Modern Security for the Systems That Can’t Change

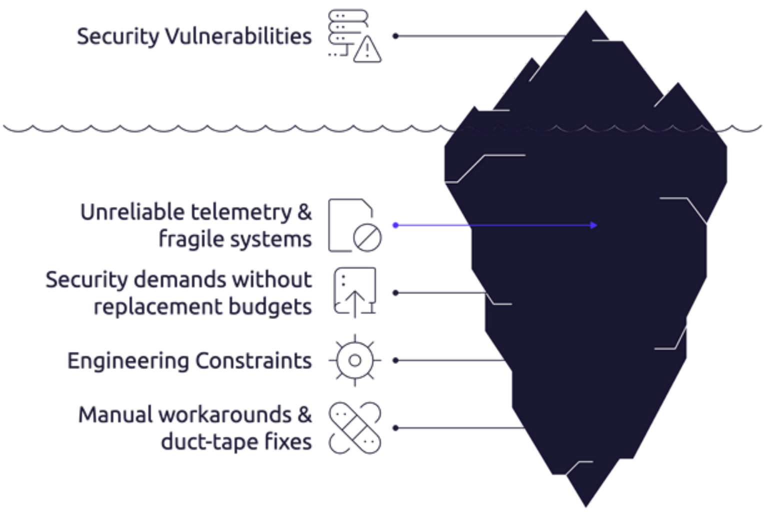
You shouldn’t have to choose between uptime and protection. SageOne secures legacy systems without reboots or delays.

OT systems are often expected to stay in service for decades, but security expectations keep rising, especially from IT teams and software vendors that assume faster upgrade cycles. You’re expected to protect systems that can’t be replaced, patched, or even touched without risk. But most security tools still assume you can do all three.

The Real-World Problem

Most legacy systems weren’t built for today’s security expectations. You can’t install agents or reboot without scheduling downtime, and even basic telemetry is often unreliable. Engineers are stuck between pressure from management and the realities of fragile systems, relying on manual tracking, isolated networks, and temporary fixes that don’t scale. And when vulnerabilities are flagged, it’s rarely clear which ones are urgent or which systems are actually exposed.

Legacy System Vulnerabilities Are Just the Tip of the Iceberg



Security Vulnerabilities
Unreliable telemetry & fragile systems
Security demands without replacement budgets
Engineering Constraints
Manual workarounds & duct-tape fixes

Why It Matters

Unprotected Legacy Systems Are Dangerous

- Easy targets for attackers
- Gaps in compliance and audit trails
- Weak points in otherwise modern networks

But Replacement Isn’t an Option

- Too risky to touch
- Too expensive to upgrade
- Too essential to take offline

That Leaves Engineers Stuck

- Pressure from security and compliance
- Limited visibility
- Manual workarounds that don’t scale

The SageOne Approach

SageOne offers engineers a way to secure aging systems without changing how those systems work. It doesn't require software agents. It doesn't need kernel access. And it doesn't assume your team can reboot machines just to install updates.

Passive Monitoring

Creates a real-time view of asset risk using passive methods that won't disrupt certified setups or delicate systems.

Vulnerability Detection

Reveals one-day and emerging vulnerabilities linked to specific assets.

Informed Decisions

Enables engineers to make smarter patch decisions, without causing new instability.

You can identify vulnerable endpoints, trace suspicious activity, and support smarter patching, with context and without disrupting fragile systems.

More Than Just Coverage

SageOne helps engineers reduce overhead while staying ahead of operational and compliance risks. It bridges visibility gaps, supports smarter patching and upgrade decisions, and integrates cleanly into existing workflows, without changing how the system runs.

Enhanced Visibility

See what's happening across all systems

Risk Assessment

Identify which vulnerabilities matter most

Workflow Integration

Fits into your team's existing processes

Informed Decisions

Make smarter choices about security actions

What Makes SageOne Different

Risk-Based, Asset-Centric Prioritization

Focuses attention on what matters most — based on asset value and exposure

Unified Intelligence Across Security Layers

Combines alerts, asset data, and system context for a clearer risk picture

Actionable Mitigation Guidance

Offers concrete steps teams can take — not just analysis

Governance for Security & Operations

Enables reporting and accountability across both OT and security teams

Take the Next Step

SageOne helps engineers protect aging systems without risky changes, but that's only part of the story. See how the platform also supports other key teams and initiatives across your OT environment:

- Secure Without Disrupting: How site teams reduce risk without triggering reboots or downtime.
- 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