

Lateral Movement

Attackers rarely land where they want to end up. Lateral movement is how they travel from one hacked device to your crown jewels, and the controls here are what stop them.

WHAT IT IS

Lateral movement is how an attacker spreads from the first device they compromise to the rest of your network, stealing credentials and reusing legitimate tools to reach higher privileges and more valuable systems. It happens inside the network, after the perimeter is breached, which is why it turns a single infected laptop into a company-wide breach.

WHY IT MATTERS

48%

Of breaches involved ransomware in 2026, a record high. Ransomware reaches that scale by moving laterally first.

Verizon 2026 DBIR

39%

Of breaches involve credential abuse somewhere in the attack chain, the fuel for lateral movement.

Verizon 2026 DBIR

9 days

Attackers moved through Change Healthcare's network before deploying ransomware in 2024.

US Congressional testimony

WHAT HAPPENED

In February 2024 attackers logged in to a Change Healthcare remote-access portal using a stolen password on an account with no multi-factor authentication. They moved through the network for nine days before deploying ransomware, in a breach later reported to affect around 193 million people. The company paid about 22 million dollars. (US Congressional testimony, 2024)

RED FLAGS TO WATCH FOR

Lateral movement hides in legitimate activity, so watch the behaviour of accounts and logins across your network.

- A workstation suddenly authenticating to many other machines.
- An administrator account used at an odd hour or from an unusual location.
- A service account logging in interactively, like a person.
- New remote services or scheduled tasks appearing across several hosts.

THE ONE RULE THAT STOPS IT

Put multi-factor authentication on every internet-facing and privileged login, so one stolen password cannot open the rest of your network.

THEN BUILD THE HABIT AROUND IT

- Segment the network so a compromise in one zone cannot spread freely.

- Give every machine a unique local administrator password.
- Keep privileged accounts off ordinary workstations.
- Monitor for unusual internal logins, since perimeter tools miss movement inside the network.

MYTHS AND FACTS

MYTH

A strong perimeter keeps attackers out, so internal movement is not a concern.

FACT

Perimeter defences only guard the boundary. Lateral movement happens inside the network after a foothold, so internal monitoring and segmentation matter just as much.

MYTH

If one laptop is infected, only that laptop is at risk.

FACT

A foothold is where an attack starts, not where it ends. Attackers use that first device to steal credentials and reach others across the network.

MYTH

Our antivirus will catch an attacker moving between machines.

FACT

Lateral movement often uses legitimate tools and real credentials, so it leaves no malware for antivirus to flag and needs behavioural detection.

THE LEGAL DUTY

Limiting lateral movement is now a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs Sweden-based managed detection and response that watches for lateral movement inside your network, around the clock. Read the full guide at the link below.

[Read the Full Article →](#)