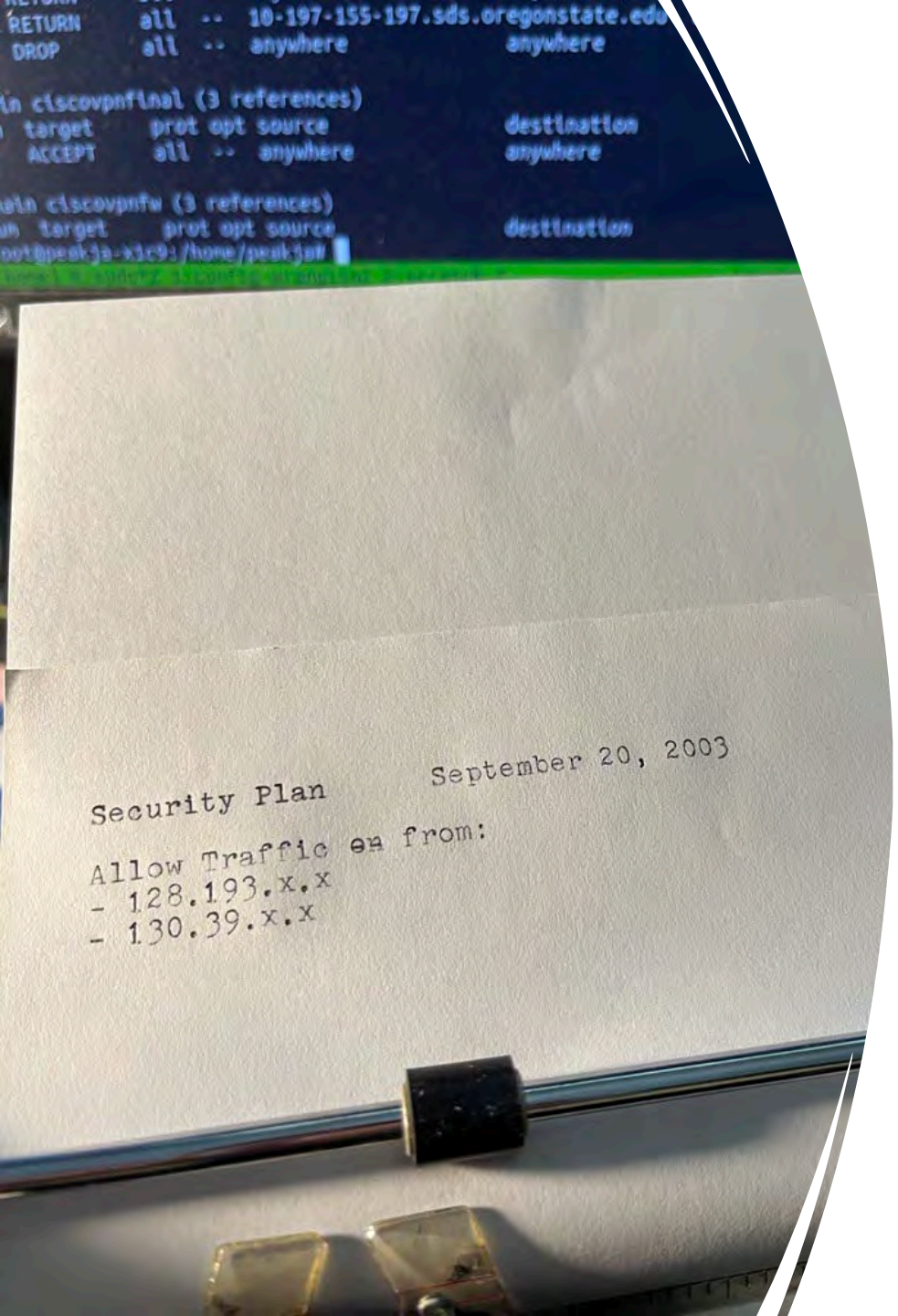
Zero Trust: Identity's Critical Role

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

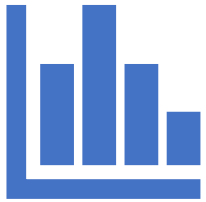
Graphic: CISA ZTMM

Zero Trust Maturity Model Pillars

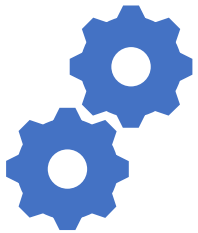
Identity	set of attributes that uniquely describes a user or entity, including non-person entities
Devices	any asset (including its hardware, software, firmware, etc.) that can connect to a network
Networks	internal networks, wireless networks, and the Internet
Applications & Workloads	systems, computer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

