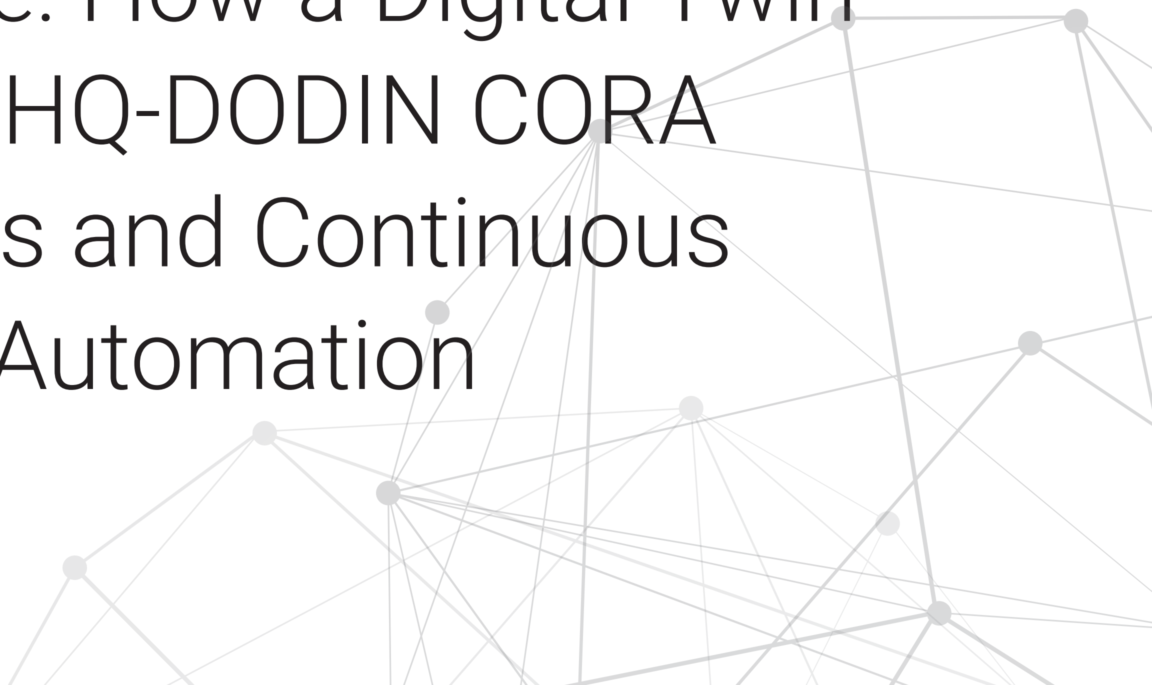
FORWARD NETWORKS

WHITE PAPER

From Compliance to Resilience: How a Digital Twin Drives JFHQ-DODIN CORA Readiness and Continuous Network Automation



Executive Summary

In March 2024, the US Department of Defense (DoD) strategically shifted its network defense paradigm from a static, compliance-based inspection model (CCRI) to a dynamic, risk-focused Cyber Operational Readiness Assessment (CORA). This change mandated continuous, threat-informed cyber resilience, further rendering formerly manual audit preparation inadequate and inefficient.

This whitepaper asserts that modernizing the Department of Defense Information Network (DODIN) cyberdefense requires a novel technological leap. The Forward Enterprise Digital Twin Platform provides the continuous visibility and predictive risk modeling capabilities necessary to meet CORA audit requirements. By automating STIG compliance verification and viewing real-world threats using the MITRE ATT&CK framework, the digital twin allows DoD entities to move beyond reactive readiness to a state of proactive, measurable, and mission-aligned cyber defense, ensuring success in a short-notice CORA environment.

Part 1: The Strategic Shift: CORA, Risk-Based Metrics, and the Mandate for DODIN Cyber Resilience

FROM CCRI TO CORA: THE END OF “CHECK-THE-BOX” COMPLIANCE

The previous Command Cyber Readiness Inspection (CCRI) model was popularly perceived by network operators as a compliance exercise. Its primary focus was auditing adherence to Security Technical Implementation Guides (STIGs), often resulting in a static, point-in-time test. This approach proved insufficient against sophisticated, Advanced Persistent Threats (APTs) and lacked the agility to accurately measure operational security.

