Attack surface: what do you expose to the internet that you don't know about?

This month, build your external inventory from registrar accounts, DNS zones, certificate transparency logs, cloud accounts and IP allocations, and get free exposure alerts from Shadowserver and your national CERT. Then compare it with an outside scan every week, and give each exposed service an owner and a reason to be public, or take it off the internet.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.2**	**IT and security teams in organizations of any size that need to know what they expose to the internet**

Latest version
sheets.einblick.dev/attack-surface/

If you only do five things

1. **Build the inventory from records, not memory.** List every domain, DNS record, cloud endpoint and IP range you hold. The patching sheet's deadlines only work on systems someone knows about.
2. **Get the free outside view this week.** Send your IP ranges and domains to Shadowserver[1] and, where it takes sign-ups, your national service. In Germany, CERT-Bund reports to the abuse contact registered for each IP range[17].
3. **Give every exposed service an owner and a reason.** CISA advises closing or restricting every port without a documented operational need[2]. Block unclaimed services after a notice period, keeping a quick way back.
4. **Take remote access and databases off the internet.** Put them behind a VPN or gateway with phishing-resistant MFA[2]. Exploits opened 32% of Mandiant's 2025 intrusions, and the estimated mean time to exploit is -7 days, before the patch is out[4].
5. **Watch for leaked secrets and passwords.** Turn on secret scanning and leaked credential alerts. Of the ransomware victims Verizon found with a credential or infostealer leak that year, half had one within 95 days before being named[5].

Build the external inventory

1. **Start from what you pay for.** Pull domains from registrar accounts, IP ranges from your regional internet registry and provider contracts, and cloud and SaaS accounts from finance records.
2. **Export every DNS zone.** Flag CNAMEs that point at cloud services: that is where takeovers start[6].
3. **Search certificate transparency logs.** Public CAs are expected to log every certificate they issue, so a search for your domains, for example on crt.sh, shows hostnames nobody listed. Attackers read the same logs[7].
4. **Export public endpoints from each cloud.** List public IPs, load balancers, CDN, storage and app hostnames with Azure Resource Graph[6], AWS Config[9] or your cloud's equivalent.
5. **Claim your SaaS tenants.** Self-service sign-ups can leave unmanaged Entra directories on your domains; take them over by verifying the domain[8]. Do the same in other SaaS that verifies domains.
6. **Scan what you own and compare.** Scan from outside every week. Anything that answers but isn't listed gets an owner or gets switched off.

What to look for in every scan

- **Remote access and OT protocols.** CISA's minimum list of ports to check includes SSH, Telnet, RDP, VNC, TeamViewer, Modbus, DNP3 and BACnet[2]. Firewall and VPN admin pages are in the edge devices sheet.
- **Databases.** Elasticsearch, MongoDB and other data stores should never answer from the internet; Shadowserver reports open ones daily[1]. Cloud storage is in the cloud configuration sheet.
- **Forgotten and temporary systems.** Services that should have been decommissioned or kept internal, and old configuration pointing at former suppliers[10]. Include dev, test and file transfer servers.
- **Dangling DNS.** A CNAME to a deleted resource lets an attacker claim the name, serve content and get a valid certificate on your subdomain[6]. Any AWS account can claim a deleted S3 bucket or Elastic Beanstalk name[9].

Leaked credentials and secrets

- **Scan every repository and its history.** GitHub scans all branches and history for free on public repositories; private ones need Secret Protection[11], but Team and Enterprise plans get a free assessment[12]. GitGuardian counted 28.6 million new secrets in public GitHub commits in 2025[13].
- **Revoke first, then clean up.** Rewritten history still lives in forks and clones[14]. GitGuardian found 64% of valid secrets from 2022 still working four years later[13].
- **Look beyond code.** About 28% of GitGuardian's secret incidents came only from collaboration and productivity tools[13].
- **Act on leaked password alerts.** Entra ID's leaked credentials detection works with Entra ID Free; on-premises passwords need password hash sync[15]. Reset the password and revoke sessions when it fires.

What changed in 2026

- **The NCSC retired Web Check and Mail Check** on 31 March 2026 and recommends commercial EASM instead[19].
- **Exposed PLCs at US water utilities came under attack.** CISA saw more than 100 water sector entities targeted in July 2026, often via PLCs on cellular modems[2], which may not show up in routine scans[3].
- **Exposure will help set US federal patch deadlines.** From December 2026, BOD 26-04 deadlines treat a system as exposed if any method finds it so. Agencies attest public IPs and domains quarterly[20].
- **New S3 buckets can avoid name takeover.** Buckets in S3's account regional namespaces can't be claimed by another account. They aren't the default, and older buckets keep the risk[9].

