RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: PART3-R05

Taming Identity Sprawl to Close the Cybersecurity Exposure Gap

Larry Chinski

Vice President Global Strategy
One Identity

Disclaimer

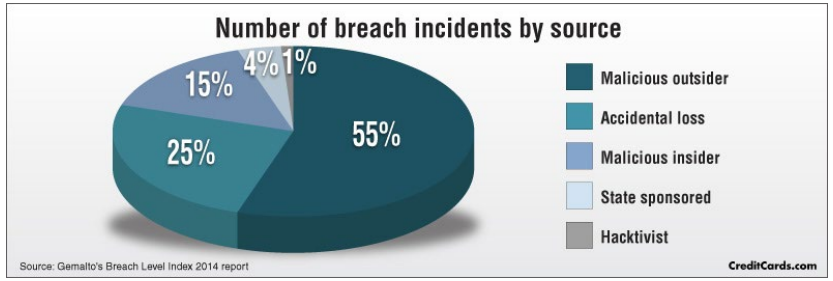
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Four Stages of Vendor Presentations

Scary Stats



Headlines

About Us

Technical Deep Dive

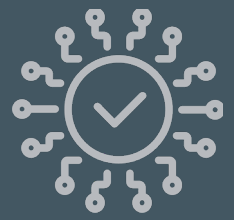
RSAConference2022

Segment 1

Understanding the Cyber Security Current State

Current State of Cyber Security – Part 1

Understanding the current threat surface



Infrastructure-centric

PROTECT everything

(Fragmented Approach to Identity)

Identity-centric

VERIFY everything

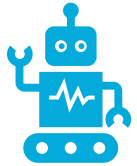
(Unified Approach to Identity)

The traditional perimeter is eroding, and **identity is emerging as the new perimeter**

Current State of Cyber Security – Part 2

Identities have increased exponentially

Millions of users
internal, external and customers



More machines than humans
everything instrumented

Ever-expanding accounts
legacy, cloud, hybrid, edge

Identity sprawl

RSAConference2022

Segment 2

Understanding the Challenge

The Current State

Identity is now more difficult to protect

Yesterday

- Employees
- Hired for one job
- Single access point
- People
- Office-bound

Today

- Employees, contractors, suppliers, partners
- Roles change frequently
- Access changes based on circumstances
- People + applications + machines
- Hyper-dispersed, mobile

Understanding the Identity Challenge

- Identities not limited to actual people
  - Devices, apps, bots, etc
- Multiple tools deployed
- Tools are independent and siloed
- Identities in one tool unaware of identities in others
- Fragmented state created
- Multiple processes created based on types of tools in use

