UNMANAGED DEVICES

The Device You Don't Know About Is Already on Your Network

Personal laptops, home computers, contractor devices, and forgotten endpoints are accessing your organization's data right now — outside every security control you have deployed. They do not appear in your device inventory. They do not trigger alerts. They are simply there.

32.5%	46%	80–90%	1 in 4
of devices on corporate networks operate entirely outside IT control	of compromised systems holding corporate credentials are unmanaged devices	of successful ransomware attacks originate from unmanaged endpoints	SMBs experienced a cyberattack or data breach in the past 12 months

Sources: Palo Alto Networks Device Security Threat Report (2025) · Verizon DBIR (2025) · Market.us Endpoint Security Report (2025) · Proton SMB Cybersecurity Report (2026)

WHY UNMANAGED DEVICES EXIST

Unmanaged devices are not the result of reckless behavior. They are the result of normal work. A partner works from home on a personal laptop. A contractor connects to SharePoint from their own machine. An employee whose corporate device is being repaired uses a family computer for a week. Each of these scenarios introduces a device that has never been enrolled, never been assessed for compliance, and never been subject to any of the controls the organization believes are in place.

The problem compounds over time. Devices that connected once tend to connect again. Credentials cached on a personal machine do not expire when the business situation that created them does. A device that accessed client data six months ago during a period of convenience may still have active session tokens today — and no one in the organization knows it exists.

WHAT ORGANIZATIONS CANNOT SEE

Microsoft Intune and Entra ID report on devices they know about. An unmanaged device does not appear in Intune because it was never enrolled. It does not trigger a Conditional Access alert because, depending on policy configuration, it may authenticate successfully using valid credentials — a username and password that belong to a real employee, on a device the organization has never seen.

This is the visibility gap. The organization's security dashboard shows a clean posture because the dashboard only reports on what is enrolled. The unmanaged device is on the network, accessing SharePoint, Exchange, and Teams. It has never had EDR installed. It has never been patched to standard. It may be running software the organization has explicitly prohibited.

WHAT A GOVERNED ENVIRONMENT REQUIRES

Control	Requirement	What It Addresses
Enrollment required	Every device accessing governed resources enrolled in Intune before access is granted	No unmanaged device can reach any governed resource under any circumstance
Compliance gate enforced	Conditional Access blocks non-compliant devices automatically — no manual intervention required	Enrollment alone is not sufficient — the device must meet the compliance standard
No personal devices	Personal device access to governed resources is prohibited without exception	Personal devices cannot access email, SharePoint, Teams, or any governed workload
Hardware standard enforced	Devices must meet capability specification — TPM 2.0, Secure Boot, BitLocker active	Devices below specification cannot be enrolled and therefore cannot access governed resources

These controls work together as a single gate. A device must be enrolled, compliant, and meet the hardware specification before it can access any governed resource. There is no path around this gate — no exception for a partner's personal machine, a contractor's laptop, or a device that was intended to be temporary. The gate is binary. The device either meets the standard or it does not connect.

THE INSURANCE CONSEQUENCE

Cyber insurance carriers now require documented evidence of device management — not attestation, evidence. Enrollment reports, compliance state logs, and Conditional Access policy configuration are becoming standard components of the renewal package. An organization that cannot demonstrate 100% managed device coverage is presenting an unquantifiable attack surface to an underwriter who is trying to price a policy around it.

The underwriter's position is straightforward: if you do not know what is on your network, neither do we. Organizations that operate inside a governed environment do not reconstruct this evidence at renewal. It exists as a continuous, verified record — produced automatically, every month, from the same telemetry that enforces the standard.

This brief is part of AnchorOne's Spring 2026 governance series.

— Dan Cull, Founder, AnchorOne