SurfaceScan

EXTERNAL ATTACK SURFACE MANAGEMENT

Know Your Attack Surface

Continuous, automated security monitoring of everything your organisation exposes to the internet, so you can fix what matters before attackers find it.

surfacescan.dev

Automated external security monitoring for ISO 27001 & NIS2 compliance

THE PROBLEM

What Is Your Attack Surface?

Your attack surface is everything your organisation exposes to the internet: domains, subdomains, IP addresses, open ports, web applications, email configurations, and TLS certificates. Every one of these is a potential entry point for attackers.

The challenge? Most organisations don't have a complete picture. Subdomains get created and forgotten. Certificates expire unnoticed. Ports are left open after a migration. New services go live without security review. Your attack surface is constantly changing, and what you can't see, you can't protect.

Shadow infrastructure

Forgotten subdomains, test environments, and legacy services that no one monitors but attackers can still find.

Configuration drift

TLS certificates expire, email security records weaken, and new ports open, often without anyone noticing until it's too late.

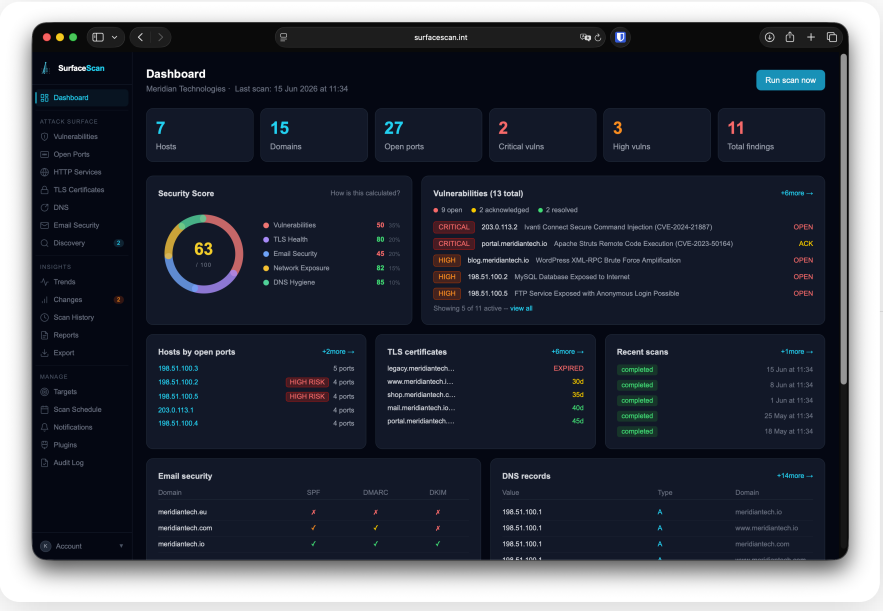
Compliance pressure

Frameworks like ISO 27001 and NIS2 require continuous risk assessment, not just an annual penetration test.

Limited visibility

Internal security tools watch the perimeter from inside. Attackers see you from the outside. And so should you.

SurfaceScan gives you that outside-in view. It continuously discovers, maps, and monitors your entire external attack surface, automatically, and tells you exactly what needs attention.



HOW IT WORKS

Automated, Continuous Scanning

SurfaceScan runs a multi-stage scanning pipeline against your external assets. You provide your root domains and IP ranges. The platform handles everything else. No agents to install, no firewall changes required. Scans run on a schedule you define, or on demand.

01
Asset Discovery
Automatically enumerates all subdomains and related hostnames across your registered domains.

02
DNS Resolution
Resolves every discovered hostname to map your live infrastructure and detect orphaned DNS records.

03
Port Scanning
Identifies open ports across all discovered IP addresses and classifies them by service and risk level.

04
TLS Inspection
Audits every certificate for expiry, weak protocols, self-signed certs, and configuration issues.

05
Web Service Probing
Identifies HTTP services, technologies, response codes, and server configurations across your surface.

