Your whole security stack, checked every day, mapped to NIS2.

ARGOS continuously audits the configuration of the systems an organisation already runs, from Microsoft 365 and Active Directory to firewalls, endpoint protection, backup, servers, databases and cloud. It reads each system through its own management API with read-only access, runs **1,330** security checks, scores every system and every client on one scale, and alerts the moment something drifts. Every finding comes with the risk, the exact fix and its NIS2 and ISO 27001 reference.

54
supported systems across identity, network, endpoint, backup, servers and cloud

1,330
security checks with risk, remediation and framework mapping

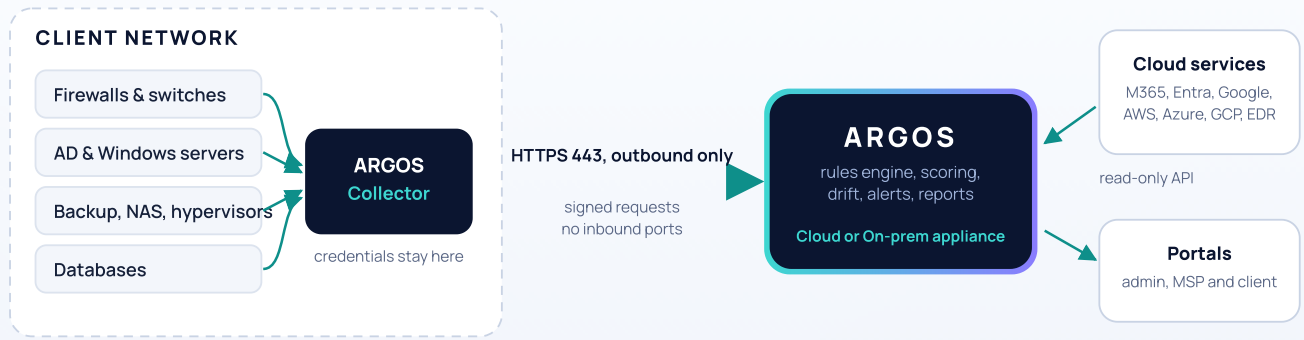
516
change-watch templates for alerts on configuration changes

24 h
daily scans as standard, down to hourly, with full drift history

0
write permissions: ARGOS only reads configuration, never changes it

Key features

- **One view across every vendor.** A single posture score per system and per client, with findings ranked by severity and exploitability.
- **Continuous, not yearly.** Scheduled scans keep every result; the history shows what changed, when, and who changed it where audit logs allow.
- **Alerts that matter.** Failed checks, configuration drift, failed or missing backups, by e-mail, Microsoft Teams and the daily digest. Snooze for 1, 10 or 30 days, or mute with a reason.
- **Clear remediation.** Every finding explains the risk and the exact steps to fix it, with optional fix scripts shown for review and never executed.
- **Audit-ready compliance.** Findings mapped to NIS2 Article 21(2) measures, ISO/IEC 27001:2022 Annex A and CIS Controls v8, with evidence packs for auditors.
- **Executive reporting.** A monthly management report alongside the technical findings report.
- **Client portal.** Each client sees its own live posture, alerts and reports; client admins manage their own users.
- **Built for MSPs.** Multi-tenant console with white-label branding: every client in one place, under the partner's own brand.



Cloud services are read directly through their APIs. On-premises systems are read by the on-site Collector, or ARGOS runs entirely inside the network as a virtual appliance, including air-gapped.

ARGOS

SUPPORTED SYSTEMS

54 systems, 1,330 checks

Figures are the number of security checks per system in rule set `2026.11.14.4`. **CLOUD** = read over the vendor's cloud API.

