Zero Trust: Identity’s Critical Role

Session Abstract

• Come join Oregon State University’s Identity and Access Management team, part of the Office of Information Security, to learn how we are implementing Zero Trust through our “Smart Access” program. The Smart Access program enables a foundational capability to provide and secure appropriate access to data and systems.

• As part of our Smart Access program, Oregon State University completed an RFP, purchased a commercial IGA (Identity Governance and Access) system, and hired an implementation partner. We are early in our Zero Trust journey and will approach the next phase of this project during the time of this conference.

• Attendees will come away with an understanding of Zero Trust goals for a large R1 university and our approach to implementing Zero Trust principles.
Zero Trust: Identity's Critical Role

Andy Morgan
Jason Peak
Why should Higher Ed care about Zero Trust?

Our networks are not as simple as they were 20+ years ago:

• BYOD
• Access to cloud apps
• Remote access to networks
• Multiple campuses

How do we re-establish trust and security where all these things are true?
What is Zero Trust?
NIST SP 800-207

• Builds up trust by considering the entire context of the session being established
• Moves defenses from static, network-based perimeters to focus on users, assets, and resources
• Assumes no implicit trust based solely on network location or device ownership
• Focuses on protecting resources, not network segments
CISA's Zero Trust Maturity Model

- Re-packaging of NIST 800-207
- A guide to climb the mountain
- A checklist of likely steps to take
- Each organization will decide what maturity level is appropriate for them
Zero Trust Maturity Model Pillars

<table>
<thead>
<tr>
<th>Identity</th>
<th>set of attributes that uniquely describes a user or entity, including non-person entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>any asset (including its hardware, software, firmware, etc.) that can connect to a network</td>
</tr>
<tr>
<td>Networks</td>
<td>internal networks, wireless networks, and the Internet</td>
</tr>
<tr>
<td>Applications &amp; Workloads</td>
<td>systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments</td>
</tr>
<tr>
<td>Data</td>
<td>all files and fragments</td>
</tr>
</tbody>
</table>
Cross-Cutting Capabilities

Visibility and Analytics

Automation and Orchestration

Governance
# Maturity Levels

<table>
<thead>
<tr>
<th>Traditional</th>
<th>Optimal</th>
<th>Advanced</th>
<th>Initial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually configured</td>
<td>Fully automated</td>
<td>Where applicable, automated controls for lifecycles</td>
<td>Starting automation</td>
</tr>
</tbody>
</table>

### Traditional
- Passwords or MFA
- On-premises identity stores
- Limited identity visibility
- Permanent access with periodic review
- Manually tracking device inventory
- Limit compliance visibility
- No flexible criteria for resource access
- Manual deployment of threat protections to some devices
- Manually inventory and categorize data
- On-prem data stores
- Static access controls
- Minimal encryption of data at rest and in transit with ad hoc key management

### Optimal
- Continuous data inventorying
- Automated data categorization and labeling enterprise-wide
- Optimized data availability
- DLP anti-blocking
- Dynamic access controls
- Encrypts data in use

### Advanced
- Phishing-resistant MFA
- Consolidation and secure integration of identity stores
- Automated identity risk assessments
- Need/session-based access
- Most physical and virtual assets are tracked
- Enforced compliance implementation with integrated threat protections
- Initial resource access depends on device posture
- Expanded isolation and resilience mechanisms
- Configurations adapt based on automated risk assessment application profile assessments
- Encrypts applicable network traffic and manages issuance and rotation of keys
- Initial isolation of critical workloads
- Network capabilities manage availability and compliance demands for more applications
- Dynamic configurations for some portions of the network
- Encrypts more traffic and formalizes key management policies
- Some mission critical workloads have integrated protections and are accessible over public networks to authorized users
- Formal code deployment mechanisms through DevOps pipelines
- Static and dynamic security testing prior to deployment
- Limited automation to inventory data and control access
- Rights to implement a strategy for data categorization
- Some highly available data stores
- Encrypts data in transit
- Initial centralized key management policies

