

ATTACK SURFACE MANAGEMENT.



Every internet-facing asset an organization exposes — **domains, subdomains, cloud services, and forgotten infrastructure** — mapped continuously, not once a year. You cannot secure what you do not know you own.

- SHADOW IT DISCOVERY
- ATTACK SURFACE SCORING
- CONTINUOUS MONITORING
- FRAMEWORK MAPPING

01 THE MECHANISM

Asset Discovery
Continuously finding **domains, subdomains, IPs, and cloud assets** you own but may not actively track.

Exposure Assessment
Technical checks across **DNS, TLS, email authentication, headers, and service exposure** for every discovered asset.

Drift Detection
Flagging **new, changed, or forgotten assets** as the footprint shifts over time.

02 THE FLOW

The Discovery Cycle CONTINUOUS

1

Seed domains expand into a full external footprint via **subdomain enumeration and certificate transparency logs**.

2

Newly discovered assets are automatically checked against a **technical control catalog** — DNS, TLS, headers, email auth, service exposure.

3

Findings are **scored and mapped to framework controls** for prioritization.

The Drift Cycle ONGOING

1

A **baseline snapshot** of the known-good footprint is established.

2

Recurring scans **compare current state against baseline** to surface new or changed assets.

3

Unowned or forgotten assets — shadow IT, orphaned subdomains, expired certs — trigger review.

03 DISCOVERY MODULES & COVERAGE

MODULE	WHAT IT SURFACES
Subdomain & DNS Enumeration	Forgotten subdomains, stale DNS records, and zone misconfigurations.
Email Authentication & TLS	Weak SPF, DKIM, and DMARC; expired certificates and deprecated protocols.
HTTP Security Headers	Missing CSP, HSTS, and other browser-enforced protections.
Service & Config Exposure	Open ports, exposed admin panels, directory listings, and leaked config files.

04 EXPOSURE SIGNALS COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Annual Penetration Test	No	Point-in-time; the footprint changes within weeks of the report.
Asset Inventory Spreadsheet	No	Manually maintained; drifts out of date the moment it's saved.
Single-Domain Vulnerability Scan	No	Misses subdomains, shadow IT, and assets outside the known scope.
Cloud Provider Security Dashboard	No	Only sees what's provisioned inside that one cloud account.
Combined Attack Surface Management (Discovery + Assessment + Drift Detection)	Yes	Continuously maps the full external footprint, including what you didn't know you owned.

ATTACK SURFACE.

DISCOVER · ASSESS · MONITOR

05 PROGRAM OPERATIONS

You can't protect what you don't know you own. Shadow IT and forgotten assets are a leading root cause of breach.

Discovery must be continuous, not periodic. New subdomains, cloud instances, and microsites appear between assessment cycles.

Not every finding is equal. Severity and breadth logic keeps one repeated header issue from drowning out a critical exposed admin panel.

Unauthorized scanning carries legal risk. Always operate from a documented authorization gate, even for your own assets.

06 CONTROL MAPPING

OWASP TOP 10:2025

Community-ranked **application security risk categories**.

OWASP ASVS 5.0

Verification-level requirements for **application security controls**.

NIST CSF 2.0

Identify function coverage for asset and risk management.

CIS CONTROLS V8.1

Inventory and control of enterprise assets safeguards.

07 WHAT THIS DOES NOT SOLVE

Internal network exposure

Sees the **internet-facing perimeter** only, not what's reachable from inside the network.

Zero-day vulnerabilities

Flags **known misconfigurations** and CVEs, not undisclosed flaws.

Social engineering

No technical scan detects a **convincingly worded phishing email**.

Insider misuse of access

Authorized users **abusing valid credentials** falls entirely outside scan scope.

08 MYTHS VS. REALITY

MYTH	REALITY
"We did a pentest last year, we're covered."	Pentests are point-in-time — the footprint has already changed since the report shipped.
MYTH	REALITY
"IT approved every domain and subdomain we run."	Marketing, sales, and business units routinely spin up assets IT never sees.
MYTH	REALITY
"Our cloud dashboard shows everything."	It only shows what's provisioned in that one account — not forgotten or shadow accounts elsewhere.
MYTH	REALITY
"A scan of our main site covers us."	Subdomains, staging environments, and orphaned assets sit entirely outside that scope.
MYTH	REALITY
"More scanning tools mean better coverage."	Overlapping tools without a shared control catalog create duplicate noise, not more visibility.

09 SPEAK THE PROGRAM — KEY TERMS

ATTACK SURFACE

Every internet-facing **asset, service, and entry point** an organization exposes, known or not.

SHADOW IT

Technology assets provisioned **outside official IT oversight** and inventory.

CERTIFICATE TRANSPARENCY LOG

Public record of issued TLS certificates used to **discover subdomains**.

ASSET DRIFT

The gap between an organization's **assumed footprint** and its actual, current one.

ATTACK SURFACE SCORE

A composite metric weighing findings by **severity and breadth** across the footprint.

AUTHORIZATION GATE

A control requiring **documented consent** before any external scan begins.