Protect the Plant. Don’t Disrupt It.

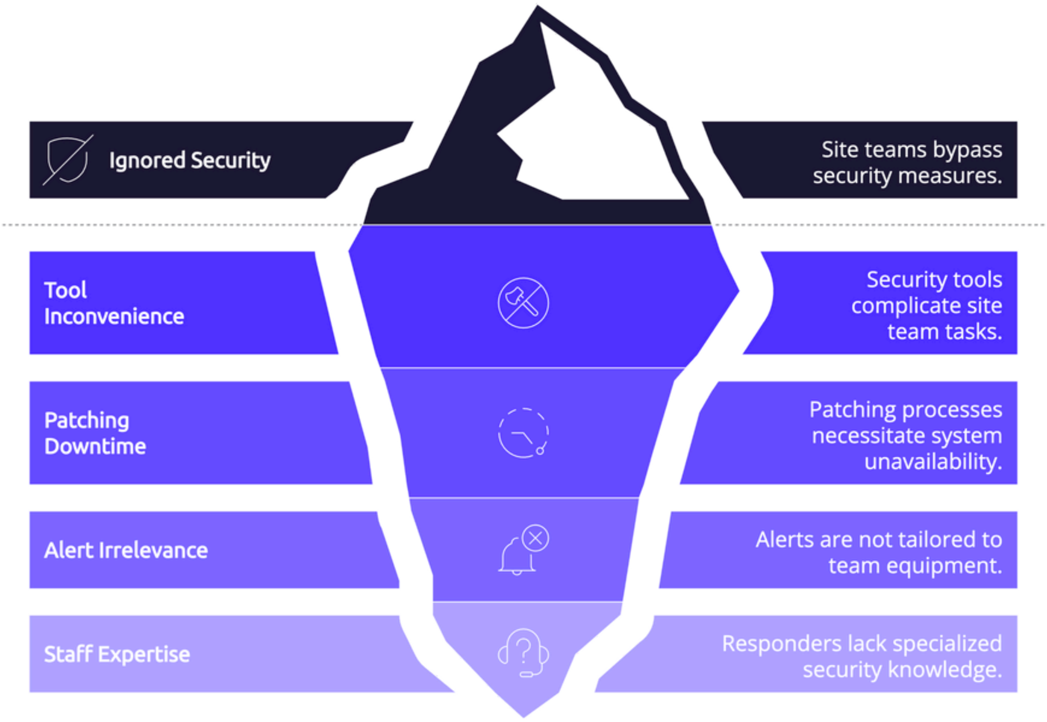
Security tools shouldn’t interrupt operations. SageOne fits your workflows instead of disrupting them.

Most security tools weren’t built for uptime. They assume systems can be taken offline—triggering reboots, floods of alerts, or maintenance windows teams can’t afford. So OT teams avoid or work around them, which raises risk instead of reducing it.

The Real-World Problem

Site teams aren’t ignoring security because they don’t care. They’re ignoring it because most tools make their jobs harder. Patching requires downtime, alerts don’t align with their systems, and the responders aren’t security pros—they’re operators and engineers who need simple, straightforward guidance. When tools add confusion instead of clarity, teams look for ways around them.

Security Neglect Rooted in Tool Inconvenience.


Ignored Security
Site teams bypass security measures.
Tool Inconvenience
Security tools complicate site team tasks.
Patching Downtime
Patching processes necessitate system unavailability.
Alert Irrelevance
Alerts are not tailored to team equipment.
Staff Expertise
Responders lack specialized security knowledge.