### Initial
- MFA with passwords
- Self-managed and hosted identity stores
- Manual identity risk assessments
- Access expires with automated review
- All physical assets tracked
- Limited device-based access control and compliance enforcement
- Some protections delivered via automation
- Initial isolation of critical workloads
- Network capabilities manage availability and compliance demands for more applications
- Dynamic configurations for some portions of the network
- Encrypts more traffic and formalizes key management policies
- Some mission critical workloads have integrated protections and are accessible over public networks to authorized users
- Formal code deployment mechanisms through DevOps pipelines
- Static and dynamic security testing prior to deployment
- Limited automation to inventory data and control access
- Rights to implement a strategy for data categorization
- Some highly available data stores
- Encrypts data in transit
- Initial centralized key management policies

### Governance
- Visibility and Analytics
- Automation and Orchestration
- Governance

Graphic: CISA ZTMM
Identity’s Critical Role

• Identity is the most important pillar because the other pillars don’t work if you don’t know WHO

• As the perimeter goes away, you can’t just rely on network location for trust. You must know WHO.
Zero Trust @ OSU
Carrot or Stick?
A very short dramatization...

[Professor] Zero Trust? wait, you don't trust *me*?
[Registrar] Not even a *little* bit?
[Campus IT] Sorry no, not one bit!
[Everybody] Ahh, *Smart Access*, now that sounds nice, I'm in!
Where we're coming from

...Corvallis, Oregon

Students 35,000
Employees 8,700
Accounts 100,000
Identities 500,000
IAM Staff 3
IAM Manager 1

Photo: OSU stock, Frank Miller
Identity Pillar Maturity Levels

**Traditional**
- Passwords or MFA
- On-prem identity stores
- Limited identity risk assessments
- Permanent access with periodic review

**Initial**
- MFA with passwords
- Self-managed and hosted identity stores
- Manual identity risk assessments
- Access expires with automatic review

**Optimal**
- Continuous validation and risk analysis
- Enterprise-wide identity integration
- Tailored, as-needed automated access

**Advanced**
- Phishing-resistant MFA
- Consolidation of identity stores
- Automated identity risk assessments
Where Are We Now?
...Minneapolis!

**Traditional**
- Passwords or MFA
- On-prem identity stores
- Limited identity risk assessments
- Permanent access with periodic review

**Initial**
- MFA with passwords
- Self-managed and hosted identity stores
- Manual identity risk assessments
- Access expires with automatic review

**Optimal**
- Continuous validation and risk analysis
- Enterprise-wide identity integration
- Tailored, as-need automated access

**Advanced**
- Phishing-resistant MFA
- Consolidation of identity stores
- Automated identity risk assessments
OSU’s Target Maturity Level for Identity

- **Traditional**
  - Passwords or MFA
  - On-prem identity stores
  - Limited identity risk assessments
  - Permanent access with periodic review

- **Initial**
  - MFA with passwords
  - Self-managed and hosted identity stores
  - Manual identity risk assessments
  - Access expires with automatic review

- **Optimal**
  - Continuous validation and risk analysis
  - Enterprise-wide identity integration
  - Tailored, as-need automated access

- **Advanced**
  - Phishing-resistant MFA
  - Consolidation of identity stores
  - Automated identity risk assessments
Identity Pillar Goals

• Strong authentication
  • Mitigate phishing attacks
• Visibility of all accounts
  • Consolidate 11 AD domains
  • Manage all AD accounts
  • Link all accounts to identities
• Visibility of access for all accounts
Device Pillar Goals

- Central management of all* OSU-owned devices
- Greatly improved device management by automated patching
- Access to some applications will only be granted when the session comes from a compliant device
Goals for the Other Pillars

- Network
- Applications & Workloads
- Data

OSU intends to increase maturity of these pillars over time, and IAM will support these efforts.
**Possible Solutions**

What software components* are required to move beyond *Traditional* maturity?

