
AVEVAWORLD
PARIS

Mike Lemley

Product Security Chief Architect

THINK SECURE

AVEVA

OCTOBER 2024

Agenda

AVEVA World 2024
Paris

THINK SECURE

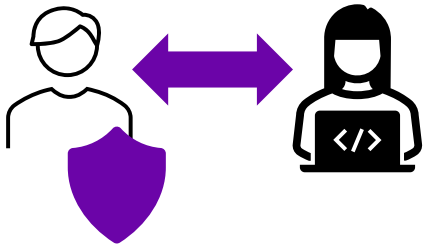
- Culture of building security in
- Shared responsibilities in a hybrid infrastructure
- Resiliency of CONNECT data services
- Identity
- Operational countermeasures
- Future

AVEVA

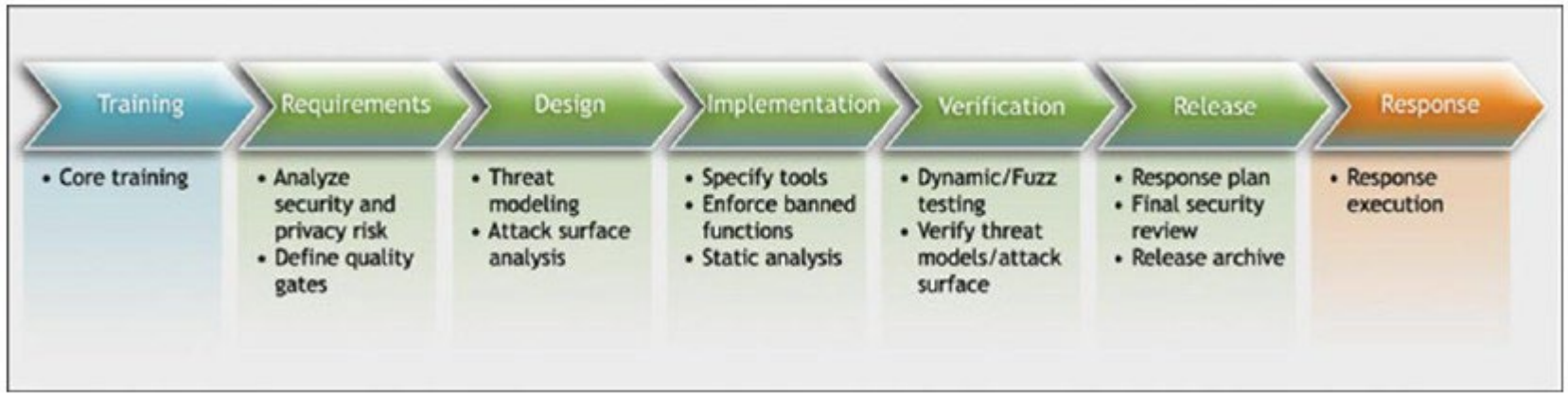
Culture of building security in

Security Development Lifecycle Execution

- Secure frameworks, platforms
- Scorecard
- Security Tools & partners



Architecture is accountable for secure architecture



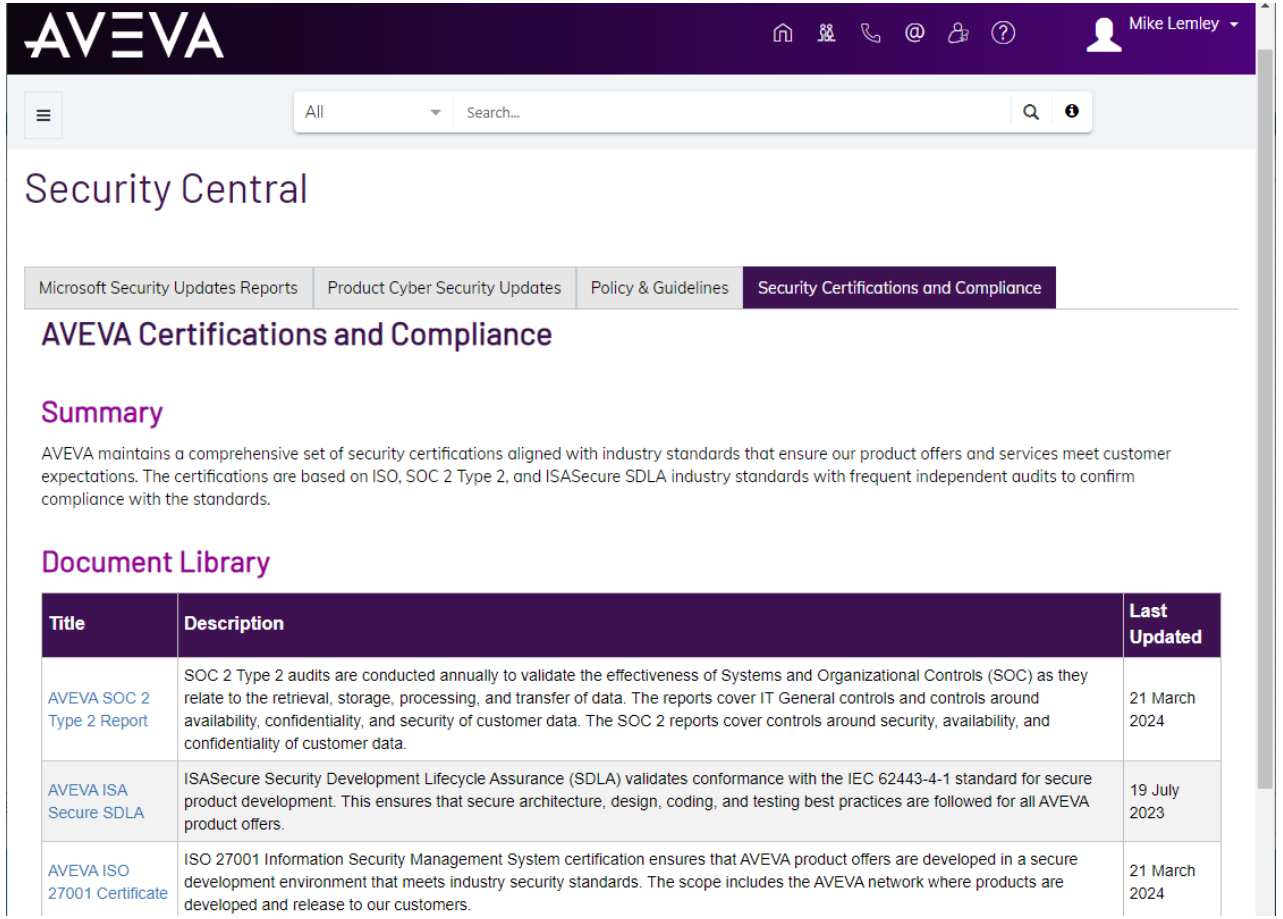
AVEVA Certification & Audit Strategy

- Now