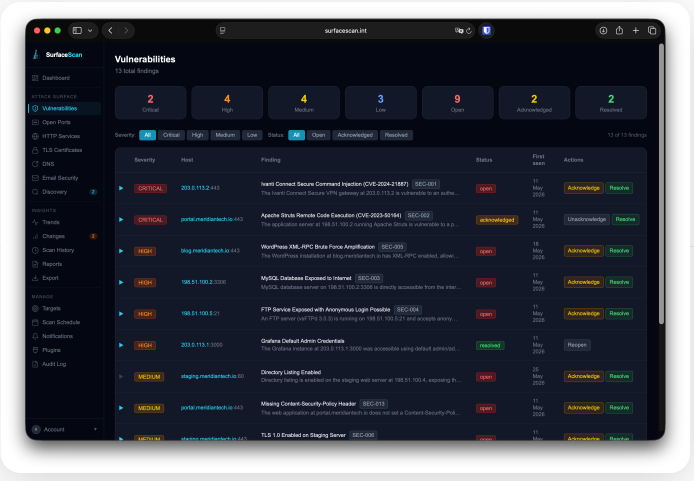
06
Email Security
Validates SPF, DMARC, and DKIM configurations to ensure your domains are protected against spoofing.

07
Vulnerability Detection
Runs thousands of security checks against discovered services to identify known vulnerabilities and misconfigurations.

08
Change Detection
Compares every scan to the previous one and highlights what's new, changed, or resolved. Nothing slips through.

09
Reporting
Generates detailed security reports with findings, severity ratings, and remediation guidance, ready for auditors.

Every finding is classified by severity, linked to the affected asset, and tracked across scans. When something gets fixed, SurfaceScan confirms it automatically on the next run.



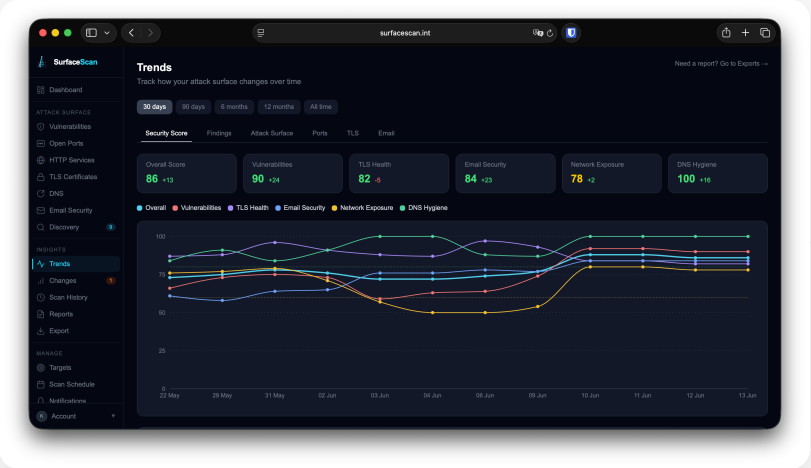
VISIBILITY

Dashboard & Reporting

Everything comes together in a single dashboard. At a glance, you see your security posture, open findings, asset counts, and how your score has changed over time. No digging through spreadsheets or waiting for a consultant's report.

