Making Zero Trust Real

Your Presenter:
Ahmad Abdulfattah
Ahmad.Abdulfattah@oneidentity.com

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and principal analyst for Forrester Research, based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted

Reference: https://go.forrester.com/speakers/john-kindervag/

Zero Trust is a Concept

The principle of least privilege is **a security concept in which a user is given the minimum levels of access or permissions** needed to perform their job.

Not the same meaning “Least Privilege”

No solution covers all

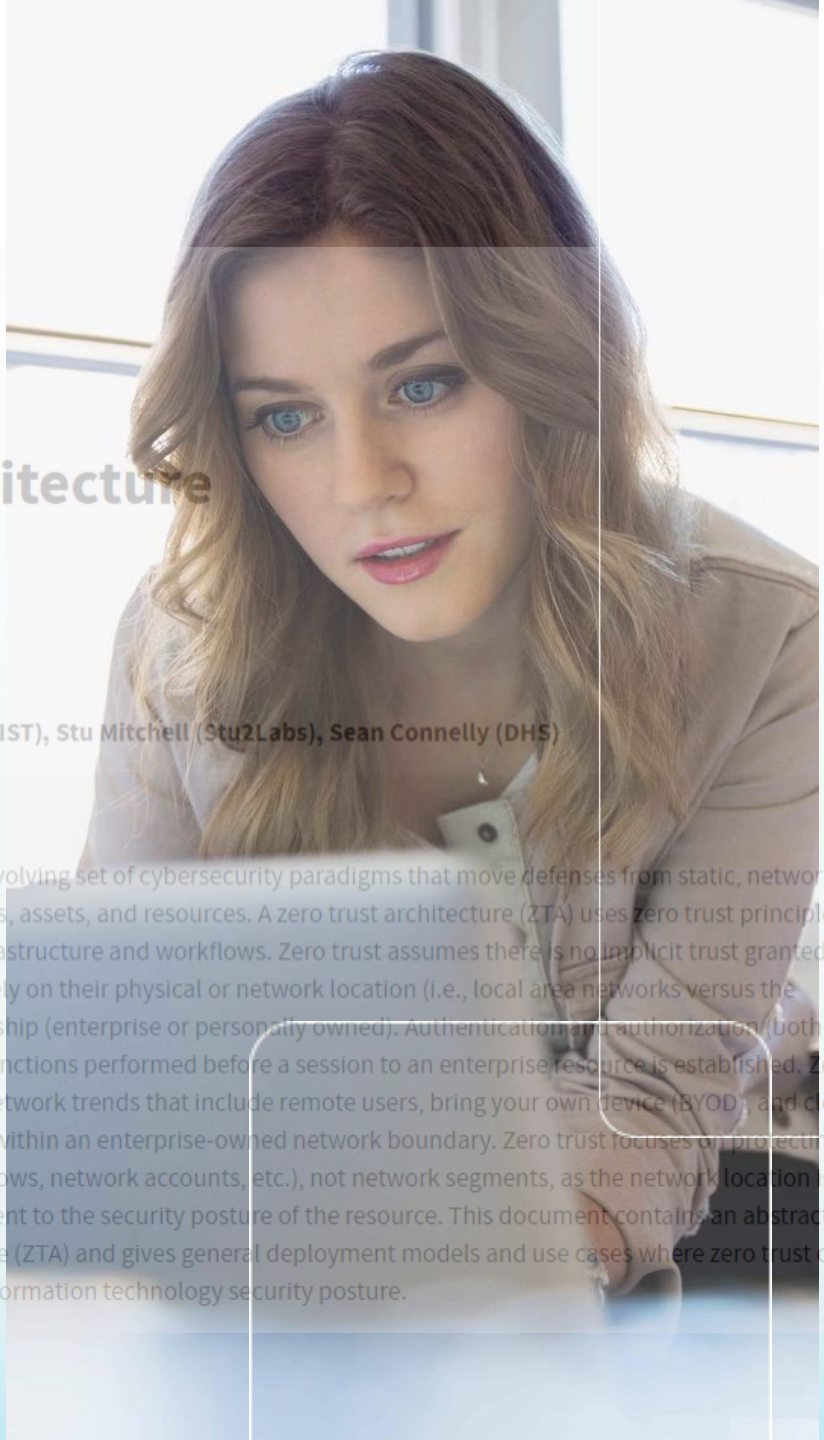
A mentality, not a product

ONE IDENTITY

Standardizing Zero Trust - NIST

NIST SP 800-207, *Zero Trust Architecture, Aug 2020*

https://csrc.nist.gov/publications/detail/sp/800-207/final



ZERO TRUST

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.