  - ISO 27001
  - SOC-2
  - ISASecure/IEC 62443
- Future
  - Cloud Security Alliance (CSA) Star Level 1

Certifications and Compliance

- Self-service
  - Certifications and compliance
  - Policy & Guidelines
- Coming soon for PI customers.

https://softwaresupportsp.aveva.com/#/securitycentral

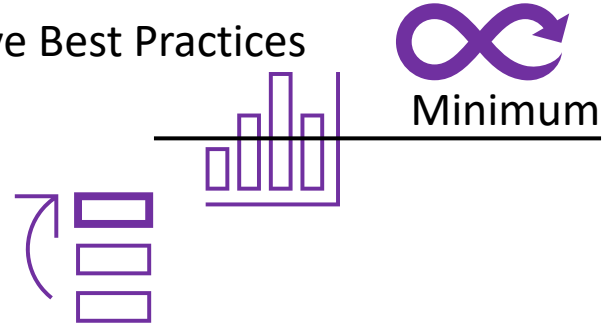


Scorecard

- Itemize Best Practices
  - Clear maturity levels identified

- Quickly evaluate Best Practices
  - Multiple choice selection

- Help plan to iteratively improve Best Practices
  - Minimum bar
  - Rank (Prioritized advice)



What is a Measurement?

Best Practice Maturity Measurement

I bathe **monthly** and clean my hands before meals.

What's my score?