THREAT-INFORMED DEFENSE: CORA’S FOCUS ON MITRE ATT&CK AND OPERATIONAL READINESS

The Cyber Operational Readiness Assessment (CORA) now serves as the DoD’s modern framework for evaluating a unit, base, or command’s genuine cybersecurity posture across the various components and networks that comprise the IT infrastructure. It represents a critical strategic shift, moving from mere administrative compliance to mission resilience and DODIN Defense.

Key Pillars of the CORA Framework:

- Risk-Based Metrics: CORA utilizes a risk-based calculus, guided by JFHQ-DODIN directives, to prioritize mission-critical systems and high-priority cyber terrain.
- Threat-Informed Assessment: The assessment directly integrates threat intelligence and the MITRE ATT&CK framework. This allows assessors to measure an organization’s vulnerability to known adversary Tactics, Techniques, and Procedures (TTPs), establishing a higher bar for defense.
- Agile and Continuous Requirement: The process is designed to be flexible and adaptive, often announced with and sometimes with minimal warning (as little as 30 days), making continuous readiness paramount for all network administrators and engineers.

Part 2: The Digital Twin Solution: Enabling Continuous CORA Readiness and Network Automation

The threat-informed nature of CORA demands a capability that eliminates the need for the manual, weeks-long “assessment crunches” that can cripple network teams’ productivity. The Forward Enterprise Digital Twin provides the foundational architectural capability for this continuous, proactive defense posture.

CONTINUOUS READINESS: AUTOMATING STIG COMPLIANCE AND CONFIGURATION VALIDATION

Traditional CORA preparation is resource-intensive, requiring network teams to spend countless hours manually querying and validating device configurations.

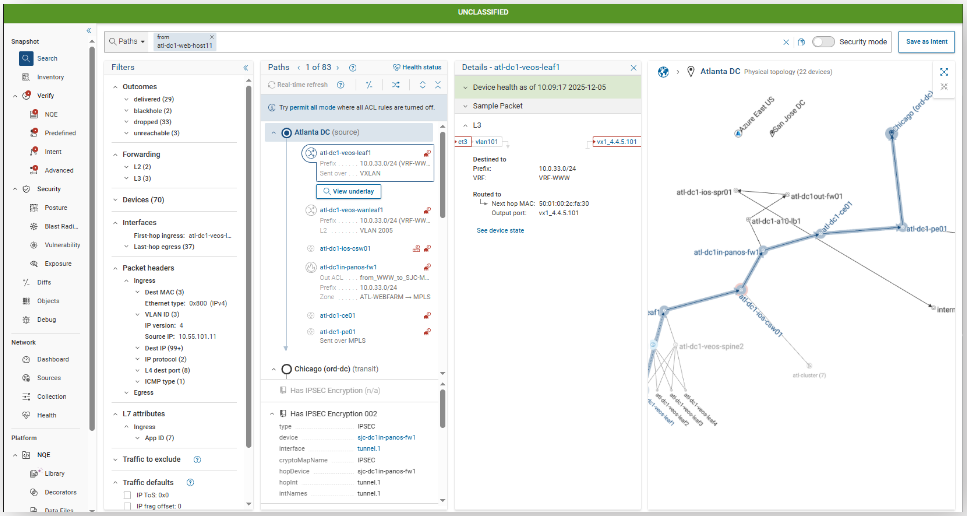
Automated Monitoring & STIG Compliance Validation: Forward Networks collects data from the live network, providing a near-time, “single pane of glass” view. The platform automates the validation of all network configurations, security policies, and compliance with directives (STIGs, FRAGOs, CTOs). This makes maintaining continuous readiness vastly simpler for a DoD entity.