<table>
<thead>
<tr>
<th>Component</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Repository</td>
<td>midPoint, COmanage</td>
</tr>
<tr>
<td>Account Provisioning</td>
<td>midPoint</td>
</tr>
<tr>
<td>Access Management and Recertification</td>
<td>Grouper</td>
</tr>
<tr>
<td>Authentication Risk</td>
<td>Duo Trust Monitor, Shibboleth plugin?</td>
</tr>
<tr>
<td>Strong Auth (MFA, phishing-resistant, passwordless)</td>
<td>Shibboleth, Duo</td>
</tr>
<tr>
<td>Device Compliance (OS, patch level, anti-virus)</td>
<td>Duo Device Health (Advantage license)</td>
</tr>
<tr>
<td>Zero Trust “Policy Engine”</td>
<td>Shibboleth plugin?</td>
</tr>
</tbody>
</table>

*There are many other commercial offerings for these components
# OSU’s Probable Solution

<table>
<thead>
<tr>
<th>Service</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Repository</td>
<td>Saviynt IGA</td>
</tr>
<tr>
<td>Account Provisioning</td>
<td>Saviynt IGA</td>
</tr>
<tr>
<td>Access Management and Recertification</td>
<td>Saviynt IGA, Grouper?</td>
</tr>
<tr>
<td>Authentication Risk</td>
<td>Azure SSO</td>
</tr>
<tr>
<td>Strong Auth (MFA, phishing-resistant, passwordless)</td>
<td>Azure SSO</td>
</tr>
<tr>
<td>Device Compliance (OS, patch level, anti-virus)</td>
<td>MS Defender for Endpoints (MDE), JAMF</td>
</tr>
<tr>
<td>Zero Trust “Policy Engine”</td>
<td>MS Conditional Access</td>
</tr>
</tbody>
</table>
Implementation Work
<table>
<thead>
<tr>
<th><strong>Saviynt Timeline</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IGA RFP</strong></td>
</tr>
<tr>
<td><strong>Sprint 1:</strong></td>
</tr>
<tr>
<td>• Establish identity repository</td>
</tr>
<tr>
<td>• Account provisioning for core directories</td>
</tr>
<tr>
<td><strong>Sprint 2:</strong></td>
</tr>
<tr>
<td>• Integrate 8 enterprise applications</td>
</tr>
<tr>
<td>• Account deprovisioning</td>
</tr>
<tr>
<td>• Reporting</td>
</tr>
<tr>
<td>• Initial access reviews</td>
</tr>
<tr>
<td><strong>Sprint 3:</strong></td>
</tr>
<tr>
<td>• Roles</td>
</tr>
<tr>
<td>• Access requests</td>
</tr>
</tbody>
</table>
Implementation Challenges

• Translating the details of our environment for our implementation partner

• UAT was hard and time-consuming due to our complexity (hundreds of attributes)

• Questioning our processes without being able to modify them:
  • Why do we let people change usernames? Because we make them based on name, why?
  • Could our identity de-duplication process be simpler?
Saviynt Capabilities Review (so far)

**Pros**
- Single identity repository for all users
- Automated provisioning
- All* accounts are visible and linked to identities
- Access Request workflows
- Cool features yet to tap (SoD, GRC)

**Cons**
- API and documentation have gaps
- Configuration management is crude
- Cannot use set-math to combine Roles
- Advanced skills are needed, may need to buy expert services from vendor
- Complex config necessitates some compromises
- Designed for corporations
Our RFP recommendations

Due diligence
• Get an extended test-drive
• Understand what the support contract actually covers
• Think about the cost – we paid for rapid implementation

Photo: Kevin M. Gill, Wikimedia, CC2
Wrap-Up
Zero Trust Next Steps

• Continue integrating apps with Saviynt
• Adopt institutionally-defined Roles
• Build access policies in Saviynt
• Deploy passwordless and phishing-resistant MFA
• Automate Banner access requests and recertification
• Consolidate AD domains
• Expand single identity store
Acknowledgements

- David McMorries (CISO)
- Marjorie McLagan (Deputy CISO)
- Emily Longman (SOC Manager)
- IAM Team
  - Andy Morgan
  - Chris Evans
  - Doug Weir (Manager)
  - Jason Peak
SOURCES

NIST SP 800-207 Zero Trust Architecture
https://csrc.nist.gov/pubs/sp/800/207/final

Cybersecurity and Infrastructure Security Agency (CISA)
Zero Trust Maturity Model
https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
• Vendor lock-in concerns?
• Can we run this with 3 people?
• How do we scale up roles?
• Does Zero Trust work across the InCommon Federation?
• Can we retire Grouper? (We love Grouper, though)
• Are we okay with the annual expense to run/support Saviynt?
• How do we feel about Microsoft’s IGA offering?
• Is anyone else doing Zero Trust formally?
• Does anyone else use Saviynt IGA?