Free help from outside

- **Shadowserver.** Free daily reports on exposed services for the IP ranges and domains you control[1].
- **NCSC Early Warning (UK).** Free alerts on vulnerable or exposed services for any UK organization that registers its IPs and domains[16].
- **CERT-Bund (Germany).** It reports infected systems and open services to the network operator of each IP range[17]. Essential and important entities can ask the BSI to check their public systems[18].
- **Commercial EASM.** It adds continuous discovery, takeover checks and history. Ask how it validates findings and how fresh its data is[10].

What you can skip

- **A commercial EASM before you have owners.** Discovery without owners makes a longer list, not a smaller attack surface. Use the free sources first.
- **Hiding from scanners.** Exposed services are scanned daily anyway[10]. BOD 26-04 even has agencies unblock CISA's scanners[20].
- **Perfect TLS grades on brochure sites.** Close exposed remote access, databases and dangling DNS first.

Measure exposure over time

- **Exposed services without an owner.** Aim for zero, counted weekly.
- **High-risk exposures.** Remote access, databases, admin pages and OT protocols on the internet, each with an approved exception that expires.
- **Found by someone else first.** New assets you learned about from a scanner, CERT or supplier instead of your own records. This should fall each quarter.
- **Time to close.** From first sighting to closed or shielded. Aim for one working day for high-risk exposures.
- **Valid leaked secrets.** Count them and name the oldest.

Mistakes that cost the most

- **Scanning only the ranges you know.** Cloud, SaaS and supplier systems sit on other addresses, and vendor-installed modems may not show up in routine scans[3]. Discover from DNS and certificates too.
- **Deleting the resource before its DNS record.** Delete the record, wait out the TTL, then delete the resource[9].
- **Notices to a mailbox nobody reads.** CERT-Bund sends its reports to the abuse contact registered with RIPE for each IP range[17]. Make sure yours reaches a person and providers forward reports for your addresses.

What this looks like at your size

Small team, no security staff

- Ask your IT provider for one list of domains, DNS records, public IPs and cloud accounts, each with an owner.
- Keep all domains in one registrar account with MFA, and subscribe to Shadowserver and your national service.
- On GitHub Team or Enterprise, run the free secret risk assessment and rotate what it finds[12].

Growing, with IT or security staff

- Run discovery weekly from DNS exports, CT logs and cloud inventories, and compare it with the inventory.
- Open a ticket with an owner for every new exposure, and add a dangling DNS check to decommissioning.
- Report the five measures above every month.

Enterprise or regulated

- Choose a commercial EASM with the NCSC's buyer questions and feed it your cloud and asset inventories[10].
- Have each business unit attest its public IPs and domains quarterly and list systems suppliers host for it, as BOD 26-04 requires of agencies[20].
- Add acquisitions, subsidiaries and OT sites, including vendor-installed modems, to discovery.

Version history

5 Nov 2026, version 1.2 Dropped CISA Cyber Hygiene, which serves only US organizations.

Sources

1. Subscribe to Reports. Shadowserver Foundation, checked 4 Nov 2026. shadowserver.org
2. Internet Exposure Reduction Guidance. CISA, revised 21 Aug 2026. cisa.gov
3. CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs. CISA, 30 Jul 2026. cisa.gov
4. M-Trends 2026: Data, Insights, and Strategies From the Frontlines. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
5. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
6. Prevent dangling DNS entries and avoid subdomain takeover. Microsoft Learn, 20 Jul 2026. learn.microsoft.com
7. RFC 9162: Certificate Transparency Version 2.0, Sections 1 and 11.5. IETF, Dec 2021. rfc-editor.org
8. Admin takeover of an unmanaged directory. Microsoft Learn, 18 Jun 2026. learn.microsoft.com
9. Threat tactic spotlight: Subdomain takeover. AWS Security Blog, 16 Jun 2026. aws.amazon.com
10. External attack surface management (EASM) buyer's guide. NCSC (UK), 18 Sep 2025. ncsc.gov.uk
11. Secret scanning. GitHub Docs, checked 4 Nov 2026. docs.github.com
12. Running the secret risk assessment for your organization. GitHub Docs, checked 5 Nov 2026. docs.github.com
13. The State of Secrets Sprawl 2026 (vendor research report). GitGuardian, 2026. gitguardian.com
14. Removing sensitive data from a repository. GitHub Docs, checked 4 Nov 2026. docs.github.com
15. Risk detections in Microsoft Entra ID Protection. Microsoft Learn, 21 Oct 2026. learn.microsoft.com
16. Early Warning. NCSC (UK), checked 4 Nov 2026. ncsc.gov.uk
17. CERT-Bund Reports: FAQ. BSI, checked 4 Nov 2026. bsi.bund.de
18. BSI-Gesetz (BSIG), § 15. BMJV (Germany), checked 4 Nov 2026. gesetze-im-internet.de
19. NCSC to retire Web Check and Mail Check. NCSC (UK), 6 Nov 2025. ncsc.gov.uk
20. BOD 26-04: Prioritizing Security Updates Based on Risk. CISA, 10 Jun 2026. cisa.gov