Solution Brief

AHEAD

Zero Trust

Seven Actions Used in Over 99% of Data Breaches

01 Use of email phishing attacks

02 Exploiting a vulnerable application or device

03 Installation of command and control

04 Capturing credentials (stealing passwords)

05 Lateral movement in the environment

06 Access and authentication to data

07 Resulting in data exfiltration or ransomware

Business Imperative Technology Outcome

Assess & Develop Strategy
Prioritize on the top Tactics, Techniques, & Procedures (TTPs)

Design Mitigation Architecture
Built on a Zero Trust philosophy

Plan for Data Recoverability
Cyber Recovery based on a when — not if — scenario

Zero Trust Architecture

Verify Every User & Device

- Require secure and authenticated access to all resources
- Trust no one, both inside and outside the network

Adopt Least Privileges

- Enforce access controls and segmentation
- Give only the required privileges to complete necessary work

Intelligently Limit Access

- Inspect and log all activities
- Use Visibility, Analytics, & Automation to keep policies in check

Identity and Access Management Within Zero Trust Architecture

FIVE PRIMARY OBJECTIVES:

Business Objectives & Program review, including relevant compliance standards.

Identity Assets and Applications in scope

Identify users in scope

Develop processes for Authorization, Authentication, and Attestation

Propose and Implement Matching Solutions

Maturity Level	01	02	03	04
Phishing	• Education & Awareness	• Anti-Phishing Solution	• Phish Testing	• Phish Testing w/Automated Training
Vulnerability	• Web Application Firewall • Vulnerability Scanning	• Application Testing Web Access Filtering • Patching	• Breach Testing • Vulnerability Management	• Continuous Breach Testing • Vulnerability Management w/ Automated/Prioritized Remediation
Endpoint Protection	• Anti-Malware	• Managed Anti-Malware	• EDR Solution	• Managed EDR Solution
Credential Theft & Escalation (IAM)	• Multi-factor Authentication (MFA)	• Adaptive MFA	• Adaptive MFA w/Single Sign On (SSO)	• Endpoint Privilege Management
Lateral Movement (Zero Trust)	• Local Admin Password Solution (LAPS) • Blacklist Model-Prod/Dev/ Test Separation	• Privileged Account Management (PAM) • Compliance Based Segmentation	• Privileged Account Management (PAM) w/ Workflow Management • Hybrid Black/Whitelist Critical App Segmentation	• Identify Governance Program w/Automation • Full Whitelist Model Full App Segmentation
Data Encryption			• Anti-Encryption w/Alerting	• Anti-Encryption w/Analytics and Automation
Data Loss	• Immutable Backups w/MFA	• Single Channel DLP • Multi-factor Delete Confirmation	• Multi-Channel DLP • Analytics w/Anomaly Detection	• Multi-Channel DLP w Monitoring & Kill Switches • Air-Gapped Backup w/ Analytics

Outcomes

AHEAD's integrated security professionals are ready to help you not only evaluate when and where your most sensitive company assets may be vulnerable, but quickly safeguard those assets. Besides being one of the most popular buzzwords in IT today, Zero Trust is a valuable security protocol that is helping enterprises better protect themselves from outside threats. Reach out to our security experts to find out how adopting a Zero Trust model could improve your organization's security posture.

AHEAD

Accelerate Your Impact

Learn more at www.ahead.com