Astro

Practical, Low-Cost Ways to Operationalize Zero Trust Using What You Already Own

This paper provides practical, prioritized actions organizations can take today to operationalize Zero Trust concepts using existing infrastructure, starting with identity, access, and continuous trust.

February, 2026

www.astrodefend.com
info@astrodefend.com

Practical, Low-Cost Ways to Operationalize Zero Trust Using What You Already Own

Zero Trust is often presented as a sweeping transformation: new vendors, new architectures, and major operational disruption. For many organizations, that narrative has created fatigue, stalled initiatives, and underutilized tools.

The reality is simpler.

Zero Trust is not a product. It is a set of principles that can be applied incrementally, often using controls and platforms organizations already have in place. When implemented pragmatically, these principles materially reduce risk without requiring wholesale change.

The goal is **not perfection**.
The goal is **progress**.

Where to Start: High-Impact, Low-Friction Zero Trust Controls

Below is a prioritized checklist of Zero Trust-aligned actions that most organizations can implement using existing platforms such as identity providers, endpoint management tools, and cloud-native security features.

These are ordered roughly from lowest effort / highest immediate impact to more advanced but still achievable.

Zero Trust Operationalization Checklist

Foundational Access Control

☐ Enforce MFA for all users, including administrators
☐ Require stronger controls for privileged roles (stronger authentication, session limits)
☐ Block legacy authentication protocols where possible
☐ Implement Continuous Access Evaluation (CAE)
☐ Implement Token Protection where possible
☐ Review and reduce standing administrative privileges (Implement PIM)

Why it matters:
Most attacks don't break in. They log in. Identity remains the single most common initial access vector.

Risk-Based Conditional Access Policies

☐ Enable risk-based authentication and access decision
☐ Implement token revocation or re-evaluation when risk changes
☐ Require MFA for Medium & High-Risk Sign-Ins
☐ Block Access for High-Risk Users and force a password reset
☐ Monitor for anomalous sign-ins and impossible travel scenarios

Why it matters:
Trust should not be permanent. Access decisions made at login should be revisited continuously.

Zero Trust Operationalization Checklist (Continued)

Device & Endpoint Context

□ Apply different access policies based on device trust level
□ Require device compliance for access to sensitive resources
□ Block access from unmanaged or non-compliant endpoints
□ Enforce basic endpoint security baselines through posturing

Why it matters:
A trusted identity on an untrusted device is still a risk.

Application & SaaS Access

□ Configure SSO for all SaaS/Application access
□ Apply least-privilege access to SaaS application integrations
□ Regularly review application permissions and OAuth grants
□ Remove unused or over-privileged app integrations
□ Monitor sign-in behavior across cloud and SaaS platforms

Why it matters:
Cloud sprawl quietly expands the trust boundary far beyond the network.

Non-Human & Machine Identities

□ Inventory service accounts, API keys, and automation identities
□ Identify long-lived or static credentials
□ Reduce excessive or inherited permissions
□ Rotate credentials and limit scope where possible
□ Monitor autonomous activity for abnormal behavior

Why it matters:
Machine identities often operate with broad access and little oversight. When compromised, they enable silent lateral movement using legitimate permissions.

What This Looks Like In Practice

Organizations that succeed with Zero Trust do not attempt to “finish” it.
Instead, they:

- Focus on reducing implicit trust
- Add context where none existed before
- Replace standing access with just-in-time decisions
- Improve visibility into identities beyond human users

These improvements compound over time, improving security posture without paralyzing the organization.

Common Pitfalls to Avoid

- Treating Zero Trust as a single project instead of an operating model
- Buying new tools before fully using existing ones
- Ignoring non-human identities and automation
- Chasing architectural perfection instead of measurable risk reduction

How to Accelerate Without Overspending

Most organizations already own powerful Zero Trust-enabling capabilities but lack:

- Clear prioritization
- Cross-team alignment
- Practical implementation guidance

This is where focused, advisory-led engagement makes the difference

Ready to move beyond Zero Trust theory?

We help organizations:

- Evaluate their current Zero Trust maturity
- Identify high-impact improvements using existing tools
- Prioritize actions that reduce real-world risk
- Avoid unnecessary technology spend

Contact us for a complimentary consultation to assess your current state and identify where we can help accelerate your Zero Trust journey, without significant new investments.