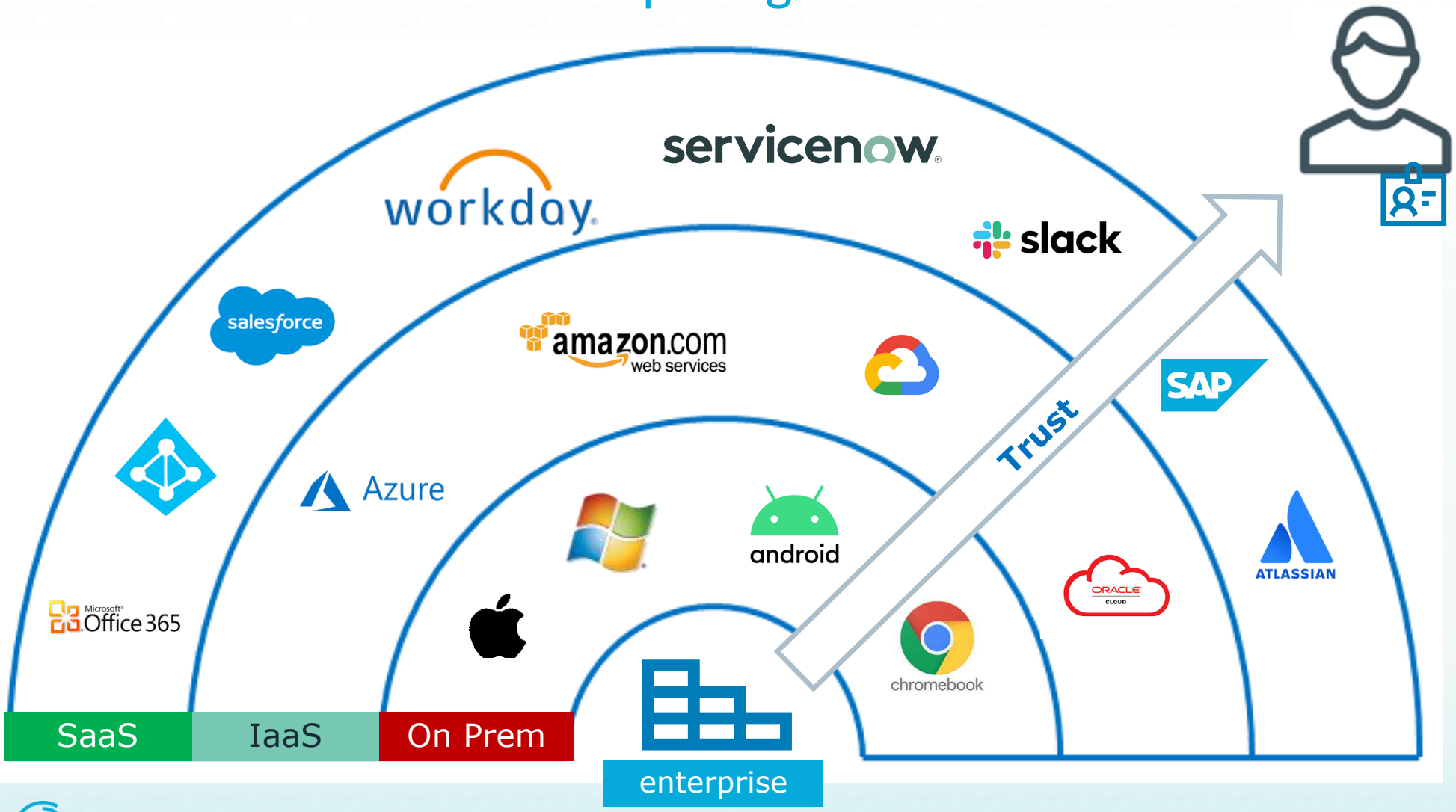
Reference: NIST SP 800-207 "Zero Trust Architecture"

