SIT APPLIANCE | PROACTIVE, RECURRING TECHNICAL SECURITY CHECKS

You cannot fix risks you cannot see. SIT Appliance finds them.

SIT Appliance provides independent, proactive and recurring technical security checks before an incident occurs. It maps the IT environment it can reach, identifies systems, services, products and versions, and matches them against relevant known vulnerabilities. SIT Appliance identifies the technical conditions for a breach without carrying out the intrusion. Analysis takes place locally. No information leaves your network.

BETTER INFORMATION. BETTER DECISIONS.

Better priorities start with an accurate view of your environment.

Sound prioritisation starts with a detailed, accurate view of your environment. SIT Appliance identifies the IP-based systems covered by the checks and establishes which services, products and versions are actually present. It then matches this information against vulnerability data. A clearer view of your environment produces a more accurate vulnerability assessment and a stronger basis for deciding what to fix first.

Dedicated physical hardware. Greater precision. Automatic checks.

Connect SIT Appliance to your network. No software is installed on servers or endpoints, no privileged target accounts are needed and no server capacity is required for the analysis engine. SIT Appliance analyses the IP-based systems you choose to include, whether at your own site, other sites, IT providers or in the cloud, wherever network connectivity allows access. Checks then run automatically and repeatedly, with little ongoing effort from your team.

See your environment more clearly

SIT Appliance's dedicated physical hardware is integral to our advanced fingerprinting. It provides consistent conditions for precise identification of systems, services, products and versions. This improves vulnerability matching and risk prioritisation without installing our analysis engine on your servers.

Find relevant vulnerabilities

SIT matches the detailed view of your environment against a broad, continuously updated set of vulnerability data. Risks that go undetected never enter the priority list. SIT identifies relevant and critical vulnerabilities that other market-leading solutions miss. Our comparative tests also show that we complete scans in less than half the time. An accurate view is therefore essential: SIT identifies relevant vulnerabilities and gives you a stronger basis for deciding what to fix first.

Prioritise the right risks

SIT Risk Score (0–10) is calculated for each identified vulnerability. It goes beyond theoretical CVSS scores, combining technical severity with exploits, CISA KEV, EPSS, active exploitation, attack chains and business criticality. Your priorities reflect your own environment and business context.

Identify the conditions for a breach

SIT Appliance identifies the technical conditions for a breach and uses known multistage attacks to inform priorities, without carrying out the intrusion. This allows automatic, unattended checks in production with low operational risk.

Turn risk findings into the right actions

More information is not the goal. Better decisions are. The Top Priorities report shows which Critical and High findings to address first and recommends actions. Technical Report retains the full picture of identified risks. SIT prioritises the actions that reduce risk most in your environment.

PROACTIVE. AUTOMATIC. RECURRING.

Track threats. Take action. Verify the impact.

SIT Appliance performs scans automatically and on a recurring basis. Between scans, new vulnerabilities, zero-days and updated threat intelligence are matched against the last known state of your IT environment. New relevant threats are identified and you are notified. The next scan shows what has changed and whether your actions have made a difference.



From analysis to verified results

- **Top Priorities.** Shows which Critical and High findings to address first and recommends actions.
- **Delta Report.** Shows what has been resolved, what remains and what has appeared since the previous scan.
- **SIT Risk Index history.** Shows how your technical risk level changes over time.
- **Technical Report.** Retains the full picture of identified risks for technical analysis and follow-up.
- **Traceable follow-up.** Reports, history and exceptions support systematic security work, ISO 27001/NIS2 assessments and ongoing review. Technical results can be combined with your own assessments.

Why SIT Appliance

- **Your environment.** Your data. Your control. Local analysis in a hardened, locked-down and encrypted Appliance. No information leaves your network. Developed in Sweden.
- **Broad technical coverage.** SIT Appliance analyses IP-based systems at other sites, IT providers and in cloud environments that are reachable through your internal network.
- **Agentless and unauthenticated.** No agents or privileged accounts on target systems. SIT builds its assessment from what is visible on the network.
- **Optimise your security stack.** SIT replaces or consolidates functions where it delivers better results and complements EDR, XDR, SIEM, SOC and other systems with different roles. SIT Appliance supports integration into existing workflows.
- **Technical evidence for regulatory requirements.** Recurring checks, Delta Report and history provide traceable evidence for risk analysis, security testing and verification of remediation, including work with ISO 27001, NIS2 and Sweden's Cybersecurity Act.

See more clearly. Set the right priorities. Reduce risk.

SIT Appliance gives you a clearer technical view of your IT environment, shows what to fix first, tracks new relevant threats between scans and verifies the impact of your actions.

Better information. Better decisions. Verified risk reduction over time.

LOCAL ANALYSIS. NO INFORMATION LEAVES YOUR NETWORK. DEVELOPED IN SWEDEN.