Guardare

Guardare CVE Exposure Monitor

Continuous visibility into newly published vulnerabilities across your live environment

Most organizations don’t struggle with finding CVEs.

They struggle with determining:

- Does this affect us?
- Which assets are exposed?
- Has remediation actually happened?
- What is our real exposure window?

Guardare CVE Exposure Monitor continuously correlates newly published vulnerabilities against your active environment to surface actionable risk in near real time.

Rather than forcing analysts to manually review advisories, inventory systems, and patch status across multiple tools, Guardare identifies what matters and suppresses what doesn’t.

How It Works

Continuous CVE Monitoring

- Automatically ingests newly published CVEs from sources such as the National Vulnerability Database (NVD).

Environment Correlation

- Matches affected products, versions, and CVEs against your asset inventory.

Real-Time Validation

- Pulls current asset and configuration state to determine whether systems are exposed.

Risk Prioritization

- Displays impacted assets as At Risk or Resolved.

Automated Alerting

- Sends targeted notifications with vulnerability details and remediation guidance.

Guardare

866.454.7670 • info@guardare.com • www.guardare.com
601 Cleveland St, Suite 700 • Clearwater, FL 33755

Guardare

Use Case: Zero-Day Firewall Vulnerability

Scenario

A critical zero-day firewall exploit is published affecting a specific firewall model and firmware version. Your environment contains multiple instances of the impacted firewall.

What Guardare Does

✓ Detects the newly published CVE automatically
✓ Correlates affected versions against your environment
✓ Pulls live firmware and patch status
✓ Determines exposure state

If patched: Status displays Resolved; no unnecessary alerts are generated.
If vulnerable: Status displays At Risk; administrators receive immediate notifications and remediation guidance.
After patching: Status updates automatically without manual validation.

“Know what affects you.
Act before attackers do.”

Outcome

Reduce exposure response from hours or days to minutes.

No manual asset lookups.
No spreadsheet tracking.
No cross-referencing vendor advisories.

Use Case: Eliminate Alert Fatigue

Scenario

A high-severity CVE is published for a network appliance that does not exist in your environment.

What Guardare Does

✓ Ingests the CVE
✓ Correlates against your asset inventory
✓ Finds no affected systems
✓ Logs the event without creating unnecessary alerts

Outcome

Maintain a high signal-to-noise ratio and keep analysts focused on vulnerabilities that actually matter.

Key Benefits

Reduce Mean Time to Detection — Identify exposure immediately after disclosure
Shrink the Exposure Window — Track publication through remediation
Increase Analyst Efficiency — Remove manual validation and cross-tool investigations
Prioritize Real Risk — Focus on vulnerabilities actively impacting the environment

Guardare

866.454.7670 • info@guardare.com • www.guardare.com
601 Cleveland St, Suite 700 • Clearwater, FL 33755