Hygiene

maturity

a. Bathe never (0)

b. Bathe monthly (1)

c. Bathe weekly (5)

d. Bathe weekly and clean hands before meals (10)

Foundation repeated

Response option

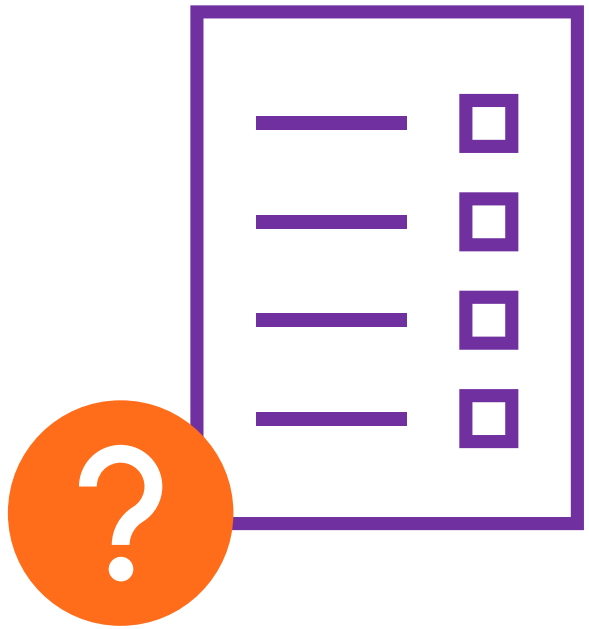
Points
(0 to 10)