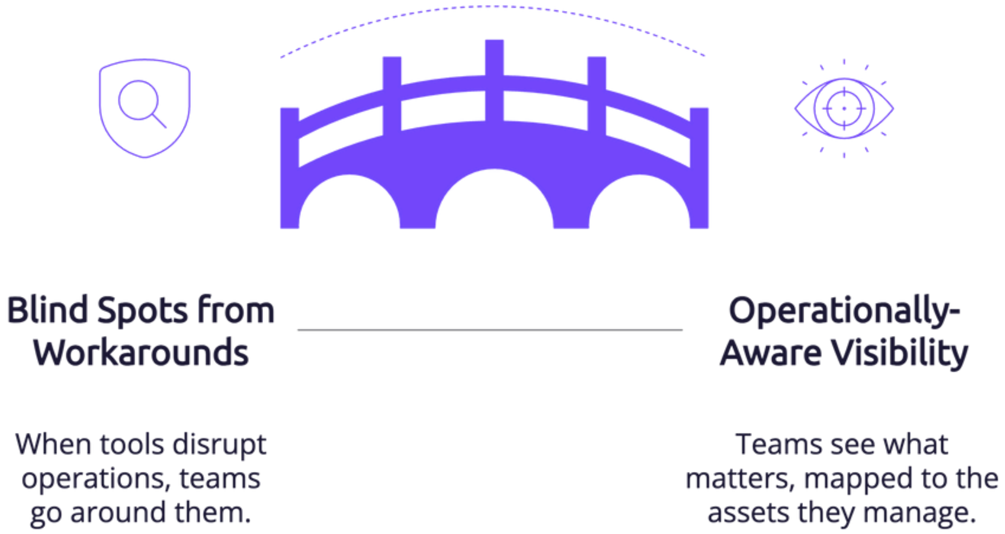
Why It Matters

When security creates friction, people work around it, and that’s when risk gets embedded in your operations. The longer teams go without the right tools, the more likely it is that something gets missed, ignored, or worked around. Visibility fades. Vulnerabilities pile up. And soon, even small issues become big ones. That’s why security tools can’t just be secure, they have to be usable. If they don’t help teams move forward with confidence, they hold them back.

The SageOne Approach

SageOne gives site teams visibility without adding complexity. It organizes events around the machines operators actually manage, helping them spot real issues faster. Instead of flooding dashboards with alerts, it links events to assets and surfaces the context needed to understand what happened, when, and why it matters.

SageOne bridges the gap to OT security visibility.



When tools disrupt operations, teams go around them.

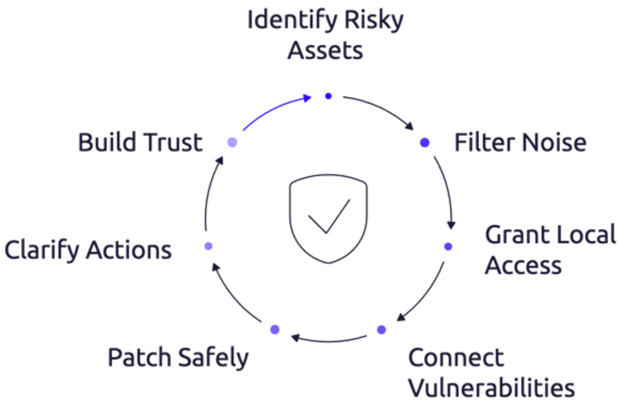
Teams see what matters, mapped to the assets they manage.

With built-in vulnerability ticketing, SageOne highlights time-sensitive threats tied to real systems—so teams can prioritize what to patch, what to isolate, and what can wait. Role-based access ensures each site sees only what's relevant, whether you're overseeing one plant or coordinating across many.

More Than Just Uptime Protection

SageOne helps teams reduce risk without causing disruption. It supports high-impact tasks like identifying risky assets, filtering noise, and giving local teams just enough access to act. By connecting vulnerabilities to real OT systems, SageOne makes patching safer, actions clearer, and tools more trusted.

SageOne Security Enhancement Cycle



What Makes SageOne Different

Uninterrupted production

Deploy and operate without interrupting production. This ensures continuous operation.

OT team design

Designed for OT teams, showing relevant information. It is not just for SOCs.

Triage ready

Incidents appear in asset charts directly. No raw alert streams are present.

Role-based visibility

Every team sees only relevant information. This depends on their site or function.

Vulnerability aware

Highlights high-risk CVEs without flooding teams. Scan noise is reduced for efficiency.

Take the Next Step

SageOne helps site teams reduce risk without slowing operations, but that’s only part of the story.

See how the platform also supports other teams and initiatives across your OT environment:

- Protect Legacy Systems: How engineers secure aging assets without patching, rebooting, or replacing them.
- Act Fast on OT Threats: How analysts get faster answers with asset-based investigation tools.
- Full Technical Overview: SageOne’s architecture, deployment model, and key capabilities.

→ Explore SageOne

→ Contact Us