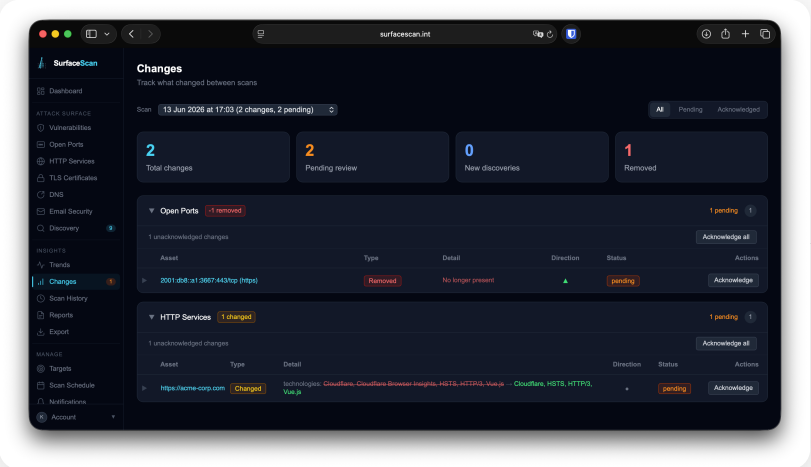
Security Score

Your security score is a single number (0-100) that represents your overall external security posture. It's calculated from five weighted categories: vulnerabilities, TLS health, email security, network exposure, and DNS hygiene. It updates automatically after every scan. It tells you exactly where you stand and what to fix first.



Change Detection

Every scan is compared to the previous one. New subdomains, changed TLS certificates, newly opened ports, resolved vulnerabilities. Everything is surfaced in a dedicated Changes view. Acknowledge changes individually or in bulk, add notes and ticket references, and keep a clean record for audit purposes.

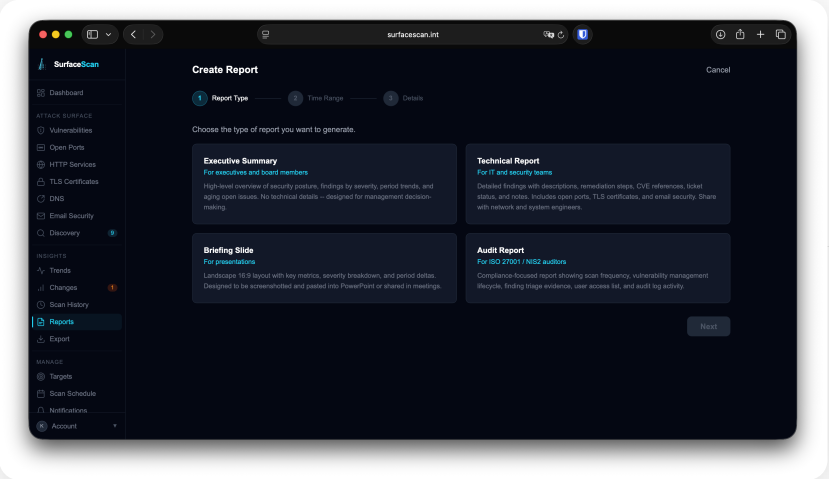


EVIDENCE

Reporting & Audit Trail

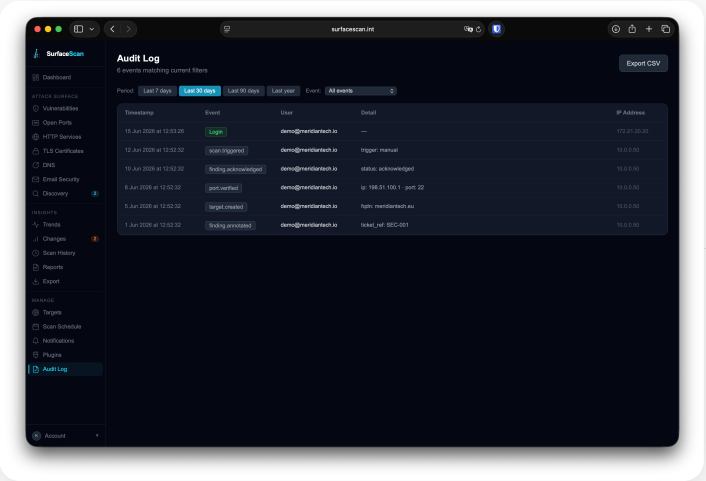
Reports & Exports

Generate professional PDF reports at any time: executive summaries for management, technical reports for your team, or audit reports for external assessors. Export raw data in CSV, JSON, Excel, or PDF format with filters for severity, status, and asset category. All data is yours.