Extracted from CISA ZTMM

Cross-Cutting Capabilities



Visibility and Analytics



Automation and Orchestration

Governance

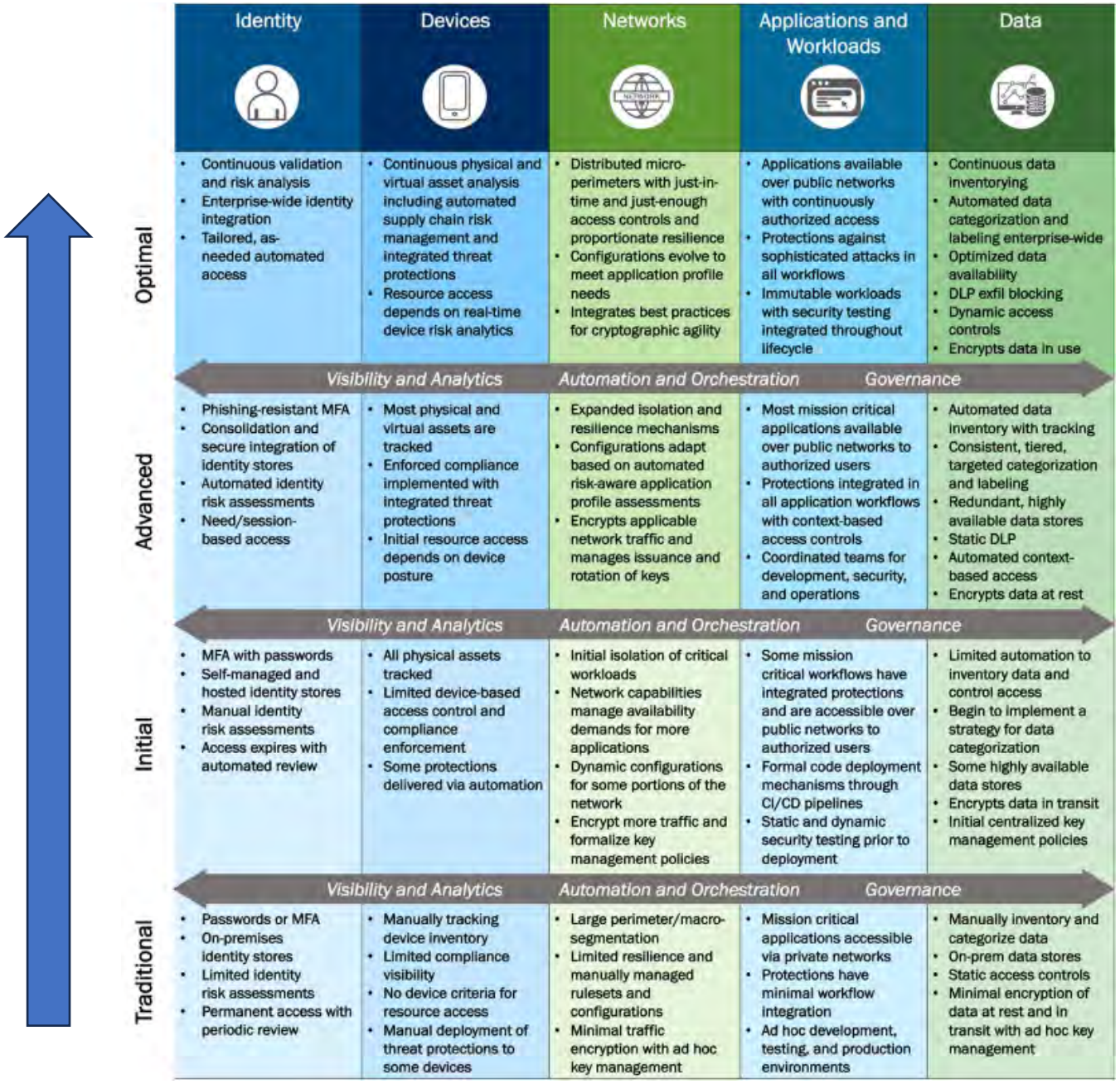
Maturity Levels

OPTIMAL
Fully automated

ADVANCED
Where applicable, automated controls for lifecycles

INITIAL
Starting automation

TRADITIONAL
Manually configured



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?

