AHEAD

Developing a Zero Trust Maturity Roadmap

Introduction

For enterprise leaders, security is a frequent, ongoing concern that cannot be overlooked. And despite its critical role in determining the success or failure of an organization, many security 'grey areas' remain. This is, in part, because the security industry as a whole has been disproportionately focused on products.

At AHEAD, we believe that security is a process – not a product. There is no end state to zero trust maturity – the goal of any zero trust program is to constantly get better. It is about developing the right processes to reach the desired security posture and only then incorporating the tools and technologies to enable it. This is particularly important when it comes to implementing zero trust throughout the enterprise, where buzzword stigma and opportunistic product naming conventions have muddied the waters for organizations looking for real zero trust architecture (ZTA) solutions.

In this eBook, we'll outline our holistic approach to zero trust by examining our maturity roadmap, the process of standing up a zero trust security program, and the architectural strategy required to enable it.

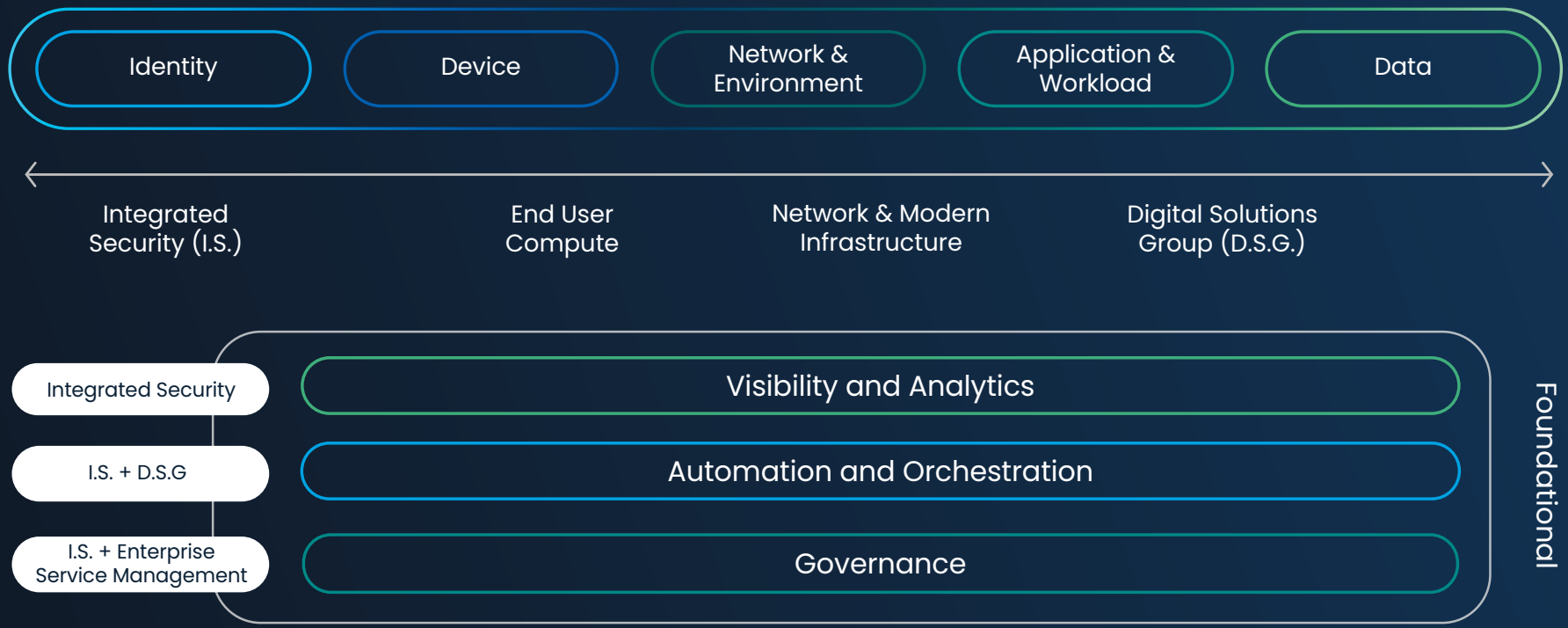
Our Holistic Approach

Rather than contribute to the confusion around zero trust by establishing our own definition, AHEAD aligns to the CISA industry standards laid out by the U.S. Government, which breaks down into five pillars: Identity, Devices, Network & Environment, Application & Workload, and Data. In addition to these pillars, it is vital to include Visibility & Analytics, Automation & Orchestration, and Governance as foundational elements for a successful zero trust program.

How AHEAD excels—and how pure-play security firms fall short—is through our practice areas, which aligns 1-to-1 with the five zero trust pillars and foundational components required to successfully implement a true zero trust program. This allows us to eliminate silos in your organization and enable the cross-pillar connectivity and visibility needed for a holistic application of zero trust. To help you reach maturity faster, we identify the most impactful use cases and pillars to prioritize in your tech stack and model the five pillars against your key assets and applications.