e. Unanswered

AVEVA

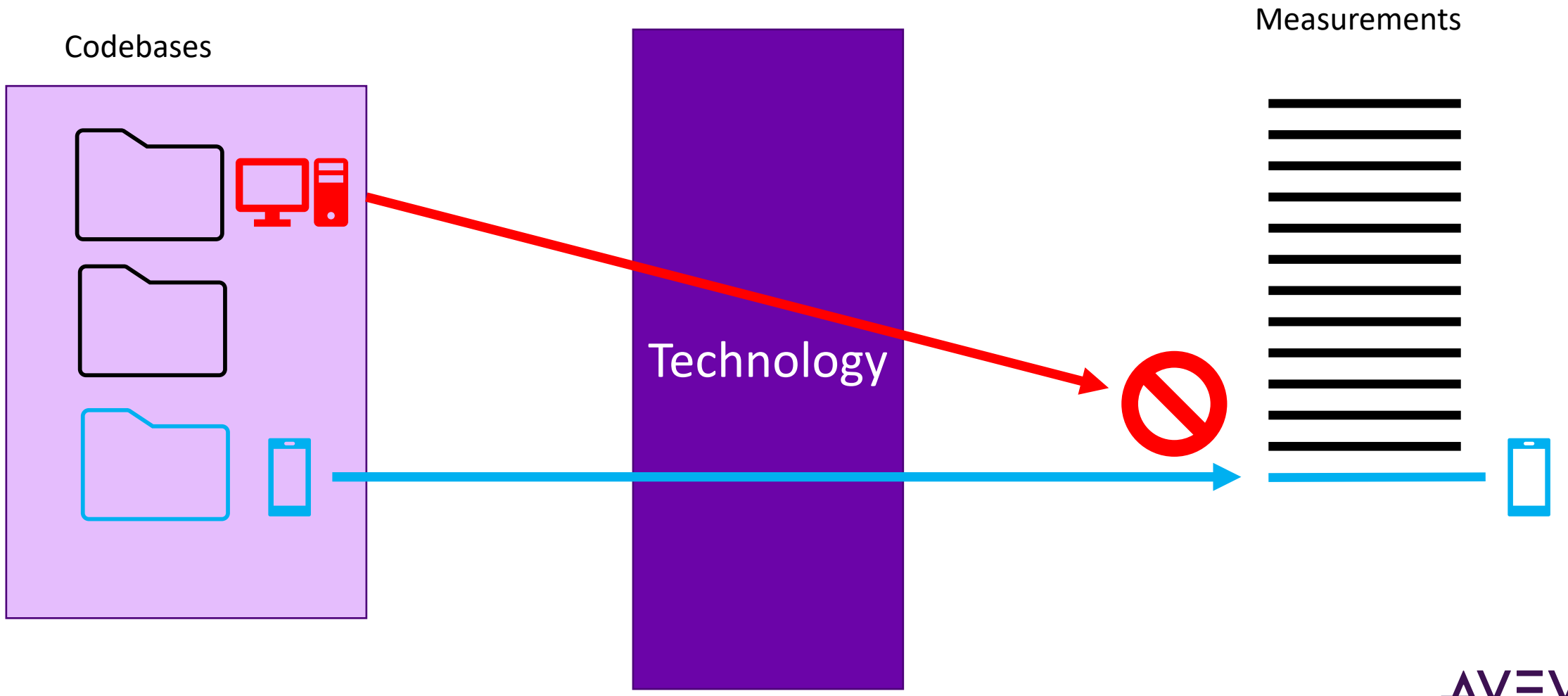
None of the response options apply

- Talk to your technical leadership, escalating up to Architecture
- Possible outcomes:
  - Wrong codebase configuration
  - Need new option
  - Unclear wording
  - Waiver needed
- NEVER
  - We should be 10 – I'll take a "similar" 10 response.



Ask Appropriate Questions

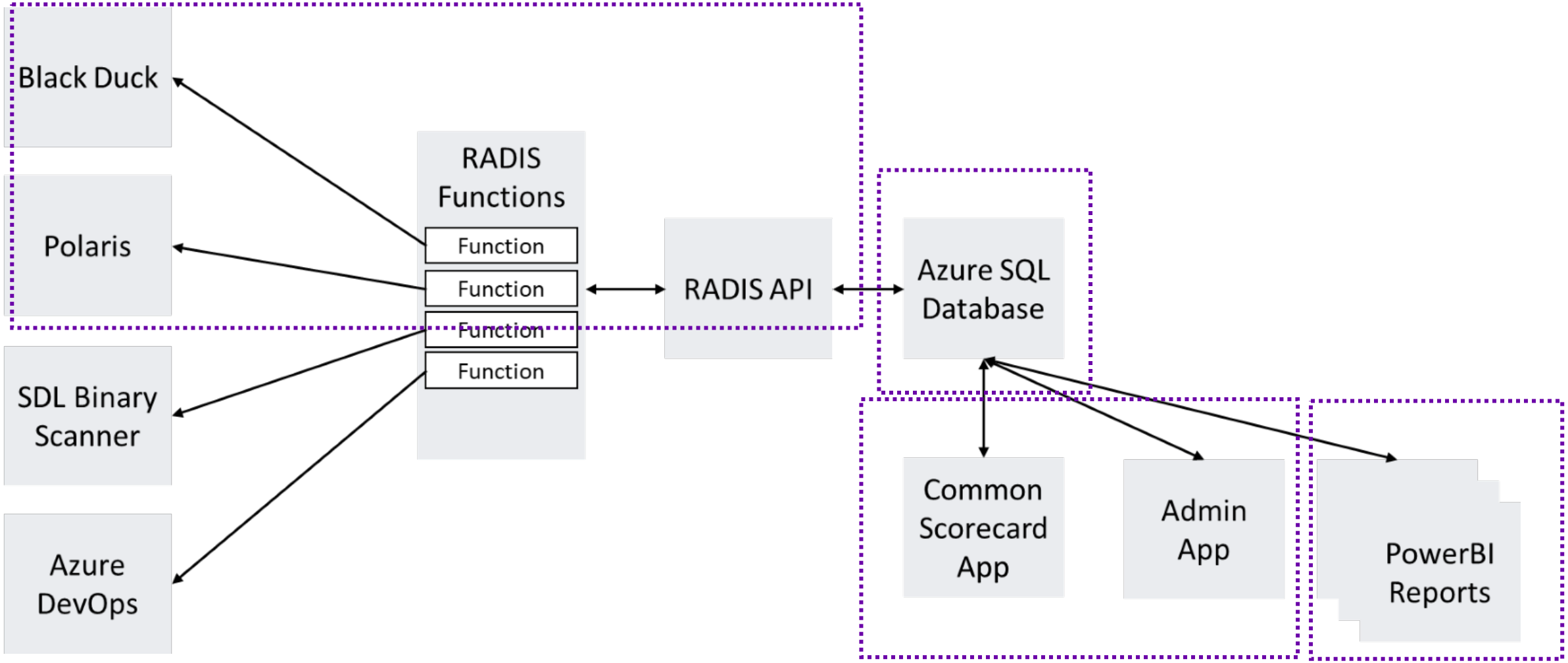
Codebases::Measurements



Scorecard in a nutshell

- Prioritized advice
- Quick assessments
- Identify blockers in planning
- Consistent advice
- Continuous improvement