IDENTITY AND CLOUD — 7 SYSTEMS · 267 CHECKS

Microsoft 365	CLOUD	71
Microsoft Azure	CLOUD	41
Amazon Web Services	CLOUD	31
Google Cloud	CLOUD	35
Google Workspace	CLOUD	28
Okta	CLOUD	25
Active Directory		36

NETWORK AND EXPOSURE — 19 SYSTEMS · 483 CHECKS

External exposure	CLOUD	54
FortiGate		31
WatchGuard Firebox		27
Palo Alto Networks (PAN-OS)		22
Sophos Firewall		20
pfSense		20
OPNsense		20
MikroTik RouterOS		18
UniFi Network		19
Cisco Meraki	CLOUD	21
Network Discovery		5
Check Point firewall		33
Cisco ASA / Firepower		33
SonicWall firewall		26
Zyxel firewall (USG FLEX / ATP)		32
DrayTek Vigor router		17
Network switches		34
TP-Link Omada		27
Ruckus wireless		24

ENDPOINT, EDR AND RMM — 11 SYSTEMS · 172 CHECKS

Microsoft Defender for Endpoint	CLOUD	21
ESET PROTECT	CLOUD	24
Bitdefender GravityZone	CLOUD	19
CrowdStrike Falcon	CLOUD	19
SentinelOne Singularity	CLOUD	20
Sophos Central	CLOUD	19
Trend Vision One / Apex One	CLOUD	16
Kaspersky Security Center		19
NinjaOne	CLOUD	5
Datto RMM	CLOUD	4
Action1 (patch management)	CLOUD	6

BACKUP AND STORAGE — 4 SYSTEMS · 78 CHECKS

Veeam Backup & Replication		22
Acronis Cyber Protect Cloud	CLOUD	18
Synology NAS (DSM)		19
QNAP NAS		19

SERVERS, VMS AND DATABASES — 11 SYSTEMS · 300 CHECKS

VMware vSphere		18
Microsoft Hyper-V		21
Proxmox VE		21
Windows Server		29
Linux Servers		23
Exchange Server (on-premises)		20
Server management (iDRAC / iLO / BMC)		23
Microsoft SQL Server		40
MySQL / MariaDB		35
PostgreSQL		35
Oracle Database		35

VULNERABILITY RESULTS — 2 SYSTEMS · 30 CHECKS

Vulnerability Scan Results		11
Website Vulnerability Scan	CLOUD	19

Each system is read through its own management interface with a dedicated read-only account or API key. Where the platform allows, ARGOS verifies that the credential it was given cannot write and reports any excess permission. Results of external vulnerability scanners can be imported alongside the configuration findings.

Platform specifications

CAPABILITY	SPECIFICATION
ASSESSMENT	
Security checks	**1,330** checks across **54** systems, versioned rule set with release notes
Severity levels	Critical, high, medium, low, informational; ranked by severity and exploitability
Scoring	One posture score and grade per system and per client, trended over time
Scan schedule	On demand, or scheduled from hourly to weekly per system; daily as standard
Access model	Read-only by design; excess write permissions detected and reported
Remediation	Risk, step-by-step fix and references per finding; optional fix scripts for review only; AI-assisted explanations
MONITORING AND ALERTING	
Drift detection	Every scan stored; new, fixed and changed findings shown per scan with full history
Change watch	**516** templates, e.g. admin group membership, new firewall rule, new Conditional Access policy, sign-in from a disallowed country; changes attributed to the actor where audit logs allow
Backup monitoring	Failed, missing or disabled jobs and storage capacity alerts
Notification channels	E-mail, Microsoft Teams, daily digest for cloud systems, in-portal alert inbox
Alert handling	Acknowledge, snooze 1 / 10 / 30 days or custom, mute with a recorded reason, undo
REPORTING AND COMPLIANCE	
Reports	Technical findings report, monthly executive report, audit evidence packs
Frameworks	NIS2 Article 21(2) measures (a) to (j) and Article 23, ISO/IEC 27001:2022 Annex A (53 controls), CIS Controls v8 (93 safeguards)
Remediation workflow	Assign, track and verify fixes; accepted risks recorded with a reason
PORTAL AND MULTI-TENANCY	
Consoles	Administrator / MSP console and a separate client portal; each client sees only its own data
White-label	Partner logo, colours and domain on the portal and reports
Self-service onboarding	Guided, step-by-step setup for every system; client-submitted systems wait for approval
PLATFORM SECURITY	
Authentication	Mandatory TOTP MFA for administrators, on by default for clients; scrypt password hashing, 12-character minimum; progressive back-off, never a permanent lockout
Sessions and web	Server-side sessions (random 256-bit id), HttpOnly secure cookies, HSTS, CSRF tokens, strict Content Security Policy
Secret storage	Write-only encrypted vault, AES-256-GCM bound to client and secret name; on-site credentials never leave the Collector
Software integrity	Collector and appliance updates signed with an offline release key and verified before install