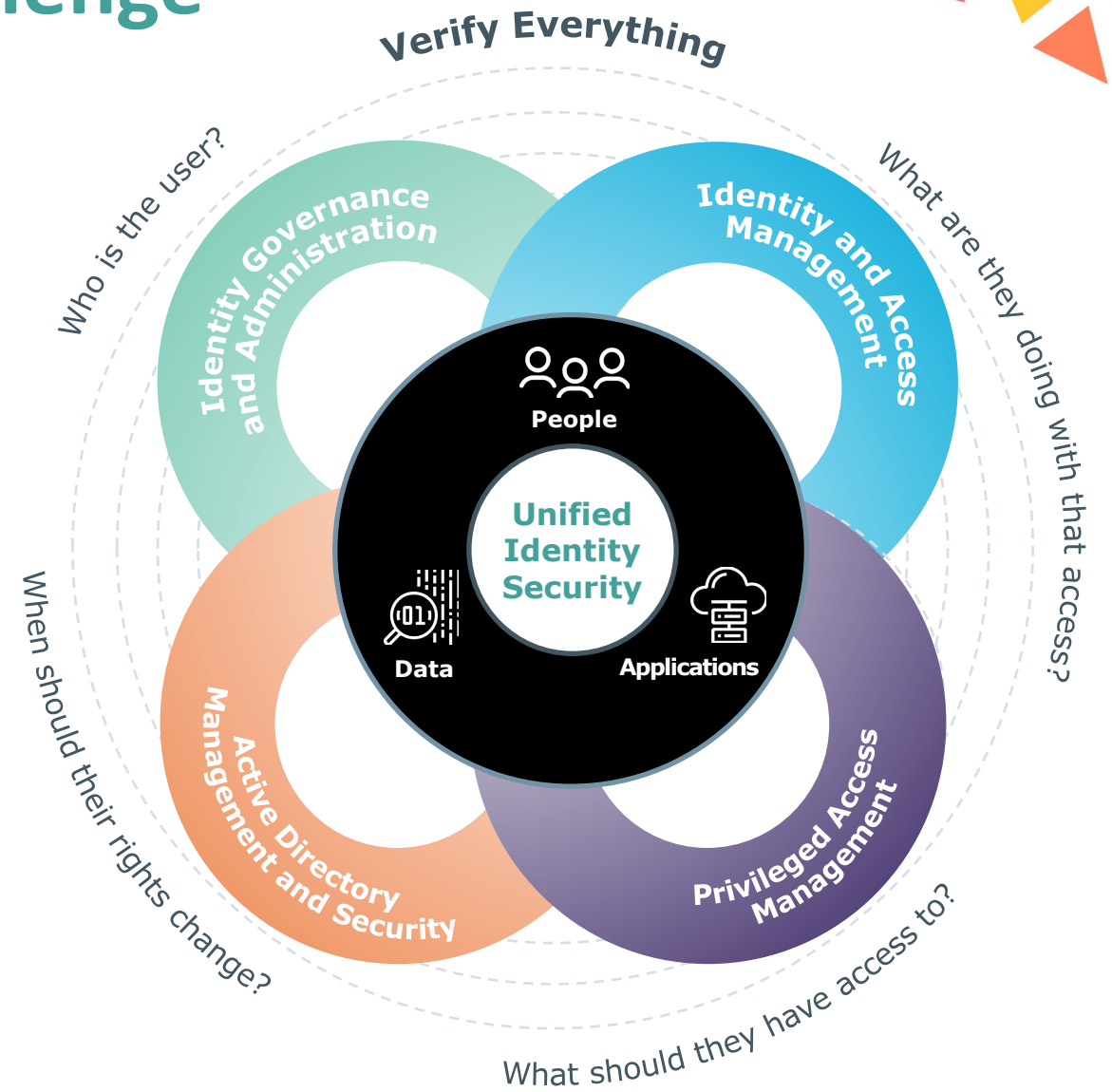
RSAConference2022

Segment 3

Addressing the challenge

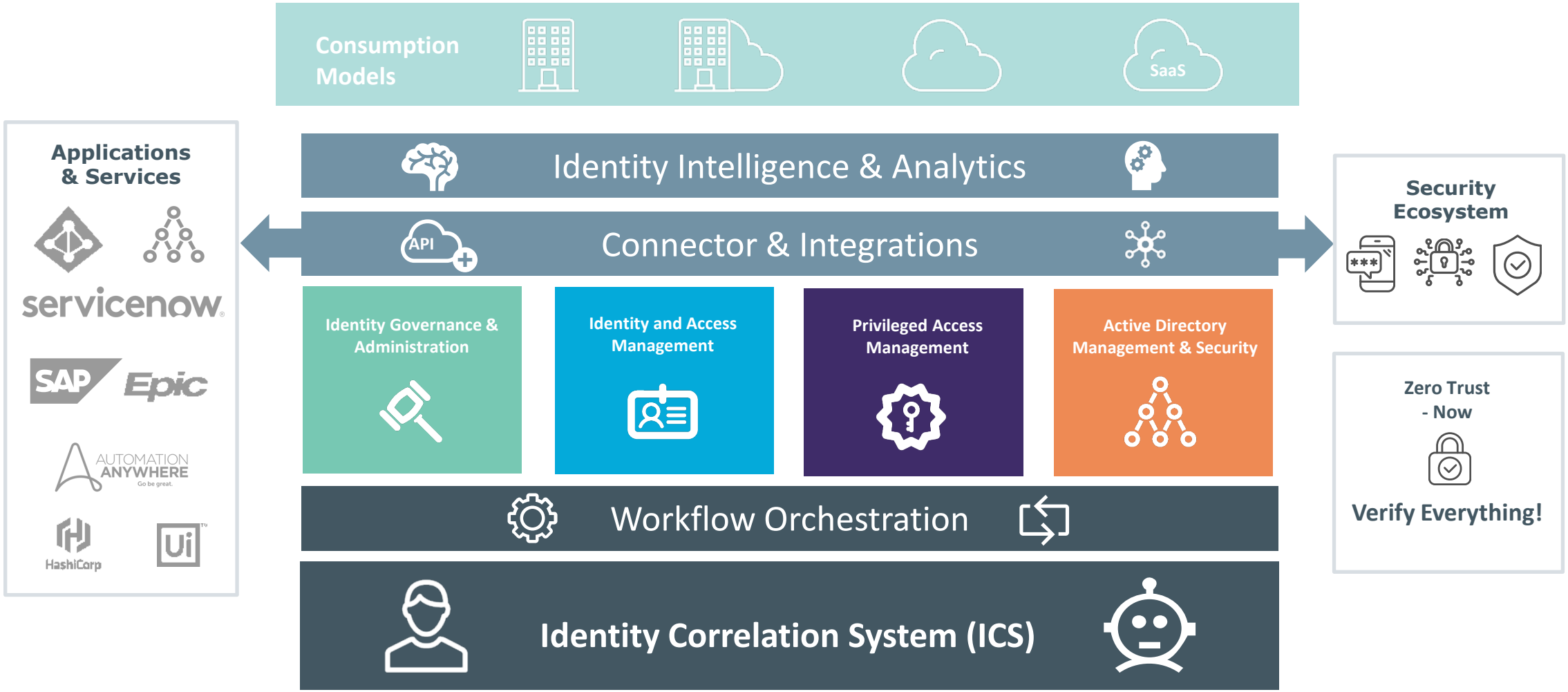
Addressing the Identity Challenge

- Unify to a single platform
- Identity becomes the center
- Individual tools integrated together and correlated based on identity events



Unified identity security platform

People | Applications | Data



The unified identity security journey

0 FRAGMENTED state

- Identity **sprawl**
- **Siloed** identity security tools
- **Exposed**

1 BASIC state

- Identity **management**
- **Point solutions** for PAM, IGA, and AD Management
- **Managed**

2 UNIFIED state

- Identity **correlation**
- **Unified platform** with best-in-class PAM, IGA, and AD Management solutions
- **Verified**

3 Resilient state

- Identity **orchestration**
- **Integrated** ecosystem to streamline processes and achieve adaptive resilience
- **Optimized**