Traditional security vendors simply cannot meet this level of detail because they rarely (if ever) have all of the relevant teams to do so.

Pillars of Zero Trust & AHEAD Practice Areas



Zero Trust Maturity

When it comes to zero trust, there are generally four fundamental maturity levels: Traditional, Initial, Advanced, and Optimal. However, it is important to note that reaching the level of 'Optimal' across all facets of a security posture is not what organizations should universally aspire towards. Rather, it is important to assess the cost and time commitments that make sense for each individual organization and aim for the maturity level that is the best fit. At AHEAD, we work with organizations to identify both the current state and appropriate desired state of their zero trust pillars, and help them plot the right course of action.

TRADITIONAL

Manual configurations, **proprietary pillars** of enforcement

ADVANCED

Some cross-pillar coordination, **centralized identity control,** policy based on cross-pillar inputs and outputs

OPTIMAL

Fully automated / dynamic policies agreement with **open standards for cross-pillar interoperability**

	TRADTIONAL	ADVANCED	OPTIMAL
Identity	• Password or MFA • Limited risk assessment	• MFA • Some identify federation with cloud and on premises systems	• Continuous validation • Real time machine learning analysis
Device	• Limited visibility into compliance • Simple inventory	• Compliance enforcement employed • Data access depends on device posture	• Consistent device security monitoring and validation • Data access depends on real-time risk analytics
Network & Environment	• Large macro-segmentation • Minimal internal or external traffic encryption	• Defined by ingress/egress micro-perimeters • Basic analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted
Application & Workload	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Access based on centralized authentication • Basic integration into application workflow	• Access is authorized continuously • Strong integration into application workflow
Data	• Not well inventoried • Static Control • Unencrypted	• Least privilege controls • Data stored in cloud environments are encrypted at rest	• Dynamic support • All data is encrypted

Achieving Zero Trust with a Phased Approach

When developing an approach for zero trust architecture implementation, the right mindset is to think of it like an application migration—from legacy to a new architecture. By adopting a three-phased approach that spans strategy, remediation, and migration, organizations can be sure they are creating a pristine environment for applying zero trust.

PHASE 1

Zero Trust Architecture Strategy and Roadmap

- Review of Business Objectives and Existing IT / Security Projects
- Analysis of Existing Policy, Process Documentation
- Working Sessions for Each Dimension of the CISA Model
- Tools Rationalization Based on Desired State
- Architecture Design Enhancement Proposals
- Identify Initial Applications for Migration

PHASE 2

Remediation and Build

Frequent Issues AHEAD Sees in Remediation Phase:

- Identity governance
  - User Models
  - Provisioning
  - De-Provisioning
  - Privileged Access Management
- Network Trust Zones Architecture
  - Shared Services Infrastructure Design
- CMDB Clean Up
  - Asset Classification

PHASE 3

Zero Trust Application Migration

Common Activities in the ZTA Application Migration Phase:

- Application Dependency Mappings
  - Port and Protocol Analysis
- Connected Systems Management
  - Interfacing with Shared Services Network
- Building Application Delivery Plans
  - Application Presentation Layer
- Migration Planning
- Cut Over Windows

Architecture Strategy & Roadmap

As stated above, the first step in any zero trust journey is to define the strategy and roadmap. This is a multi-week process that sets the table for Phase Two (Remediation & Build) by defining desired outcomes, analyzing existing policies, and generating a findings report.

Even if your organization already has a fully-defined ZTA roadmap, AHEAD teams can work cross-functionally to deliver any planned projects to boost your maturity level within any zero trust pillar.

Total timeline: 9 - 15 weeks, largely dependent on customer resource availability, customer time commitment expected 8 - 12 hours per week

1 WEEK

Review of Business Objectives & Existing IT / Security Projects

Identify efficiencies with existing projects such as network refresh, PAM roll out, IGA initiative, cloud migration, etc.

2 WEEKS

Analysis of Existing Policy, Process Documentation

AHEAD will make a "documentation request" for critical security program information

4 - 6 WEEKS

Working Sessions for Each Dimension of the CISA Model

Identity, Device, Network & Environment, Application & Workload, Data

1 - 2 WEEKS

Analysis & Deliverable Creation Based on Derived Understanding

AHEAD compiles findings into a Strategy and Roadmap document with current state findings

1 - 2 WEEKS

Customer Review of Deliverable to Ensure Findings Accuracy & Completeness

Customer is provided the initial findings document for review. After review is completed and any updates are made AHEAD moves to the final phase

1 - 2 WEEKS

Final Strategy & Roadmap, Executive Summary Readout, & Backlog Delivered

AHEAD updates findings report, generates actionable backlog, creates and presents the executive summary

For more guidance on starting the zero trust journey for your enterprise, get in touch with us today.

AHEAD

About AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

National Hubs

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

CHICAGO
401 Michigan Ave.
#3400
Chicago, IL 60611

SAN FRANCISCO
2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583