5 Ways to Fortify AD/AAD Security

Your Presenter:
Dan Conrad CISSP, CEH, MCITP
daniel.conrad@oneidentity.com
conraddan
Agenda

• Visibility, Awareness, Insight
• Zero Trust
• Efficiency = Strong Security
• Integrations and Limitations
• M&A/Design and Implementation “Opportunities”
1 - Visibility, Awareness, Insight

Basic concepts:
- What do you have?
- Why do we have it?
- Who has access?
- Why is it this way?

Discover what you have and protect:
- What were the goals when it was designed?
- Are there organizational policies?
- How does it look now compared to original design?
Zero Trust was created by John Kindervag, during his tenure as a vice president and principal analyst for Forrester Research, based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted.
2- Origin of “Zero Trust”

John Kindervag – Forrester – 2010

Zero Trust was created by John Kindervag, during his tenure as a vice president and principal analyst for Forrester Research, based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted.

What does this sound like?
2- Zero Trust is a Concept

- Compare to “Least Privilege”
- A mentality
- Terms
  - Zero Trust Architecture (ZTA)
  - Zero Standing Privilege
  - Just-In-Time Access

2- NIST – The seven tenets of Zero Trust

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Reference: NIST SP 800-207 “Zero Trust Architecture”
1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. **Access to individual enterprise resources is granted on a per-session basis.**
4. **Access to resources is determined by dynamic policy**—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Reference: NIST SP 800-207 “Zero Trust Architecture”
2 - Apply ZTA to AD

- PAM for AD – Access Control
- Establish policy to limit direct admin access to AD
- Capture AD security completely
- Vulnerable Service Accounts: Use PAM and GMSAs where possible - business process/policy
3 - AD Efficiency = Stronger Security

- Decide and drive by organizational policy
- Automate where possible to reduce deviations from established policies
- Automated access controls
- Reduce admin touch points, opportunity to introduce problems
- Efficiencies ensure policies are implemented globally = reducing errors that can leave vulnerable access
4 - Integrate and Automate...to some degree

- Just-In-Time Access
  - Azure AD
  - On-Prem AD
- Validate Access Control - AD groups
- Unix vulnerabilities in AD?
- Technical implementation of written policies - SOAR

Compartmentalize...
Admin and user access – assimilate – buy in - communicate

Reduce vulnerability window. Roll in new organizations in "current state" and manage them securely

Consider AD/AAD in the M&A process to ensure no vulnerabilities are introduced. – require ZT as a practice

Never miss a greenfield opportunity
Security Starts with Identity

Identity Governance and Administration
Unify governance, provisioning, administration, & policies for any system, platform, or applications

Privileged Access Management
Secure, audit, and analyze privileged access

AD Account Lifecycle Management
Manage, administer, & secure hybrid AD. Extend to Unix/Linux and many popular SaaS apps

Identity SaaS
Cloud-delivered identity services to enhance and expand existing IAM solutions
Wrap Up Concepts

• Consumers, users, admins, CISOs all expect stronger security – let’s deliver

• Layer controls to protect us from ourselves (and our users)
  • Wear a raincoat, carry the umbrella, get under the roof, and watch the weather
  • The user layer: Expect (and appreciate) strong security and are recognizing when it’s missing