NEXT PERIMETER

# Zero Fuss Access Control Checklist – 2025 Edition

Everything a modern business needs for secure, frictionless access

## 👤 IDENTITIES

☐ MFA enforced on all user accounts

☐ Legacy authentication blocked (e.g., POP, IMAP, SMTP)

☐ Role-based access templates applied on user creation

☐ Admin roles isolated with step-up authentication

☐ Sign-in risk monitoring enabled (impossible travel, brute force, etc.)

## 🌐 NETWORKS

☐ Geo-IP blocking in place (e.g., block logins from outside the US)

☐ Public Wi-Fi and unknown networks treated as high risk

☐ Legacy VPNs replaced with zero trust network agent

☐ Network-level threat detection (DNS filtering, anomaly alerts)

☐ All network traffic logged and retained

## 💻 DEVICES

☐ Company-owned laptops meet security baselines (patching, encryption, MDM)

☐ All endpoints run EDR + posture monitoring

☐ Windows Hello (fingerprint/IR camera) supported and required

☐ BYOD access limited to app-only (no sync/downloads)

☐ Jailbroken/rooted device access blocked

## 🛡️ POSTURE

☐ Real-time posture checks (encryption, patch level, firewall status)

☐ Risk-based session control enabled

☐ Suspicious behavior triggers playbooks (token revocation, disable user)

☐ Admin alerts on non-compliant device access attempts

☐ Integration with SIEM and automated response (SOAR)

## 📱 APPLICATIONS

☐ All apps gated with conditional access (identity + device + location)

☐ SaaS discovery in place to detect shadow IT

☐ High-risk apps (finance, admin, HR) require trusted device

☐ SSO (Single Sign-On) enforced for app access

☐ Application session lifetime policies defined

## Need help assessing your environment?

→ Book your free Access Control Readiness Assessment

→ https://nextperimeter.com/it-blog/