

# Attack Surface Management

Most breaches start with an asset the organisation had lost track of. Here is what your attack surface is, why it keeps growing and the one habit that keeps it under control.

## WHAT IT IS

Attack surface management is the continuous practice of finding, monitoring and reducing every point where an attacker could reach your systems or data. That surface now spans internet-facing systems, cloud services, remote access, forgotten assets and connected suppliers. You cannot defend what you cannot see, so it starts with discovery from the outside in.

## WHY IT MATTERS

### 20 percent

Of breaches used vulnerability exploitation as the initial access route, up 34 percent on the year before.

Verizon 2025 DBIR

### Almost eightfold

Rise in edge and VPN exploitation, from 3 percent to 22 percent of tracked cases.

Verizon 2025 DBIR

### Every 7 days

How often CISA requires US federal civilian agencies to run automated asset discovery.

CISA BOD 23-01

## WHAT HAPPENED

In May 2023 the CIOp group mass-exploited a critical flaw in Progress MOVEit Transfer, a file-transfer app many organisations expose to the internet. It was patched within days, but CISA and the FBI reported more than 3,000 US organisations and over 8,000 worldwide were compromised, many through a single supplier running MOVEit. (CISA and FBI, 2023)

## RED FLAGS TO WATCH FOR

**A first external scan of your own perimeter often turns up exposure nobody remembered.**

- Forgotten subdomains that still resolve.
- Development and test systems reachable from the internet.
- Admin panels and login pages open to the public.
- Cloud storage left world-readable.
- Assets inherited through an acquisition or a supplier.

## THE ONE RULE THAT STOPS IT

**Keep one continuously updated inventory of every asset, mark which ones face the internet and reduce what does not need to be there.**

## THEN BUILD THE HABIT AROUND IT

- Discover from the outside in, the way an attacker maps you.

- Decommission dead systems and close unnecessary ports.
- Put multi-factor authentication on every remote and admin login.
- Patch internet-facing appliances and VPNs in days, not months.
- Track the suppliers connected to you and hold them to your standard.

## MYTHS AND FACTS

### MYTH

Attack surface management is just an asset inventory.

### FACT

An inventory is a static list. Attack surface management is continuous discovery, monitoring and reduction from the attacker's side, including assets no inventory recorded.

### MYTH

We are too small to be a target.

### FACT

Attackers scan the whole internet. The MOVEit and Ivanti campaigns hit any exposed instance they found, whatever the size of the organisation.

### MYTH

Supplier security is the supplier's problem.

### FACT

Third-party involvement in breaches doubled to 30 percent in 2025, and the Miljödata attack exposed 1.5 million people through a supplier.

## THE LEGAL DUTY

Knowing and managing your assets is now a legal expectation. NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, requires it under Article 21. DORA requires it under Article 8, and ISO 27001 opens Annex A 5.9 with an asset inventory. NIS2 Article 20 makes the board personally accountable.

## GET HELP

**eBuilder Security offers attack surface management, vulnerability management and penetration testing, delivered by a Sweden-based team. Read the full guide at the link below.**

[Read the Full Article →](#)