The Network Query Engine (NQE): The Forward Enterprise Network Query Engine (NQE) acts as an “independent targeting system” for compliance. It retrieves the full configuration and state of every device using native show commands, runs the files through a mathematical model, and instantly indexes the data. This allows teams to run customized checks to detect noncompliance and configuration drift with every snapshot, alerting them only if a violation is detected.

DYNAMIC RISK MODELING: SIMULATING THREATS WITH MITRE ATTACK

CORA prioritizes mitigation based on actual risk to the mission, requiring commanders to visualize and prioritize vulnerabilities based on how they enable an adversary's TTPs.

- **Dynamic Risk Modeling and Threat Simulation:** Forward Networks utilizes threat intelligence and the MITRE ATT&CK framework to identify blind spots and weak points. Commanders can use the digital twin to model "what-if" scenarios, simulating how specific TTPs would impact their mission-critical systems and prioritizing mitigation efforts based on actual risk.



UNCLASSIFIED

Paths · from atl-dc1-web-host11

Filters

- Outcomes: delivered (29), blackhole (2), dropped (33), unreachable (3)
- Forwarding: L2 (2), L3 (3)
- Devices (70)
- Interfaces: First-hop ingress: atl-dc1-veos-l...; Last-hop egress (37)
- Packet headers: Ingress: Dest MAC (3); Ethernet type: 0x800 (IPv4); VLAN ID (3); IP version: 4; Source IP: 10.55.101.11; Dest IP (99+); IP protocol (2); L4 dest port (8); ICMP type (1); Egress
- L7 attributes: Ingress: App ID (7)
- Traffic to exclude
- Traffic defaults: □ IP ToS: 0x0; □ IP frag offset: 0

Paths 1 of 83

Try permit all mode where all ACL rules are turned off.

Atlanta DC (source)

- atl-dc1-veos-leaf1 — Prefix ...... 10.0.33.0/24 (VRF-WW... — Sent over ... VXLAN
- atl-dc1-veos-wanleaf1 — Prefix ...... 10.0.33.0/24 (VRF-WW... — L2 .... VLAN 2005
- atl-dc1-ios-csw01
- atl-dc1in-panos-fw1 — Out ACL ... from_WWW_to_SJC-M... — Prefix ...... 10.0.33.0/24 — Zone ...... ATL-WEBFARM → MPLS
- atl-dc1-ce01
- atl-dc1-pe01 — Sent over MPLS

Chicago (ord-dc) (transit)

Has IPSEC Encryption (n/a)

Has IPSEC Encryption 002

type	IPSEC
device	sjc-dc1in-panos-fw1
interface	tunnel.1
cryptoMapName	IPSEC
hopDevice	sjc-dc1in-panos-fw1
hopInt	tunnel.1
intNames	tunnel.1

