CSAEC

CyberScan — Cyber Server Audit Engine Core

CyberScan Product Datasheet

A clear, local-first Windows security posture overview

Version 1.0 | August 2026
Microsoft Windows 10 or later | 64-bit

Product overview

CyberScan - Cyber Server Audit Engine Core is a Windows desktop security assessment application for organisations and professionals who need a clear baseline view of endpoint security. It performs twelve structured local checks, presents an overall 0-100 score, explains individual findings, and offers general local AI-assisted guidance.

The business need

Small organisations often need to answer security questionnaires, prepare for professional review, or understand which endpoint controls deserve attention. CyberScan turns selected technical indicators into an accessible, point-in-time security posture overview without presenting the result as certification or guaranteed compliance.

Key benefits

Benefit	Business value
Structured baseline	A consistent starting point across twelve important controls.
Understandable findings	Plain-language severity, context, and recommended next actions.
Local-first processing	Core checks and result processing are designed to occur on the workstation.
User-controlled sharing	No automatic report submission to CSAEC.
Local AI assistance	General explanations without requiring a cloud-based AI subscription.

Who CyberScan is for

- Small and medium-sized businesses
- Independent professionals
- IT administrators and cybersecurity consultants
- Organisations preparing cyber-risk questionnaires
- Teams seeking an initial endpoint security review
- Management teams needing an understandable security posture summary

Core capabilities

Capability	What it delivers
Security score	A 0-100 summary across twelve controls.
Individual findings	Clear status, severity, explanation, and corrective guidance.
Network insight	Local device discovery and port/service exposure indicators.
Vulnerability-oriented checks	Known vulnerability and local web service assessment using specialised components where available.
Reports and assistance	User-controlled report preparation and an optional CSAEC contact workflow.

The twelve security controls

#	Control	#	Control
1	Windows Firewall Status	7	Windows Security Update Configuration
2	Disk Encryption Status	8	Antivirus or Endpoint Protection Status
3	Operating System Security and Integrity	9	Backup Configuration
4	Local Network Port Exposure	10	Wireless and Bluetooth Exposure
5	Local Network Device Discovery	11	Known Vulnerability Assessment
6	Automatic Screen-Lock Configuration	12	Local Web Service Vulnerability Assessment

Security score and findings

The overall score summarises the twelve controls, while individual findings remain the most important basis for action. Different weaknesses can have different operational impacts, and the result reflects the system condition at assessment time.

Score	Classification	Interpretation
85-100	Good	A sound baseline is indicated; review every finding and maintain controls.
60-84	Improvement Recommended	One or more controls merit attention and prioritised follow-up.
0-59	At Risk	Material weaknesses may be present; timely validation and action are recommended.

Responsible interpretation
A high score does not guarantee complete security, regulatory compliance, cyber-insurance acceptance, or successful audit results.

Local AI assistance

The integrated local AI assistant helps users understand security findings and provides general remediation guidance without requiring a cloud-based AI subscription. AI responses may contain errors, must be reviewed before changes are applied, and never autonomously modify Windows settings.

Local-first privacy approach

- Core security checks are designed to run locally.
- Scan results are processed locally.
- No security report is automatically submitted to CSAEC.
- External sharing follows a deliberate user action.
- Email clients and optional external components may involve third-party software or services.

Typical use cases

Use case	How CyberScan helps
Initial endpoint review	Establishes a readable baseline before deeper technical work.
Questionnaire preparation	Helps gather preliminary information for cyber-risk questions.
Post-change recheck	Provides a new point-in-time view after approved security improvements.
Consulting intake	Creates a structured starting point for discussion with qualified personnel.
Management overview	Summarises selected endpoint security controls without excessive technical detail.

Technical summary

Area	Summary
Platform	Microsoft Windows 10 or later, 64-bit edition
Application model	Windows desktop assessment application
Assessment scope	Twelve local security controls
Network components	Nmap for discovery, port inspection, and vulnerability-oriented checks where available
Web assessment	Wapiti for selected reachable local web services where available
AI	Local explanatory assistant; optional local runtime configuration
Processing	Local-first, with user-controlled report sharing
Hardware note	Detailed hardware requirements may vary according to the selected application build and local AI configuration.

Important limitations

- CyberScan is an initial assessment tool, not an antivirus, EDR platform, managed SOC, or continuous-monitoring platform.
- It is not a penetration-testing replacement, formal certification tool, regulatory compliance guarantee, or automatic remediation system.
- Network and vulnerability results can be affected by filtering, permissions, target state, and component availability.
- Vulnerability checks may produce false positives or false negatives.
- A completed scan does not prove that the system is free from vulnerabilities.
- Significant findings and changes should be validated by qualified personnel.

CSAEC professional support

CyberScan can provide a structured starting point for CSAEC assistance. The optional contact workflow prepares a user-reviewed report or request; it does not automatically submit information or guarantee a particular response outcome.

Take the next step

Run CyberScan to establish an initial Windows security posture overview. Review each finding, prioritise material issues, and use the authorised CSAEC contact channel when professional validation or remediation planning is required.

Legal disclaimer

CyberScan provides preliminary technical assessment and informational decision support. Results, scores, reports, and AI guidance are not certifications, compliance determinations, insurance approvals, or guarantees of protection. Users remain responsible for authorising scans, reviewing findings, validating changes, and protecting shared information.