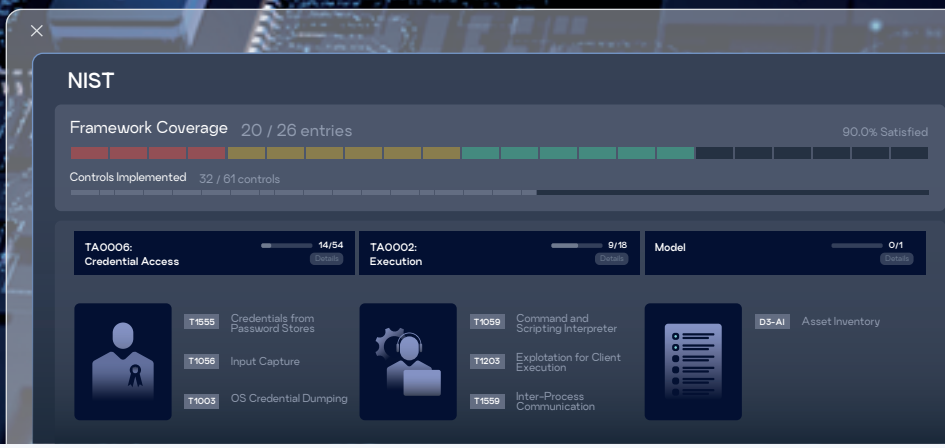
Operationalizing Zero Trust with Reach and NIST SP 1800-35

Companion Guide

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



Introduction

NIST Special Publication 1800-35 offers one of the most detailed and actionable roadmaps for implementing Zero Trust in complex, real-world environments. Developed through collaboration with industry partners, it distills Zero Trust into seven practical steps that security leaders can follow to reduce risk and modernize their architecture.

This datasheet shows how Reach helps organizations execute each of these seven steps more efficiently and effectively by leveraging exposure data, automation, and deep integration with the tools teams already use. The result: a faster path to Zero Trust maturity without the operational drag.

Reach helps organizations advance their Zero Trust posture by delivering visibility, prioritization, and automation, all grounded in real-world exposure data. Key capabilities include:

Automated assessment of your current maturity posture against standards. Connect and assess using existing security tools and historical data.

Clear prioritization of initiatives that will drive maturity, not just compliance. Recommendations are prioritized based on impact of change on users, exposure reduction, and availability of capabilities.

Visibility, analytics, and automation with policy recommendat ons. Recommended policies are tailored and offered as configurations and change tickets.

Continuous reporting on maturity against industry standards. Measure progress of maturity over time as improvements are made.

NIST Step	What It Means	How Reach Helps
1. Discover and Inventory the Existing Environment	Build a complete picture of users, devices, applications, and flows	Reach seamlessly connects to the tools in your environment to provide a comprehensive Asset Intelligence view which maps the devices, users, and identities seen in the daily workflow. Connecting to IAM, EDR and network tools ensures maximum visibility into "what's hiding in the shadows".

NIST Step	What It Means	How Reach Helps
2. Formulate Access Policy to Support the Mission	Design least-privilege access rules that align with how people work	Reach identifies the highest risk and most attacked users, enabling the creation of contextual, dynamic access policies based on how work is actually done.
3. Identify Existing Security Capabilities and Technology	Understand what tools and features are already in place	Reach automatically maps existing capabilities and configurations from your deployed tools, showing what's available, what's used, and where gaps or overlap exists.
4. Implement ZTA Components	Roll out changes across identity, device, network, and data systems	Reach generates detailed deployment guides, change tickets, and automation workflows to put Zero Trust controls in place efficiently and accurately.
5. Verify the Implementation	Confirm that policies are working and correctly enforced	Reach continuously monitors for configuration drift and validates control effectiveness across integrated tools, ensuring Zero Trust protections remain intact.
6. Continuously Improve and Evolve	Reassess and refine controls as environments and threats change	It's not enough to simply implement policies, Reach helps ensure policies remain in place performing their intended function effectively.

Real-World Example: How One Company Accelerated Zero Trust with Reach

A global insurance software provider had recently invested in a ZTNA solution but lacked the in-house expertise to implement it efficiently. With Reach, they connected their tools via API, ran exposure analysis through MasterMindAI™, and had results in three days. Within three weeks, the PoV was complete.

> **"They needed to shorten deployment time from 12–18 months to 1–2 months using Reach"**

Reach not only accelerated their roadmap but enabled ongoing governance of compliance and GenAI usage without requiring additional tools.

> **"Using Reach allows security teams to make threat-informed decisions, prioritize controls across their tools, and remediate organizational risk automatically"**

Conclusion: Exposure-Driven Maturity is the Fastest Path to Zero Trust

The seven steps outlined by NIST provide a comprehensive foundation for Zero Trust implementation. But moving from guidance to execution requires more than alignment, it requires action.

Reach bridges that gap. By operationalizing each step through automation, integration, and exposure-based prioritization, organizations can modernize their architecture, reduce risk faster, and build a Zero Trust strategy that holds up over time.

Getting Started with Reach

To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit:

Reach.Security/try-reach