

From Reactive NetOps to Continuous Compliance

The same automation that resolves incidents now produces examiner ready evidence.



Trusted by Top 10 US banks and approximately one third of the Fortune 500.

Named bank logos available upon legal clearance.

The State of Network Operations in Banking

90%+

Deep Diagnosis accuracy on traditional networks

NetBrain R12.3

2 in 3

Financial institutions still struggle to demonstrate continuous operational resilience

KPMG (DORA readiness benchmark, 2025)

30 min

To map FFIEC and OCC gaps in a single session

Working benchmark, pending services validation

Where Network Operations and Compliance Diverge

Configuration Drift

Networks deviate from documented design between audit cycles. By the time examiners arrive, the evidence no longer matches reality.

Reconstructed Evidence

Incident records assembled after the fact do not satisfy modern regulatory expectations. Examiners want contemporaneous capture.

Hybrid Blind Spots

Cloud circuits, third party ISPs, and colocation environments often go unmonitored, but you remain accountable for all of them.

Regulatory Coverage at a Glance

Regulatory Area	What Examiners Look For	What NetBrain Does
FFIEC IT Handbook	Documented network configurations, change controls, and incident response capability that match operational reality.	Auto discovers all network devices, maps live topology, and detects configuration drift against your golden path baseline in real time.
OCC Heightened Standards	Demonstrable risk governance, independent verification of controls, and contemporaneous evidence of operational resilience.	Captures every diagnostic action, change, and verification in an ITSM linked audit trail. Pre and post change validation with one click rollback.
NYDFS Part 500	Continuous monitoring of nonpublic information systems, documented incident response, and access control evidence.	Continuous monitoring of network state with anomaly detection. Deep Diagnosis produces explainable root cause analysis with full reasoning chain logged.
SOX IT General Controls	Segregation of duties, change management approvals, and evidence that production systems operate as approved.	No code automation enforces approved runbooks. Triggered Automation Framework executes within defined guardrails. Every action attributable, logged, and exportable.
GLBA Safeguards Rule	Documented safeguards, monitoring of service providers, and ability to detect and respond to security events.	Monitors hybrid environments including cloud circuits and third party connectivity with on prem equivalent visibility. Surfaces dependency risk before it becomes a reportable event.

From Network Assessment to Examination Ready Evidence

01 ASSESS

Auto discover and map every network asset across your hybrid environment. Run a gap analysis against FFIEC, OCC, NYDFS, SOX, and GLBA control areas.

02 AUTOMATE

Deploy standardized diagnostic runbooks. Connect to your ITSM. Configure continuous drift detection against your golden path. No scripting required.

03 EVIDENCE

Every incident, every diagnostic action, every configuration check captured in real time. Logged, timestamped, and exportable. Not reconstructed. Captured.

Customer Perspective

“ We used to spend the week before every exam reconstructing what the network actually did. With NetBrain, that evidence is captured as the work happens. The audit conversation changed completely. ”

— Head of Network Operations, Top 10 US Bank

Get Network Compliance Today

Audit your network for FFIEC, OCC, NYDFS, SOX, and GLBA control areas.

Visit [Financial Services](#)