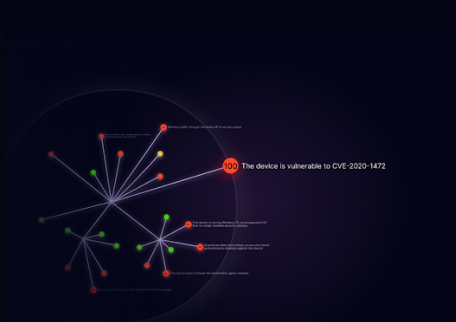
Guardare

GuardScan

Turn local discovery into actionable exposure intelligence.

See local assets. Add identity and integration context. Prioritize the exposures most likely to create risk.



Your environment changes every day. Visibility should keep up.

Unknown devices, reachable services, identity risk, and configuration drift create exposure that traditional inventories often miss. GuardScan discovers local assets, collects approved on-premises data, and continuously adds context so teams can focus on what matters first.

From local discovery to a clear security decision

DISCOVER Active hosts › **INSPECT** Ports + services › **ENRICH** Identity + local data › **CORRELATE** Exposure context › **ACT** Prioritized response

Core capabilities: feature → business benefit

1 Host Discovery

FEATURE

Uses ICMP/TCP probes, ARP, adapter, subnet and routing data, plus SNMP or broadcast discovery when available.

BENEFIT

Reveal unmanaged, forgotten, or newly connected assets before they become blind spots.

2 Exposure Intelligence

FEATURE

Evaluates reachable ports, services, versions, OS signals, and common vulnerability or misconfiguration indicators.

BENEFIT

Understand what attackers can reach and accelerate triage with richer technical evidence.

3 Network Graph Context

FEATURE

Uses interfaces, subnets, routes, discovered hosts, and reachable services to map asset relationships.

BENEFIT

Build a clearer exposure picture and identify risk that spans otherwise disconnected assets.

COMPLETE INVENTORY
of reachable local assets

RICHER CONTEXT
across devices and services

FASTER ACTION
with prioritized evidence

Guardare

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

Guardare

More context. Better decisions. Less manual investigation.

GuardScan adds directory and local integration context, then securely delivers structured results.

4 Active Directory Context

FEATURE

Collects authorized users, groups, computers, GPOs, trusts, policies, privileged objects, and delegation settings over LDAP.

BENEFIT

Add identity and domain risk to network findings without exposing Active Directory externally.

5 Approved Local Integrations

FEATURE

Runs approved workflows locally and connects to supported systems using credentials configured in Guardare.

BENEFIT

Extend coverage to sources that cannot—or should not—be reached from the cloud.

6 Results + Recommendations

FEATURE

Uploads structured results for inventory, change detection, exposure analysis, and remediation guidance.

BENEFIT

Turn collected data into prioritized recommendations instead of another list of findings.

7 Practical Deployment

FEATURE

Provides a desktop interface, background service, and native Windows, Linux .deb/.rpm, and macOS .pkg packaging.

BENEFIT

Deploy consistent scheduled or unattended collection across supported endpoints and servers.

REAL-WORLD USE CASE

A local exposure spans devices and identity

A newly connected server exposes a risky service while an inactive account remains enabled in Active Directory. GuardScan discovers the host, collects service and operating-system signals, and adds authorized directory context. Guardare correlates the evidence and raises the combined risk for action.

OUTCOME

Disable access, isolate the device, and close the service before the weaknesses form an attack path.

Built to strengthen the complete exposure picture

GuardScan feeds current network, directory, and approved local integration data into Guardare, where assets, identities, vulnerabilities, configurations, and controls can be evaluated together. The result is better context for prioritization and remediation.

Request a demo today!

See what your tools are missing.

Discover local assets and add the context cloud-only tools cannot reach.

Guardare

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