Details - atl-dc1-veos-leaf1

Device health as of 10:09:17 2025-12-05

Sample Packet

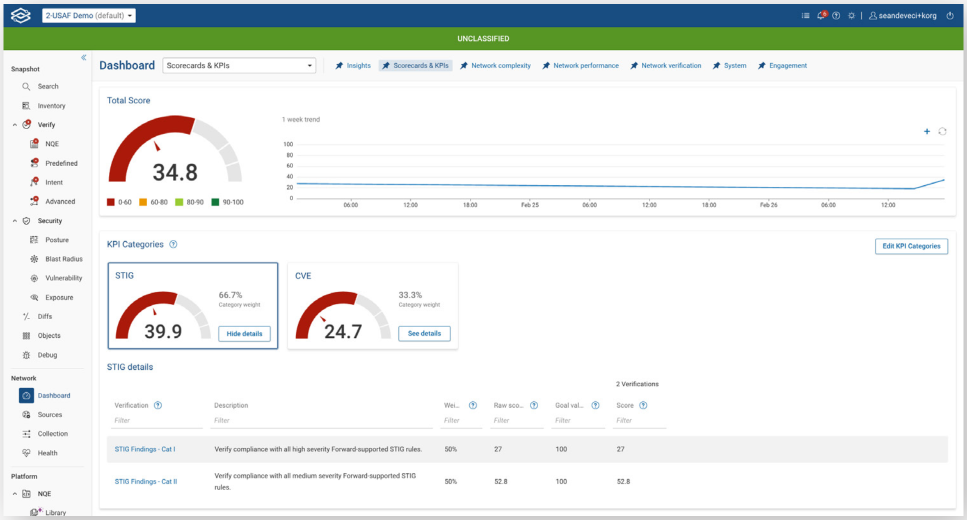
L3: et3 · vlan101 · vx1_4.4.5.101

Destined to
Prefix: 10.0.33.0/24
VRF: VRF-WWW

Routed to
Next hop MAC: 50:01:00:2c:fa:30
Output port: vx1_4.4.5.101

Atlanta DC Physical topology (22 devices)

- **Identification of Key Indicators of Risk (KIORs):** The digital twin can help identify and track KIORs, which are central to the CORA program. It provides a data-driven, quantifiable way to measure and track an organization's risk exposure over time.



2-USAF Demo (default)

UNCLASSIFIED

Dashboard · Scorecards & KPIs

Total Score: 34.8

KPI Categories

STIG: 39.9 — 66.7% Category weight

CVE: 24.7 — 33.3% Category weight

STIG details

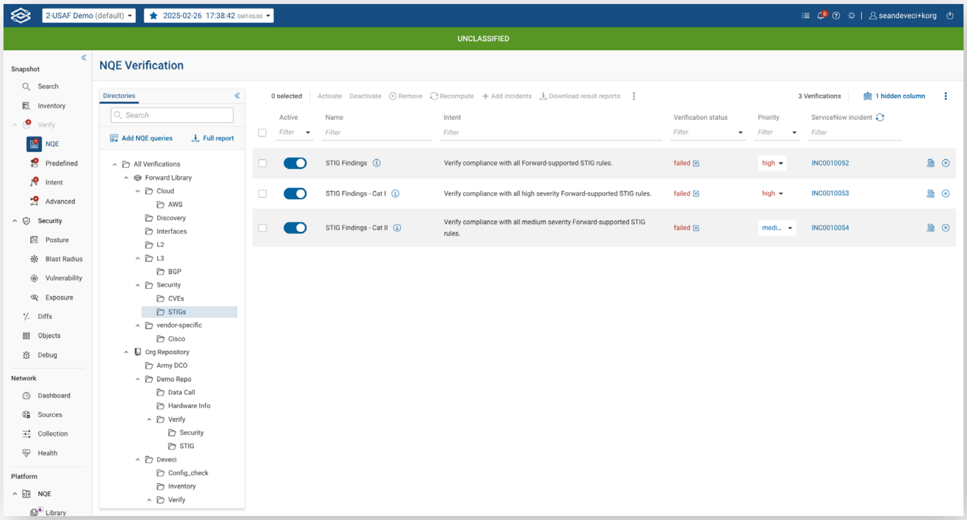
2 Verifications

Verification	Description	Wei...	Raw sco...	Goal val...	Score
STIG Findings - Cat I	Verify compliance with all high severity Forward-supported STIG rules.	50%	27	100	27
STIG Findings - Cat II	Verify compliance with all medium severity Forward-supported STIG rules.	50%	52.8	100	52.8

NETWORK CHANGE ASSURANCE AND CONFIGURATION DRIFT CONTROL

The network is a living, breathing organism. Every change carries the risk of inadvertently impacting the CORA STIG score or introducing a security gap.

