



CUSTOMER CASE STUDY | GLOBAL ENERGY UTILITY

A Global Energy Utility Replaces Manual CVE Discovery with Continuous CVE Assessment

CVE assessment across a 10,000-router enterprise network

The security team at a global energy utility uses NetBrain CVE assessment, including its dashboards, to validate exposure before engaging infrastructure teams. NetBrain correlates vulnerability data with live device inventory and configurations, so the team can tell which devices are only susceptible and which are confirmed vulnerable. Security now starts each investigation with an answer, backed by data.

KEY RESULTS

10,000

routers assessed through a tool already deployed

30 min

to a configuration-level answer for a CISA KEV alert

0

internet-exposed devices found vulnerable

IN THEIR WORDS

"I viewed the CVE feature as a nice feature, but the ability to tell the difference between susceptible and vulnerable started getting me out of bed."

– CISO, Infrastructure & Operations, Global Energy Utility

INDUSTRY

Energy. Electric and gas utility, critical infrastructure operator

ENVIRONMENT

About 35,000 employees; routers, switches, firewalls and access points

NETBRAIN CAPABILITIES

CVE assessment with dashboards, configuration inspection, API

THE CHALLENGE

After 15 years with an outside provider, the utility insourced management of its network and security devices in 2025, because the work was too strategic and the pace of change it needed did not fit an outside provider. Vulnerability management for roughly 10,000 routers came with it. A traditional scanner would have taken many man-hours, cost a great deal, and offered no guarantee of reaching every device.

THE SOLUTION

- Used the NetBrain deployment the networking team already had, integrated with every router, switch, firewall and access point.
- Correlated vulnerability intelligence from NIST, CERTs and vendor advisories against live device inventory.
- Had NetBrain inspect running configurations, such as SNMP version, access lists and public addressing, rather than matching CVE to version alone.
- Produced continuous compliance reporting for auditors: "When an auditor comes in, I just pull that week's report."
- Sent NetBrain data by API to the vulnerability risk database and used it to target credentialed scans.

RESULTS IN PRACTICE

When CISA flagged a Known Exploited Vulnerability on a widely deployed device type, the board expected an answer within the 24-hour patching objective for externally facing systems. Configuration checks produced an answer in about half an hour, and the CISO emailed the board: "We are not at risk here, here's the breakdown of the numbers." He added: "I can't imagine how else I would have done" it.

~7,500

SNMPv3 only, not an issue

~2,400

SNMPv1/v2 with access lists limiting exposure

~100

at risk with no access list, scheduled for cleanup

0

exposed to the internet

"We are not at risk here, here's the breakdown of the numbers."

CISO, INFRASTRUCTURE & OPERATIONS, GLOBAL ENERGY UTILITY

BEFORE NETBRAIN

- Vulnerability management for roughly 10,000 routers moved in-house after 15 years with an outside provider
- A traditional scanner would have taken many man-hours, cost a great deal, and offered no guarantee of reaching every device
- Matching CVE to version alone, with no way to tell susceptible from vulnerable
- Security waiting on, or second-guessing, another team's report

OPERATIONAL IMPACT

- **Confirmed findings** separate real vulnerabilities from false positives
- **30-minute answer** to a CISA KEV alert, with configuration-level evidence
- **Independent, continuous assurance:** Security pulls device data itself; this now runs continuously
- **Better prioritization** from confirmed CVEs, end-of-life devices and critical sites
- **Comparable results:** critical and high findings closely match the enterprise scanner

TRUST, BUT VERIFY

Once the team viewed NetBrain as an audit tool, the ask changed: "Do not just tell me the golden configuration exists. Show me every device that does not comply."

MANAGEMENT ACCESS	SSH permitted only from the approved jump hosts
SECURE PROTOCOLS	Deny administrative access through non-SSH protocols
CENTRAL LOGGING	Every router and switch sends logs to the approved SYSLOG host
CENTRAL AUTHENTICATION	TACACS configured and used for administrative authentication
BREAK-GLASS CONTROL	No more than two approved local emergency accounts

LOOKING AHEAD: AI IN THE CVE WORKFLOW

In a preview of the AI Copilot, the CISO saw plain-language CVE requests, impact analysis to decide which sites to patch first, and scheduled remediation, with CVE coverage expanding about 5X. NetBrain connects to a private ChatGPT instance, so the organization keeps control of its data. His reaction: "This now completed the workflow. To me, this turned it from a benefit of the product into a first-class feature of the product."

"This has now become a must-have in my toolbox."

CISO, INFRASTRUCTURE & OPERATIONS, GLOBAL ENERGY UTILITY