NETWORK CONFIGURATION ASSESSMENT

Your network configs are an attack surface. Assess them like one.

Device auditing and hardening for routers, firewalls, switches and cloud network fabric — a module of CyberSilo Threat Exposure Management.

31%

of breaches now begin with a software vulnerability — overtaking stolen credentials as the number one way attackers get in.

VERIZON DATA BREACH INVESTIGATIONS REPORT, 2026

Configuration decides whether that exploit is contained or catastrophic. An unpatched device behind correct segmentation is an incident report. The same device on a flat VLAN with an exposed management plane is a breach.

5 of 10

of the most common cybersecurity misconfigurations are network configuration failures — segmentation, ACLs, default configs, privilege separation, internal monitoring.

NSA / CISA AA23-278A

32 days

median time to fully remediate an edge device vulnerability — and only 54% are ever fully remediated at all.

VERIZON DBIR 2025

48%

of all breaches now involve ransomware — and segmentation is what decides whether it stays local.

VERIZON DBIR 2026

WHAT IT DOES

Automated and expert-led auditing of every running and startup configuration across your routers, firewalls, switches, load balancers and cloud network fabric — returned as risk-rated findings with evidence and remediation guidance.

Traditional network configuration management tells you what changed. CyberSilo tells you what an attacker can do with it, and what to fix first.

Request an exposure assessment

See your own network scored — findings, evidence and a remediation plan.

cybersilo.tech/network-configuration-assessment

FIVE THINGS YOU GET

01 Risk-rated, not rule-based

Every finding scored on exploitability, reachability from untrusted zones, asset criticality and compensating controls — mapped to MITRE ATT&CK. Two identical misconfigurations on two devices will not score the same, and should not.

02 Evidence in every finding

The exact configuration line, the command that produced it, the device, the timestamp and the standard it violates. Auditors get proof. Engineers get the line to change.

03 Attack path context

The finding shown in the path an attacker would take — entry point, the misconfiguration that enables the hop, the asset at the end of it. Fix the segment that breaks the most paths.

04 Regional compliance, natively mapped

NCA ECC, SAMA CSF, UAE NESA, Qatar NCS and PDPL — alongside CIS Benchmarks, PCI DSS v4.0.1, ISO/IEC 27001:2022, NIST CSF 2.0 and HIPAA. Audit evidence from the same assessment that drives remediation.

05 Automated platform, expert-led validation

CyberSilo analysts review findings, eliminate false positives and deliver a reviewed report. Machine coverage, human judgement on the output.

HOW IT WORKS

Discover
Agentless collection across your fleet and cloud fabric.

Assess
Parsed to a vendor-neutral model and audited.

Prioritize
Scored against exploitability and reachability.

Mobilize
Routed as owned work items with remediation syntax.

Validate
Reassessed to confirm closure.

> Gartner projects that organizations prioritizing security investments through a continuous exposure management program will be **three times less likely** to suffer a breach.

WHY NOT JUST USE YOUR NCCM TOOL

Traditional NCCM	CyberSilo
What changed?	What is exploitable, and what does it reach?
Pass / fail per rule	Risk-rated exposure with evidence
Vendor-set severity	Scored for your environment
Software only	Platform plus expert validation

CyberSilo does not replace configuration backup and restore. It decides which of those configurations is quietly costing you.

COVERAGE

Cisco IOS, IOS-XE, NX-OS, ASA, FTD, Meraki, SD-WAN · Juniper Junos · Arista EOS · Palo Alto PAN-OS, Panorama · Fortinet FortiOS, FortiManager · Check Point Gaia · HPE Aruba AOS-CX · F5 BIG-IP · Citrix NetScaler · VMware NSX · AWS · Azure · GCP

DEPLOYMENT: SaaS | Self-hosted | Air-gapped

> "We stopped triaging findings and started closing exposures."
>
> REGIONAL BANKING CUSTOMER

Request an exposure assessment

Book a technical walkthrough →