Audit Trail

Every action (finding acknowledgments, status changes, report downloads, scan triggers) is logged with timestamps and user attribution. Filter by event type, export as CSV, and present it directly to auditors as evidence of continuous security management.



COMPLIANCE

Built for ISO 27001 & NIS2

SurfaceScan isn't just a scanning tool. It's designed to generate the evidence your compliance framework demands. Whether you're working toward ISO 27001 certification or meeting NIS2 obligations, the platform maps directly to the controls auditors look for.

ISO 27001, A.8.8

Technical Vulnerability Management

Continuous vulnerability scanning with severity classification, remediation tracking, and historical records across scan runs.

ISO 27001, A.8.9

Configuration Management

TLS configuration auditing, email security validation, and change detection between scan runs to identify drift.

NIS2, ART. 21.2(D)

Supply Chain Security

Discovery of third-party assets and services exposed through shared infrastructure, DNS records, and TLS certificate SANs.

NIS2, ART. 21.2(E)

Vulnerability Handling

Structured finding lifecycle (open, acknowledged, risk accepted, resolved) with notes, ticket references, and full audit trail.

ISO 27001, A.5.23

Cloud Service Security

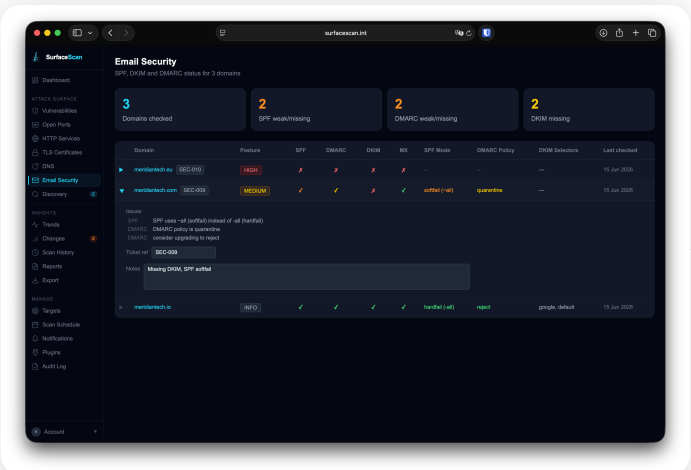
Identification of cloud-hosted services, CDN detection, and external exposure mapping across your infrastructure.

ISO 27001, A.8.16

Monitoring Activities

Scheduled, automated scans with trend analysis showing security posture over time. Notifications on new findings or changes.

Every report, export, and audit log entry SurfaceScan produces is designed to be handed directly to an assessor. No reformatting, no manual compilation. The evidence is built into the workflow.



WHY SURFACESCAN

What You Get

- **Continuous monitoring.** Scheduled scans run automatically. Your security posture is assessed regularly, not just once a year during a penetration test.
- **Complete visibility.** Discover subdomains, services, and infrastructure you didn't know were exposed. See your organisation the way an attacker sees it.
- **Compliance-ready evidence.** PDF reports, data exports, audit logs, and finding lifecycle tracking, mapped to ISO 27001 and NIS2 controls out of the box.
- **Actionable findings.** Every vulnerability is classified by severity with clear remediation guidance. Track progress, add ticket references, and mark findings as resolved.
- **Change detection.** Know immediately when something changes in your attack surface. New assets, expired certificates, opened ports. Nothing goes unnoticed.
- **Zero deployment.** No agents, no firewall changes, no infrastructure to manage. Add your domains, and the first scan starts immediately.

See your attack surface clearly

Start monitoring your external security posture today. No setup, no contracts, just add your domains and go.

surfacescan.dev

Multi-tenant

Manage multiple organisations from a single account with isolated data and access controls.

MFA Protected

TOTP-based multi-factor authentication on every account. Your security data stays secure.

European Hosted

Infrastructure hosted in Europe. Your data stays close and under EU data protection regulation.