DATASHEET

NetBrain's Approach to CVE Management

Modern networks face an overwhelming volume of CVEs, but traditional tools struggle with:

- **Disruptive scanning** that impacts production environments
- **Version-only checks** that miss config-level vulnerabilities
- **Manual processes** for prioritization and remediation

NetBrain transforms CVE management by combining automated risk assessment with network-aware context and closed-loop remediation:

- **No active scanning:** Analyzes CLI/config files without network disruption.
- **Config-level detection:** Identifies risks that version checks miss (e.g., weak SNMP settings).
- **Topology-aware prioritization:** Maps CVEs to actual business impact (e.g., core vs. edge devices).
- **Self-service automation:** From detection to validated fixes—all in one platform.

This table outlines how NetBrain addresses each stage of CVE management, delivering faster, more accurate risk reduction than traditional tools.

NetBrain CVE Management Mapping Table

CVE Management Stage	Industry Element	How NetBrain Addresses It
1. Identification and Assessment	**CVE Database (NIST, etc.)**	NetBrain automatically retrieves CVE data from NIST via API, engineer-validates updates, and synchronizes them quarterly to the Golden Assessment Library and Automation Data Tables (ADTs) for rapid customer access.
	Vulnerability Scanning	NetBrain detects vulnerabilities from config files, CLI command outputs, API or live scanning — no agents, no network disruption. Static config checks detect vulnerabilities.
	Asset Inventory	Auto-discovered from API or CLI commands. Device type, OS version, config fragments , and installed hotfix patches are parsed and mapped instantly upon upload.
2. Prioritization and Risk Assessment	**Severity Levels**	Severity metadata is attached to each CVE in the Golden Assessment. The data is exposed via AI Insight or visual dashboard. A network-wide vulnerability report for affected devices can be configured to be sent via email and is automatically updated after a vulnerability is resolved and the device is re-scanned.
	Risk Factors (exploitability, exposure)	Exposure assessed through actual configurations, hardware specs, applied patches, and special configuration impacts—not just software versions — to minimize false positives.
	Business Impact	AI Insight uses topology and context to tie CVEs to affected business services, communicating the impact in plain language.

CVE Management Stage	Industry Element	How NetBrain Addresses It
3. Remediation and Mitigation	**Patching**	Identifies missing patches and generates remediation runbooks, but does not automatically execute fixes. While our system can trigger vendor-provided remediations when available (via NI), it is excluded from our standard library because: 1. Not all CVEs support simple command-line fixes (some require manual patching), 2. Any network-modifying operation requires manual user confirmation to prevent security risks. Each case must be evaluated individually.
	Configuration Changes	If a config is the root cause (e.g., SNMPv2 open, weak passwords), NetBrain can generate validated runbooks to remediate.
	Workarounds	PSEs can script intents to suggest temporary fixes (e.g., disable vulnerable service), shown via Insight or Runbook logic.
	Mitigation Strategies	NetBrain doesn't replace firewall/IDS, but can validate their config posture (e.g., ACL presence, segmentation logic) as part of assessment.
4. Validation and Monitoring	**Verification**	After remediation, a recheck verifies whether the CVE has been resolved either by: 1. Full re-benchmarking in Playground (re-evaluates entire config against CVE rules; time scales with network size) 2. A faster option: Targeted NI re-execution (immediately verifies the specific CVE against updated configs)
	Continuous Monitoring	Run Golden Assessments and automation schedules periodically — daily, weekly, post-change — depending on deployment.
5. Reporting and Improvement	**Regular Reporting**	CVE Dashboard shows current posture, affected devices, resolved vs. outstanding issues across domains and time. The Golden Assessment Library detects vulnerabilities and visually presents them as Golden Intent displayed when opening the map. Additionally, a network-wide vulnerability report for affected devices can be shared via email.
	Continuous Improvement	Update CVE libraries dynamically. Add new entries manually within minutes. Customers can also define custom CVEs for internal risk tracking.

Key Takeaways

- **No active scanning:** All analysis is done from CLI files, data retrieved from API controllers (e.g., CVE detection in Kubernetes) or live baselines — minimizes network disruption.
- **Config-level awareness:** Goes beyond package version — detects risks embedded in how devices are configured.
- **Automation loop:** CVE detection → Insight → Remediation Runbook → Revalidation — all within a single system.
- **Customer self-service:** Playground enables the customer to drive data ingestion securely and control their analysis window.