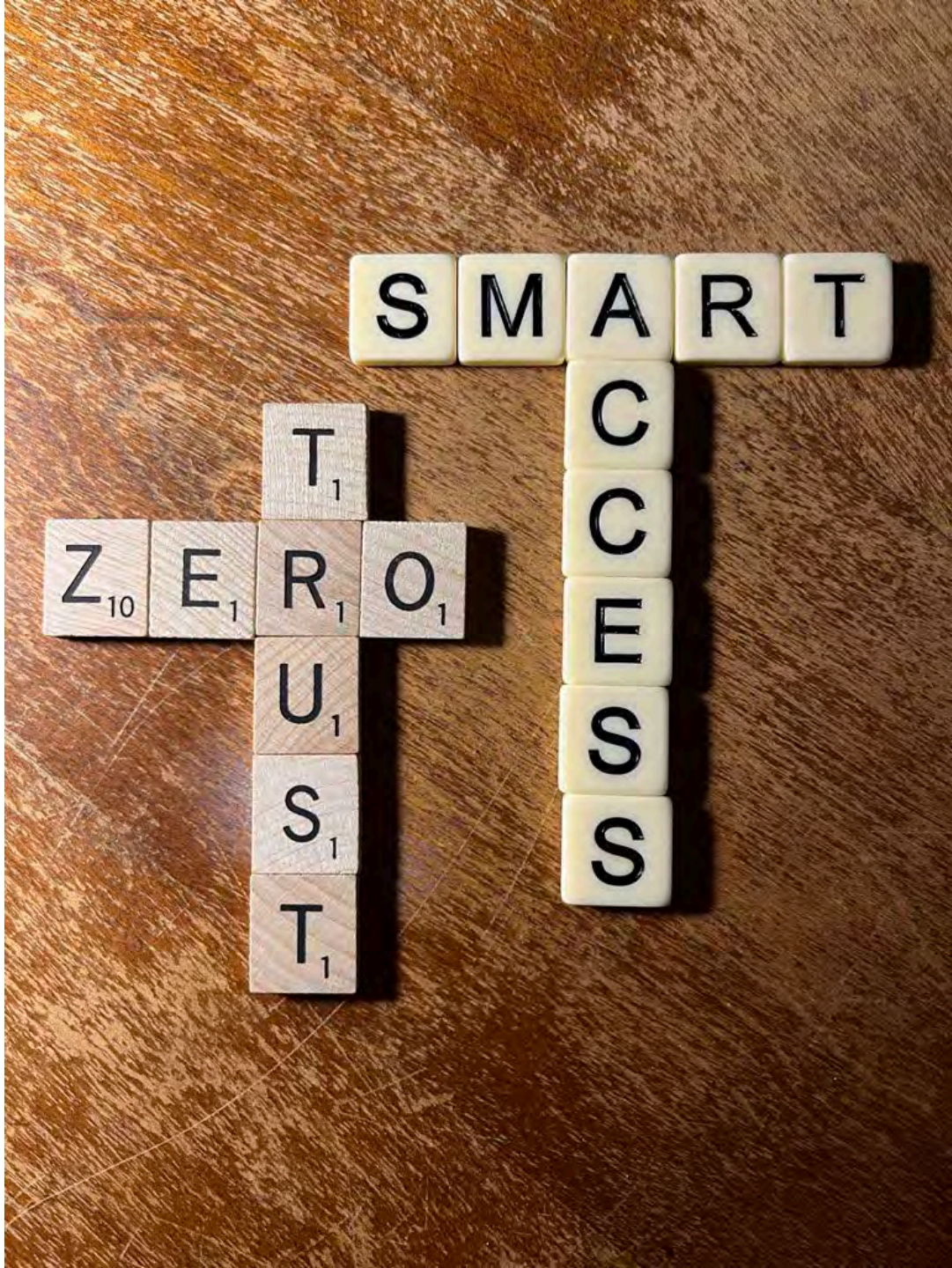
A very short dramatization...