NIST – The seven tenets of Zero Trust

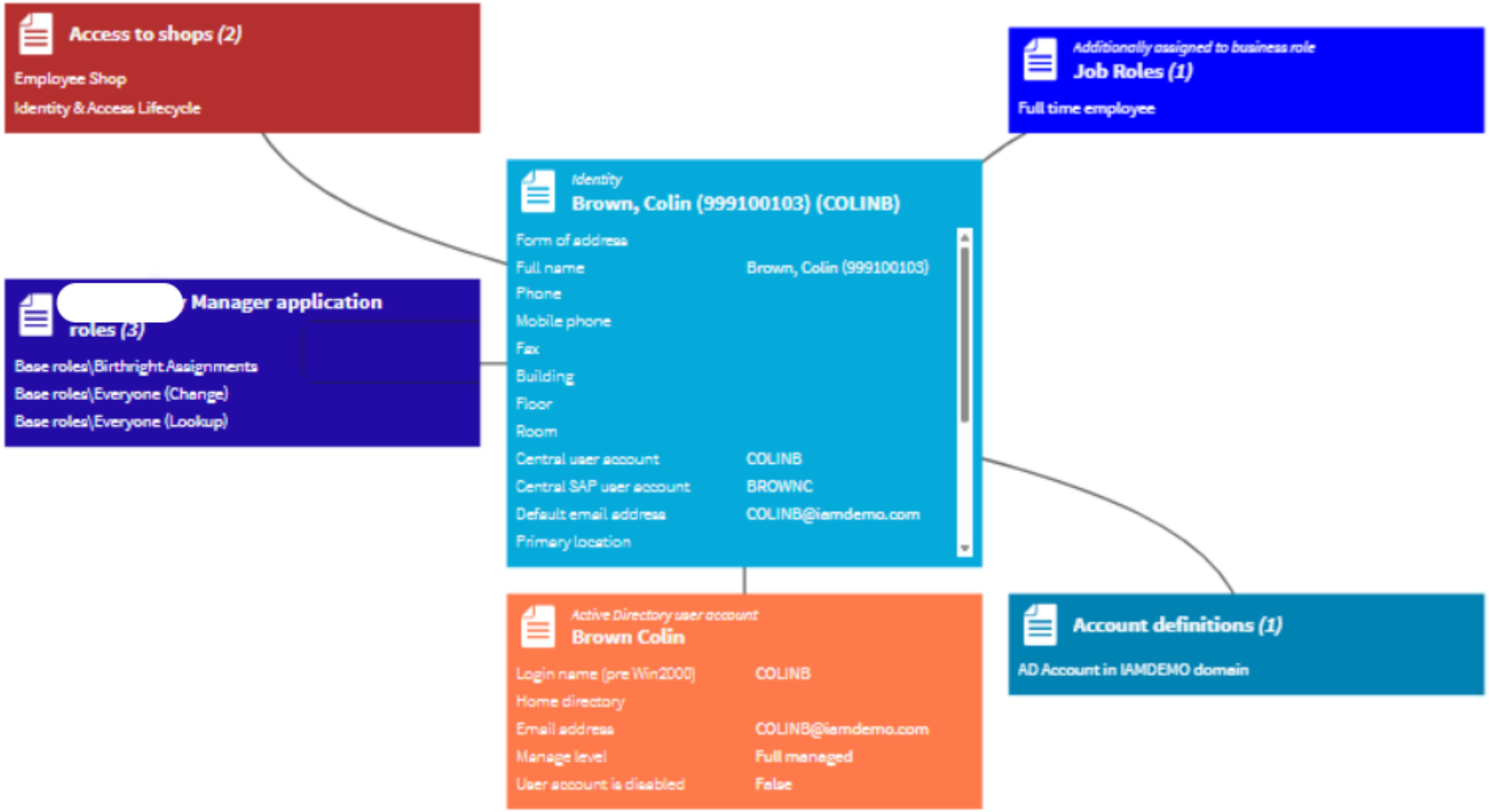
1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of 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"

All data sources and computing services are considered resources.



Identity HyperView



How To make Zero Trust Real

Control Access	Enforce least privileged access	Manage privileged access	Collect logs
•control access, ensure the least privilege model is implemented, and dynamically remove access when no longer required for any connected system	•Allow Zero Trust concepts to be applied to Active Directory by providing account lifecycle management, dynamic roles and access control, and strictly enforcing the least privilege model for access to Active Directory and all attached systems.	•Provide the complete range of privileged access management solutions to ensure the powerful identities and accounts that run the enterprise are under strict control, and this can be proven through detailed audit trails and reports.	•Flexible and scalable log management across the enterprise to ensure the most efficient and cost-effective use of SEIM

The cloud journey

Thank You!