

An open network is an open invitation.

Every unpatched device, default password, and unsecured port is a door left ajar. **Network hardening closes the gap** before an attacker forces their way in.

31%

of breaches began with attackers exploiting vulnerabilities

43 days

median time to fully remediate exploited vulnerabilities

1

weak entry point can enable lateral movement without internal controls

Source: Verizon, 2026 Data Breach Investigations Report

● **Unhardened network exposures**

Cleartext management protocols still enabled

Telnet/23, HTTP/80, SNMPv1-v2c community strings

Unauthenticated access and Layer 2 spoofing

ARP spoofing, rogue DHCP

No segmentation between user, server, and OT/IoT zones

Compromised devices can reach unrelated systems.

Default or shared local admin credentials across hosts

pass-the-hash and credential reuse at scale

Unrestricted east-west traffic and permissive egress rules

no deny-by-default

● **What hardening actually does**

Secures and restricts management access

SSHv2 + key auth, HTTPS/TLS 1.2+, SNMPv3 only; disable unused services

Applies port-based access control at the edge

802.1X, DHCP snooping, dynamic ARP inspection

Segments by function and trust level

VLANs + stateful ACLs, microsegmentation for critical assets

Moves to least-privilege, unique credentials

LAPS/PAM, MFA on all remote and privileged access

Sets default-deny at every boundary

explicit allow rules in, allow rules out, log the rest

● **Baseline hardening controls**

ACCESS

Disable Telnet, FTP, HTTP admin panels. SSHv2 and HTTPS only, keys over passwords

SEGMENT

Separate users, servers, guests, and OT/IoT; permit only required traffic between zones

CRYPTO

TLS 1.2+ only. Disable SSLv3, TLS 1.0/1.1, and weak cipher suites on every listener

L2

Enable DHCP snooping, dynamic ARP inspection, and BPDU guard; disable CDP/LLDP on user-facing ports

AUTH

802.1X on endpoint access ports, with controlled exceptions; MFA for remote and privileged access

MGMT

Restrict access to management networks and jump hosts; limit access by source IP

MONITOR

Centralize syslog and NetFlow/IPFIX to a SIEM; alert on new device joins and privilege escalation

PATCH

Firmware and OS patches on a fixed cadence; track CVEs for edge and perimeter devices specifically

Guided by CIS Controls and NIST security guidance