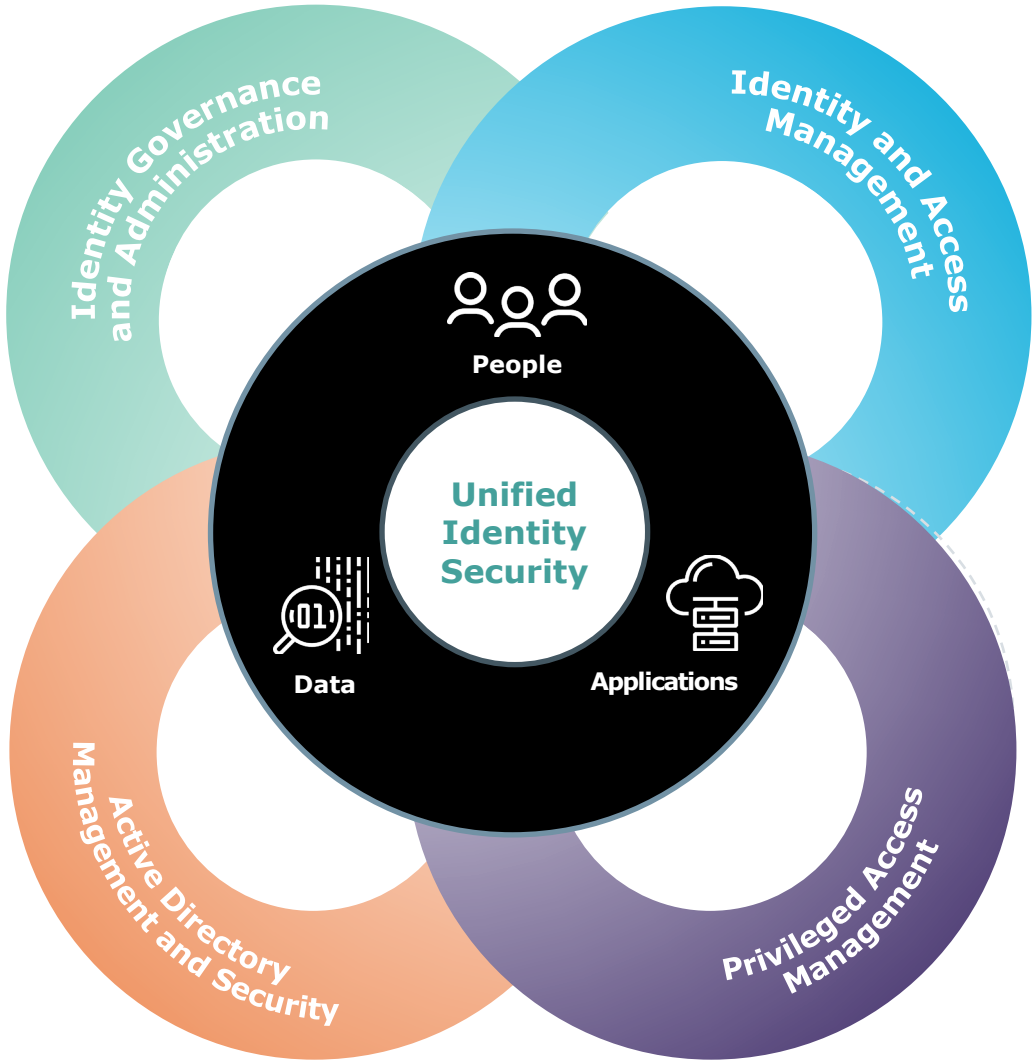
Ever-improving protection and economics

RSAConference2022

Segment 4

Using PAM as a Starting Point

Start anywhere, as long as it is PAM!



Identity Governance and Administration

Lifecycle Management, Access Certification

Identity Access Management

- Single Sign-On
- Multi-Factor Authentication (MFA)
- Advanced Directory

Customer Identity

Privileged Account Management

- Privileged Passwords
- Privileged Sessions
- Privileged Analytics
- Authentication Services
- Remote Access

Active Directory Management

- Policy Management
- AD Security

Why Start with PAM

You probably already have it!

Current State

- Identities, especially privileged accounts are being targeted by bad actors
- 85% of organizations say that employees have more privileged access than needed
- High levels of friction introduced to users who are trying to access privileged assets remotely
- Achieving Zero Trust is practically impossible due to underlying complexity
- Opaque insights into privileged user activity
- Impossible to leverage analytics to proactively identify and act on risk

Future State

- Securely store, manage, record and analyze privileged access
- Provide the right access at the right time – and nothing more
- Connect remote privileged users to servers and other critical resources through any browser, with no VPN required
- Adaptive Zero Trust attained with ability to apply and manage credentials just in time
- Know what your privileged users are doing, working with session monitoring/recording
- Use machine learning and behavioral biometrics to identify deviation from “normal” behavior

PAM Integration Components

PAM+IGA

- Privileged access governance

PAM+AD Management

- Zero Trust
- Just in Time

PAM+IAM

- PAM Remote Access

ONE IDENTITY
by Quest