Check severity profile



Critical **69** · High **393** · Medium **644** · Low **219** · Info **5**

NIS2 Article 21(2) coverage

- **a** Risk analysis and security policies
- **b** Incident handling
- **c** Business continuity and backup
- **d** Supply-chain security
- **e** Secure maintenance, vulnerability handling
- **f** Effectiveness assessment
- **g** Cyber hygiene and training
- **h** Cryptography and encryption
- **i** Access control and asset management
- **j** MFA and secured communications

Deployment options and requirements

	ARGOS CLOUD	ON-SITE COLLECTOR	ON-PREM APPLIANCE
Role	Hosted, multi-tenant service	Reads on-premises systems for ARGOS Cloud	Runs all of ARGOS inside the client network
Delivery	Web browser	Linux package, Docker image, Windows package	OVA virtual appliance
Platform	Any modern browser	Linux: Debian, Ubuntu, RHEL with Python 3.10+; x86-64 or ARM64 Docker: non-root container Windows: Windows Server 2016 or later (x64), embedded Python, no MSI or .NET needed	VMware vSphere 8; Debian 13 base with a self-contained runtime
Sizing	None (hosted)	2 vCPU, 4 GB RAM, 20 GB disk	**2** vCPU, **4** GB RAM, **60** GB thin-provisioned disk
Network	HTTPS 443	Outbound HTTPS 443 only; no inbound ports	HTTPS 443 for the console; outbound optional
Credentials	Encrypted vault (AES-256-GCM)	Stored on the Collector, encrypted and host-bound (DPAPI on Windows)	Encrypted vault on the appliance
Enrolment / setup	Account with MFA	One-time 24-hour enrolment token; local setup page	Console screen shows address and certificate fingerprint; web setup
Updates	Continuous	Signed automatic updates	Signed release bundles; online, or uploaded by hand when air-gapped
Data location	Data centres in the European Union	Sends scan results only	Stays on site; encrypted nightly backup to an SMB share
Current version	Rule set `2026.11.14.4`	`1.4.0`	`1.0.17`

Editions

FEATURE	ONE-OFF ASSESSMENT	ESSENTIALS	PROFESSIONAL	ENTERPRISE
Monitored systems	3, 6 or 10 (S, M, L)	5, up to 10	20, up to 35	40, no cap
Scan frequency	Once	Weekly	Daily	Up to hourly
History retained	Report	90 days	1 year	Unlimited
On-site Collectors / portal users	1 / 2	1 / 2	3 / 10	Unlimited
Findings report and remediation guidance	●	●	●	●
Alerts and drift history	–	●	●	●
Self-service onboarding	●	●	●	●
Executive report, remediation workflow	–	–	●	●
External exposure, External Intelligence	–	–	●	●
Change Watch alerts	–	–	●	●
Website vulnerability scan	–	–	1 site	3 sites
Audit evidence packs	–	–	–	●

Add-ons for any edition: Credential Exposure (credential leak monitoring), AI-assisted explanations. External Intelligence, the website scan (authorised sites only) and Credential Exposure are cloud only. **Deployment:** every edition runs in ARGOS Cloud or on the on-prem appliance. **MSP partners:** white-label, multi-tenant console. Licensed per client, not per user or device. Limits can be tailored per agreement.

SALES AND INFORMATION

ITACC Solutions

101 Irakleitou Str., 15238 Chalandri, Athens, Greece

Tel. +30 210 710 3540

sales@itacc.gr · info@itacc.gr

Specifications reflect rule set `2026.11.14.4` (2026-11-14) and are subject to change without notice. Feature availability depends on the edition and the deployment option. Check counts grow with each rule-set release. All product names and trademarks are the property of their respective owners and are used only to identify supported systems; ARGOS is not affiliated with or endorsed by them.

Document DS-ARGOS-001, revision 1.0, November 2026.