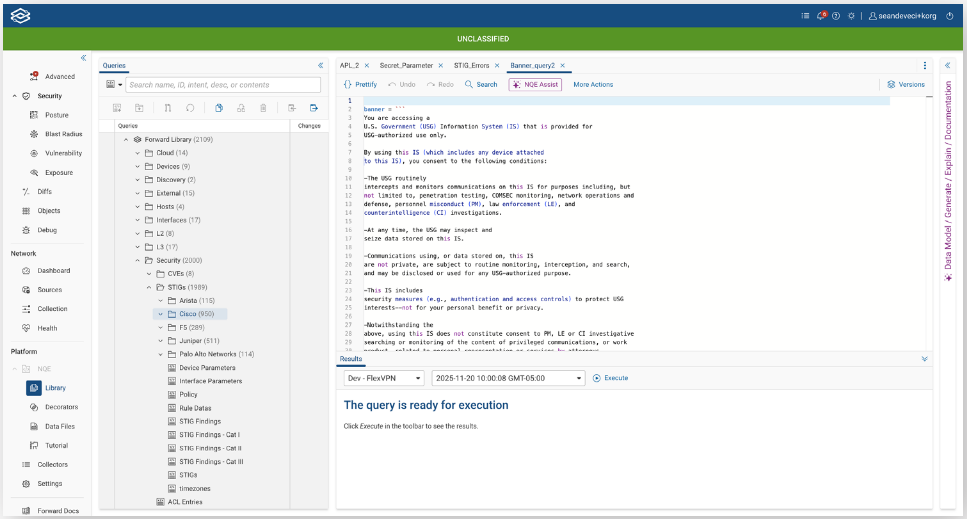
- **Historical Snapshots for Audit and Documentation:** Forward Enterprise's snapshot feature creates historical records of device configurations, routes, security posture, and vulnerabilities of your network. Teams can go back and compare the network state across any two points in time (Behavior Diffs), ensuring they know the full impact of any change and did not break anything along the way.



NQE Verification

Active	Name	Intent	Verification status	Priority	ServiceNow incident
Filter	Filter	Filter	Filter	Filter	Filter
●	STIG Findings	Verify compliance with all Forward-supported STIG rules.	failed	high	INC0010052
●	STIG Findings - Cat I	Verify compliance with all high severity Forward-supported STIG rules.	failed	high	INC0010053
●	STIG Findings - Cat II	Verify compliance with all medium severity Forward-supported STIG rules.	failed	medi...	INC0010054

- **NQE for Change Validation:** By coupling Snapshots with the NQE, teams can automatically get the compliance and vulnerability data they care about after every collection. This is crucial for verifying that configuration changes did not result in negative configuration or security drift.



```

banner = '''
You are accessing a
U.S. Government (USG) Information System (IS) that is provided for
USG-authorized use only.

By using this IS (which includes any device attached
to this IS), you consent to the following conditions:

-The USG routinely
intercepts and monitors communications on this IS for purposes including, but
not limited to, penetration testing, COMSEC monitoring, network operations and
defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.

-At any time, the USG may inspect and
seize data stored on this IS.

-Communications using, or data stored on, this IS
are not private, are subject to routine monitoring, interception, and search,
and may be disclosed or used for any USG-authorized purpose.

-This IS includes
security measures (e.g., authentication and access controls) to protect USG
interests--not for your personal benefit or privacy.

-Notwithstanding the
above, using this IS does not constitute consent to PM, LE or CI investigative
searching or monitoring of the content of privileged communications, or work
product, related to personal representation or services by attorneys
```

