

Syteca Endpoint Risk and Compliance Control (ERCC):



Continuous endpoint visibility, compliance checks, and risk scoring

Detect configuration drift and security control failures before they put your business at risk.

Syteca Endpoint Risk and Compliance Control (ERCC) continuously monitors for misconfigurations, policy drift, unapproved AI tools, and risky settings that introduce threats in the first place, keeping you audit-ready around the clock and reducing exposure before detection is even necessary. ERCC operates within the Continuous Controls Monitoring (CCM) domain and supports broader Governance, Risk & Compliance (GRC) initiatives.



Stop reacting and start preventing



Monitor AI use



Continuously monitor endpoint health



Prioritize and remediate risks



Automate compliance checks

Key capabilities of Syteca ERCC



Integrated compliance checks

Automated checks across several compliance requirements of SOC 2 core criteria and Corporate AI Usage and Baseline Policies.



Enforcement of AI use policies

Detect and control AI engine access across websites, browser extensions, desktop apps, and IDE plugins



Guided remediation

Step-by-step remediation guidance mapped to detected risks, so teams know exactly what to fix and how



Continuous health monitoring

Track endpoint health to prevent misconfigurations and security and compliance drift, and quantify risk with a clear, actionable score for every team or endpoint.

coming soon

EU AI Act compliance support, AI use metrics, proactive alerts, audit and system health reporting, Linux Agent Support (Selinux related policies)

Benefits



Fast deployment

Quick implementation with minimal technical assistance required.



Budget-friendly savings

Reduction in resources required for regular audits and incident response.



Measurable security state

Traceable endpoint health and risk scores to track improvement.



Reduced financial risks

Fewer misconfigurations mean fewer breaches and regulatory fines, lower remediation costs, and minimal reputational damage.



Easy to scale

Quickly scalable across endpoint fleets without complexity.



Faster remediation

Accelerated response times through prioritized risks and practical recommendations.

How it works

01 Collect

A lightweight agent continuously captures configuration data across OS settings, security controls, registry, services, and policies.

02 Score

The risk engine analyzes security metrics and behavioral indicators to generate a unified endpoint health score with prioritized remediation guidance.

03 Comply

Endpoint configurations are automatically audited, with results mapped to compliance frameworks and AI usage policy.

04 Remediate

Each detected risk includes a prioritized remediation guide that outlines what to fix and how to do it, thus helping your team resolve vulnerabilities quickly.

Identify and eliminate endpoint risks before they *become incidents*

The choice of 1,500+ companies worldwide



- ✓ Deploy quickly at scale
- ✓ Prevent security risks
- ✓ Lower cybersecurity expenses
- ✓ Simplify compliance monitoring

Get your free trial



Microsoft Azure
Value-add Partner



Included in the Gartner Market Guide for
Insider Risk Management Solutions



Mentioned in NIST Special Publication



Included in KuppingerCole Leadership
Compass for PAM

Syteca Inc.

24 Crescent Street Suite 403, Waltham, MA 02453 USA
+1 781-205-0530

Visit: syteca.com

European Office

Neuer Zollhof 3, 40221 Düsseldorf, Germany
+49 151 2045 3291

