Plow

Zero Trust

Maturity Self-Assessment

Plow Networks

Prepared 2026

7101 Sharondale Court
Suite 200
Brentwood, TN 37027
plow.net

This document contains proprietary and confidential information prepared for you by Plow Networks.
This document should not be reproduced without the consent of Plow Networks.

Most organizations have read the Zero Trust explainers and still don't know where they stand. This self-assessment helps you place your environment on a maturity scale across six capability areas, identify the honest gap between the tools you've bought and the posture you actually operate, and prioritize the next investment. Start with identity — every other capability depends on it.

How to use this: for each capability area, check every statement that is fully true today. Then map your count to the maturity scale at the end. Be honest — most mid-sized organizations land lower than the tools they own would suggest.

The Maturity Model

Level	Identity Characteristics	Typical Gaps
Initial	Multiple directories, password-only auth, ad-hoc accounts	No MFA, shared accounts, no lifecycle
Developing	Single primary IdP, MFA on most users, basic conditional access	Service accounts unmanaged, standing privilege
Defined	Consolidated IdP, MFA enforced universally, conditional access in production	Limited risk signals, manual privilege reviews
Managed	Risk-based access, just-in-time privilege, automated lifecycle	Behavioral analytics not yet integrated
Optimized	Continuous verification, behavioral analytics, automated response	Ongoing tuning rather than capability gaps

Capability 1 — Identity (Start Here)

Identity is the primary control plane. If it's weak, everything downstream is weak. This is where most early risk reduction lives:

☐ Authentication is consolidated to a single authoritative identity provider

☐ MFA is enforced universally, including for service principals and break-glass accounts

☐ Standing privileged access is eliminated (admin roles activate just-in-time)

☐ Conditional access uses real signals: device compliance, location, sign-in risk, app sensitivity

☐ A joiner/mover/leaver lifecycle process exists and is automated where possible

Capability 2 — Device Trust

☐ Device compliance policies exist in your MDM/UEM

☐ Conditional access gates resource access on device health and compliance state

☐ A defined response exists for when a device falls out of compliance

☐ Personal/unmanaged devices have a separate, restricted access path

©2026 Plow Networks / Proprietary & Confidential. | plow.net

Capability 3 — Application Access

☐ SaaS applications authenticate via the IdP with conditional access applied

☐ On-prem apps sit behind an identity-aware proxy or modern access broker

☐ VPN-by-default access has been replaced with per-application access (VPN is the exception)

☐ Legacy apps that can't support modern auth are documented with a treatment plan

Capability 4 — Network Segmentation

☐ The most sensitive systems are isolated from the general network (macrosegmentation)

☐ Segmentation policy can reference accurate identity context

☐ Traffic between segments is controlled and monitored

☐ Segmentation is enforced, not just mapped

Capability 5 — Data Protection

☐ Data is classified (the most sensitive data gets the most stringent access)

☐ Classification is enforced consistently across platforms

☐ DLP and retention policies are applied based on classification, not uniformly

☐ Access to regulated data is logged and reviewed

Capability 6 — Monitoring & Response

☐ Identity-based threat detection is in place

☐ Anomaly detection produces actionable (not noisy) signals

☐ Automated response playbooks exist for common identity incidents

☐ Privileged actions generate an audit trail that is reviewed

Your Maturity Snapshot

Record your checked count per capability. Identity is weighted first because the others depend on it — a low identity score caps your real maturity regardless of the other areas.

Capability Area	Items True	Next-Investment Priority
Identity (of 5)	_____ / 5	☐ High ☐ Med ☐ Low
Device Trust (of 4)	_____ / 4	☐ High ☐ Med ☐ Low
Application Access (of 4)	_____ / 4	☐ High ☐ Med ☐ Low
Network Segmentation (of 4)	_____ / 4	☐ High ☐ Med ☐ Low
Data Protection (of 4)	_____ / 4	☐ High ☐ Med ☐ Low
Monitoring & Response (of 4)	_____ / 4	☐ High ☐ Med ☐ Low

©2026 Plow Networks / Proprietary & Confidential. | plow.net

Reading Your Result

Identity below 4/5: start here regardless of what the other areas show. Identity is the foundation; investing elsewhere first produces fragile, expensive systems.

Identity solid, other areas low: you're ready to sequence the next capabilities — device trust, then application access, then segmentation, then data and monitoring. In that order.

Most areas strong: shift from capability-building to ongoing operations — policy tuning, access certification, and privileged-access review. Zero Trust decays without maintenance.

Building Your Zero Trust Roadmap?

Plow Networks helps IT leaders design Zero Trust programs that produce measurable risk reduction — starting with identity, sequenced to fit your business, and built to last.

Talk to Our Security Team →

©2026 Plow Networks / Proprietary & Confidential. | plow.net