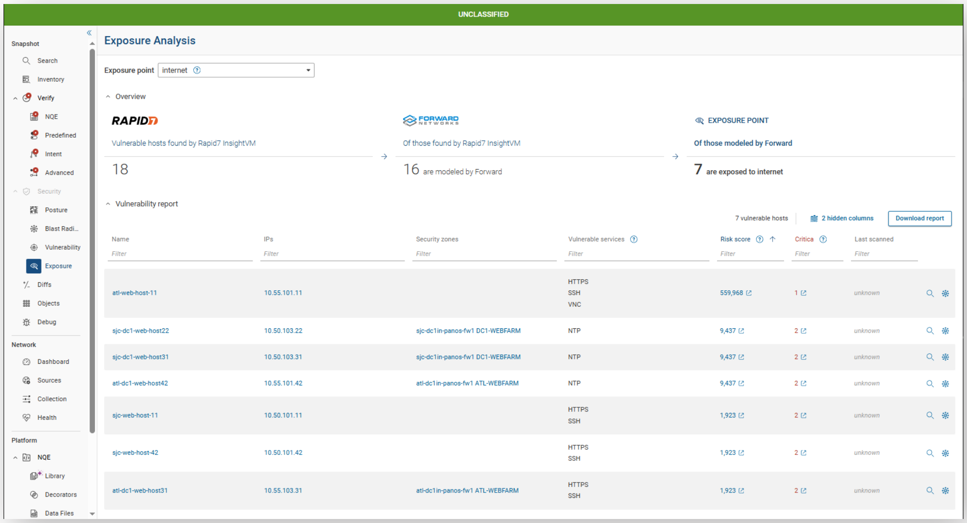
Dev - FlexVPN

2025-11-20 10:00:08 GMT-05:00

The query is ready for execution

Click *Execute* in the toolbar to see the results.

- **Data Aggregation and External Correlation:** NQE results can be imported and aggregated, eliminating the need for repetitive work. Furthermore, the platform offers the ability to integrate external systems (IPAM, golden configurations, or other platforms) via APIs, allowing for the correlation of non-device data with network state.



Exposure Analysis

Exposure point: internet

Overview

Vulnerable hosts found by Rapid7 InsightVM: 18

Of those found by Rapid7 InsightVM: 16 are modeled by Forward

Of those modeled by Forward: 7 are exposed to internet

Vulnerability report

7 vulnerable hosts

Name	IPs	Security zones	Vulnerable services	Risk score	Critica	Last scanned
atl-web-host-11	10.55.101.11		HTTPS SSH VNC	559,968	1	unknown
sjc-dc1-web-host22	10.50.103.22	sjc-dc1in-panos-fw1 DC1-WEBFARM	NTP	9,437	2	unknown
sjc-dc1-web-host31	10.50.103.31	sjc-dc1in-panos-fw1 DC1-WEBFARM	NTP	9,437	2	unknown
atl-dc1-web-host42	10.55.101.42	atl-dc1in-panos-fw1 ATL-WEBFARM	NTP	9,437	2	unknown
sjc-web-host-11	10.50.101.11		HTTPS SSH	1,923	2	unknown
sjc-web-host-42	10.50.101.42		HTTPS SSH	1,923	2	unknown
atl-dc1-web-host31	10.55.103.31	atl-dc1in-panos-fw1 ATL-WEBFARM	HTTPS SSH	1,923	2	unknown

STREAMLINED CORA REPORTING AND AUTOMATED ARTIFACT GENERATION

A primary pain point of a short-notice CORA is the scramble to generate the necessary artifacts and documentation.
Automated Artifact Generation: With Forward Networks, a large portion of the required data for an assessment can be generated automatically. This significantly reduces the time and resources spent on manual data collection and reporting, making short-notice CORAs much less disruptive.

Centralized Source of Truth: The platform acts as a single, authoritative source of truth. Results can be shared via:
.ckl file download for direct upload to compliance applications.
Sharing a secure URL attached to tickets, providing the recipient with the exact same view for quick and informed remediation.
Scorecard and KPI Dashboard: You can utilize the platform's Scorecard and KPI dashboard to track metrics over time, adding weighted scores for each metric to visualize the score increase and demonstrate continuous improvement to assessors.
Training and Education: The digital twin also serves as a safe, virtual training environment for cyber defenders to practice incident response and learn about the network's vulnerabilities without impacting the live system.

Conclusion: A Strategic Enabler for Mission Assurance

The Cyber Operational Readiness Assessment is the DoD's commitment to genuine cyber resilience and mission assurance across the DODIN. Success in this new era requires moving beyond brittle, manual processes and embracing strategic network automation and validation.

The Forward Enterprise Digital Twin Platform, with its continuous NQE-powered validation, dynamic risk modeling, and change assurance capabilities, is not solely a network audit preparation tool—it is a strategic enabler for the DoD. It provides the decisiveness, efficiency, and continuous visibility needed to transform CORA preparation from a resource-draining scramble into a validated, day-to-day operational status, ensuring the network is always in fighting shape and aligned with the mission.

ABOUT FORWARD NETWORKS

FORWARD NETWORKS