[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!



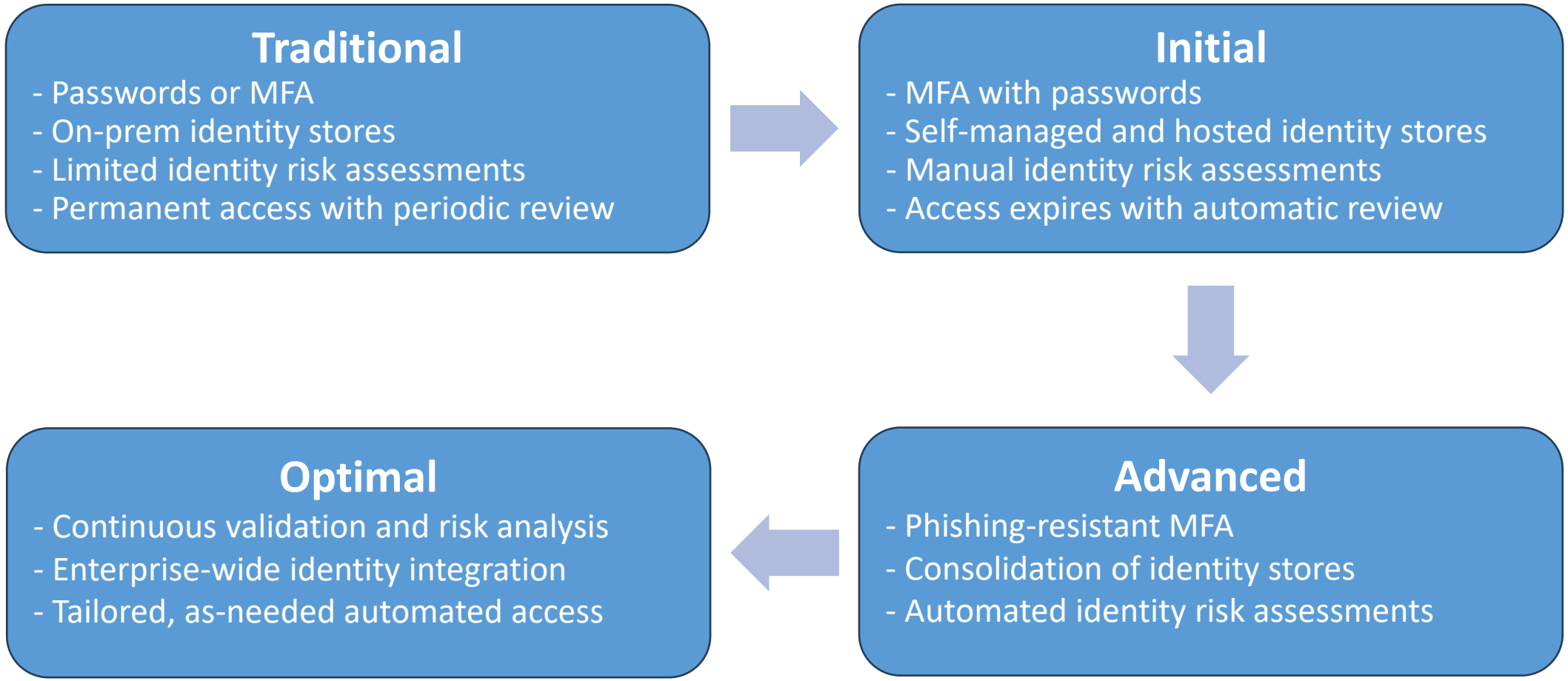
Where we're coming from

...Corvallis, Oregon

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

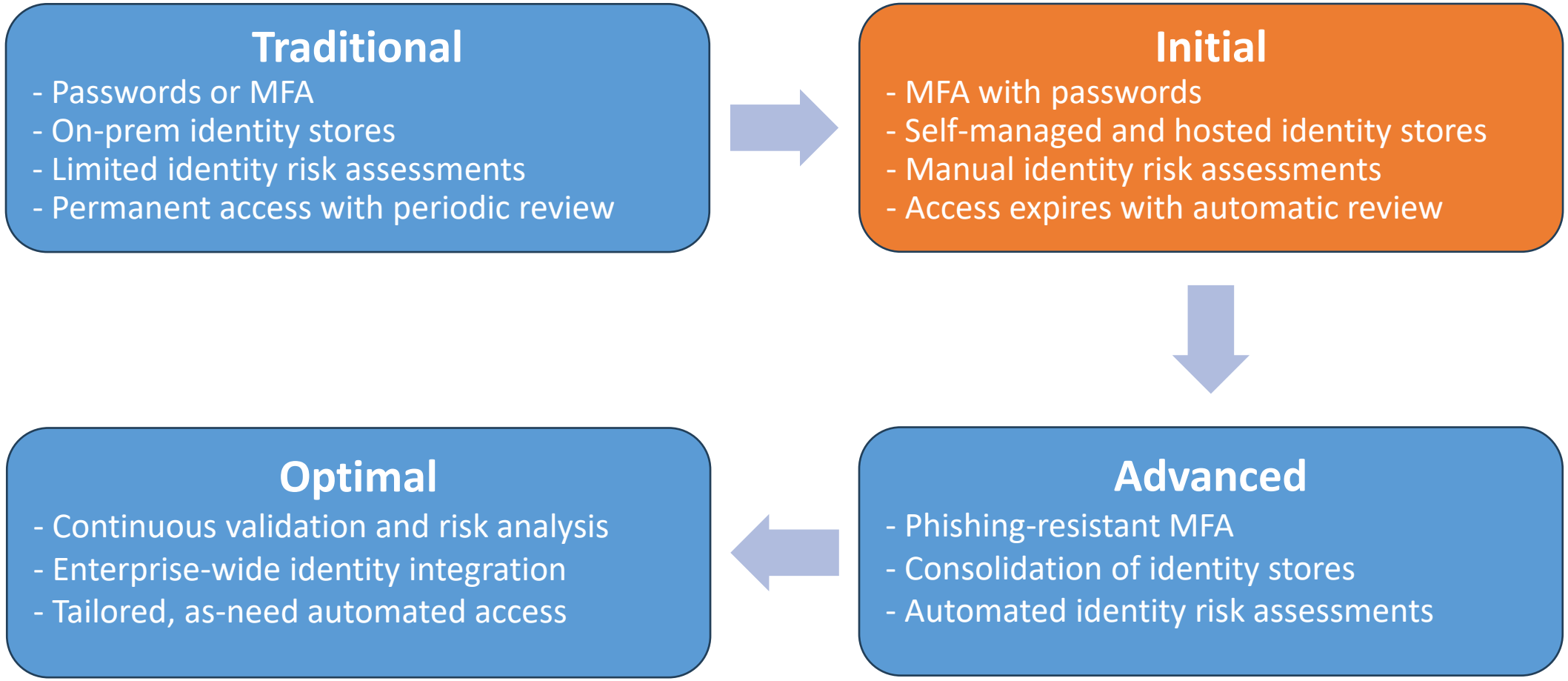
Photo: OSU stock, Frank Miller

Identity Pillar Maturity Levels

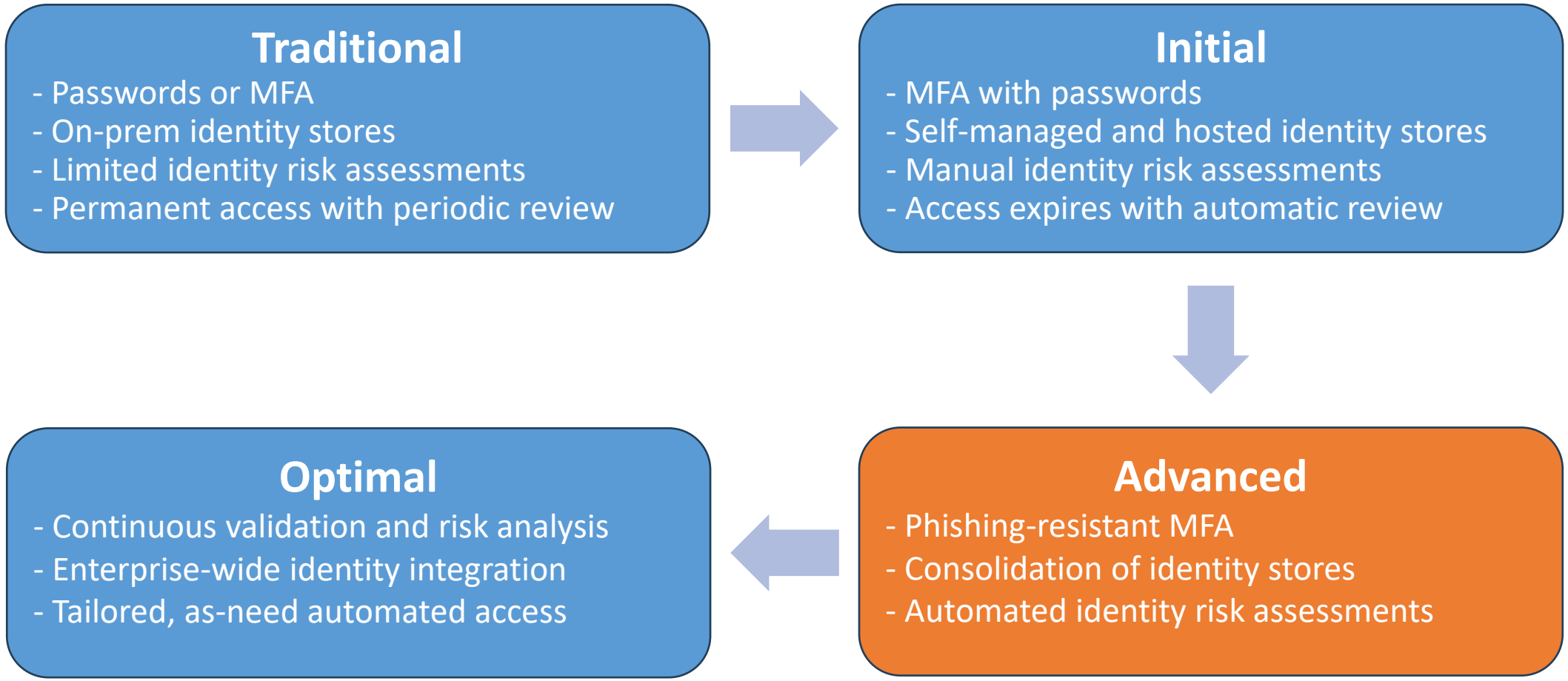


Where Are We Now?

…Minneapolis!



OSU's Target Maturity Level for Identity



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

Photo: Alec.cortez, Wikimedia

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

Photo - Patrick McCrary, OSU

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?

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

*There are many other commercial offerings for these components

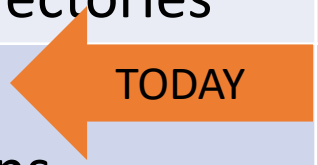
OSU's Probable Solution

Identity Repository	Saviynt IGA
Account Provisioning	Saviynt IGA
Access Management and Recertification	Saviynt IGA, Grouper?
Authentication Risk	Azure SSO
Strong Auth (MFA, phishing-resistant, passwordless)	Azure SSO
Device Compliance (OS, patch level, anti-virus)	MS Defender for Endpoints (MDE), JAMF
Zero Trust "Policy Engine"	MS Conditional Access

Implementation Work

Saviynt Timeline

IGA RFP	January 2022 – September 2022
Sprint 1: • Establish identity repository • Account provisioning for core directories	October 2022 – June 2023
Sprint 2: • Integrate 8 enterprise applications • Account deprovisioning • Reporting • Initial access reviews	May 2023 – November 2023
Sprint 3: • Roles • Access requests	October 2023 – February 2024



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?

Photo: Jason Peak