risks by criticality, allowing users to view vulnerabilities through their chosen compliance and security policy lenses, and providing insights and advice that are proven to accelerate the mean time to remediate. Nipper's pass/fail compliance evidence also accelerates vulnerability assessment reporting, making it the tool of choice for many assessors.

And now, to meet the shift in needs of security-mature organizations, Nipper has been scaled to provide continuous, near-real time configuration drift monitoring across the entire network infrastructure attack surface. Proactively assessing changes to configurations as they occur, Nipper Enterprise provides visibility of exposure by network segment and MITRE ATT&CK TTPs, giving visibility of indicators of compromise, and providing current and historic posture reporting to inform the focus and scope of incident response, to improve operational readiness and resilience.