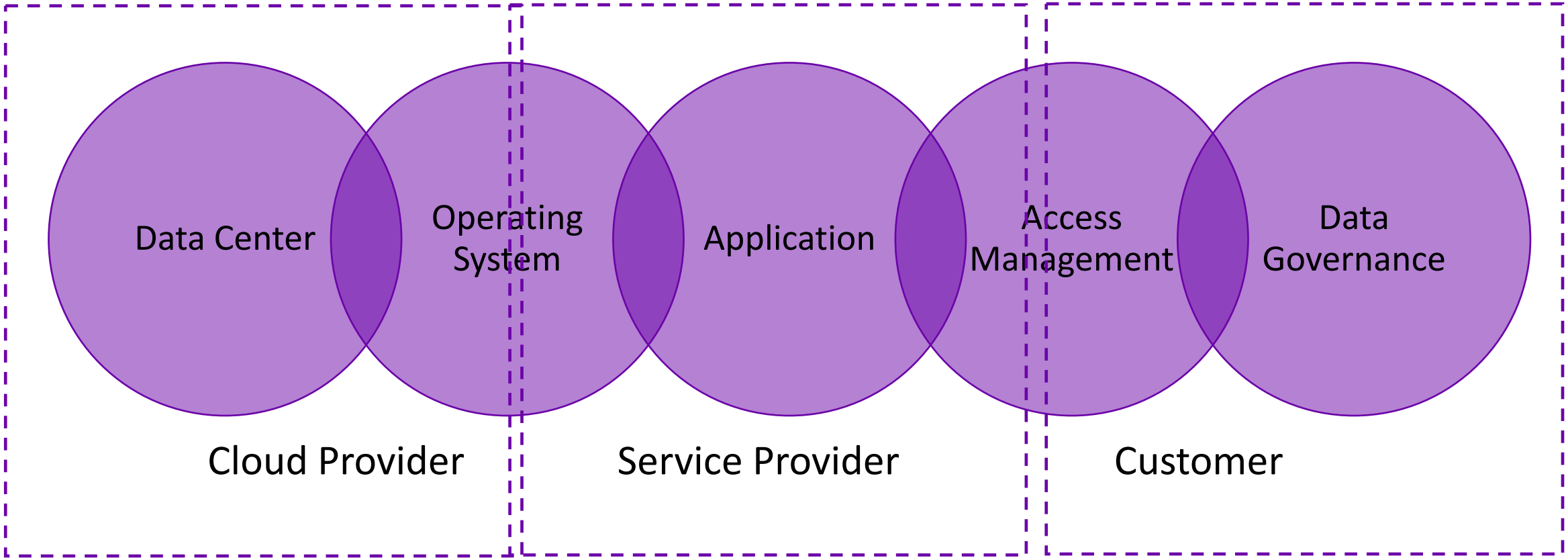
R&D Information System (RaDIS)



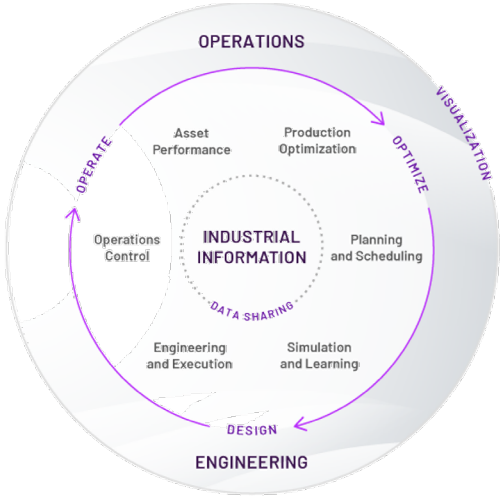
Shared responsibilities in a hybrid infrastructure

CONNECT data services

Supply chain security advantage



Industrially trusted > increasing shared responsibility



AVEVA is your Industrial Information Platform Partner

Responsible for security “at” use

Customer end users

- User management, roles & permissons
- Protecting account credentials
- Federate Identity

Responsible for security “in” the cloud

AVEVA cloud solutions

- Customer data
- Platform, applications, identity & access management
- Operation systems, network and firewall configuration
- Client- side data encryption & data integrity, authentication, server-side encryption (file system and data), network traffic encryption, integrity, identity

Responsible for security “of” the cloud

Public cloud service provider

- Software
- Compute, storage, database, networking
- Global infrastructure
- Regions, availability zones, edge locations

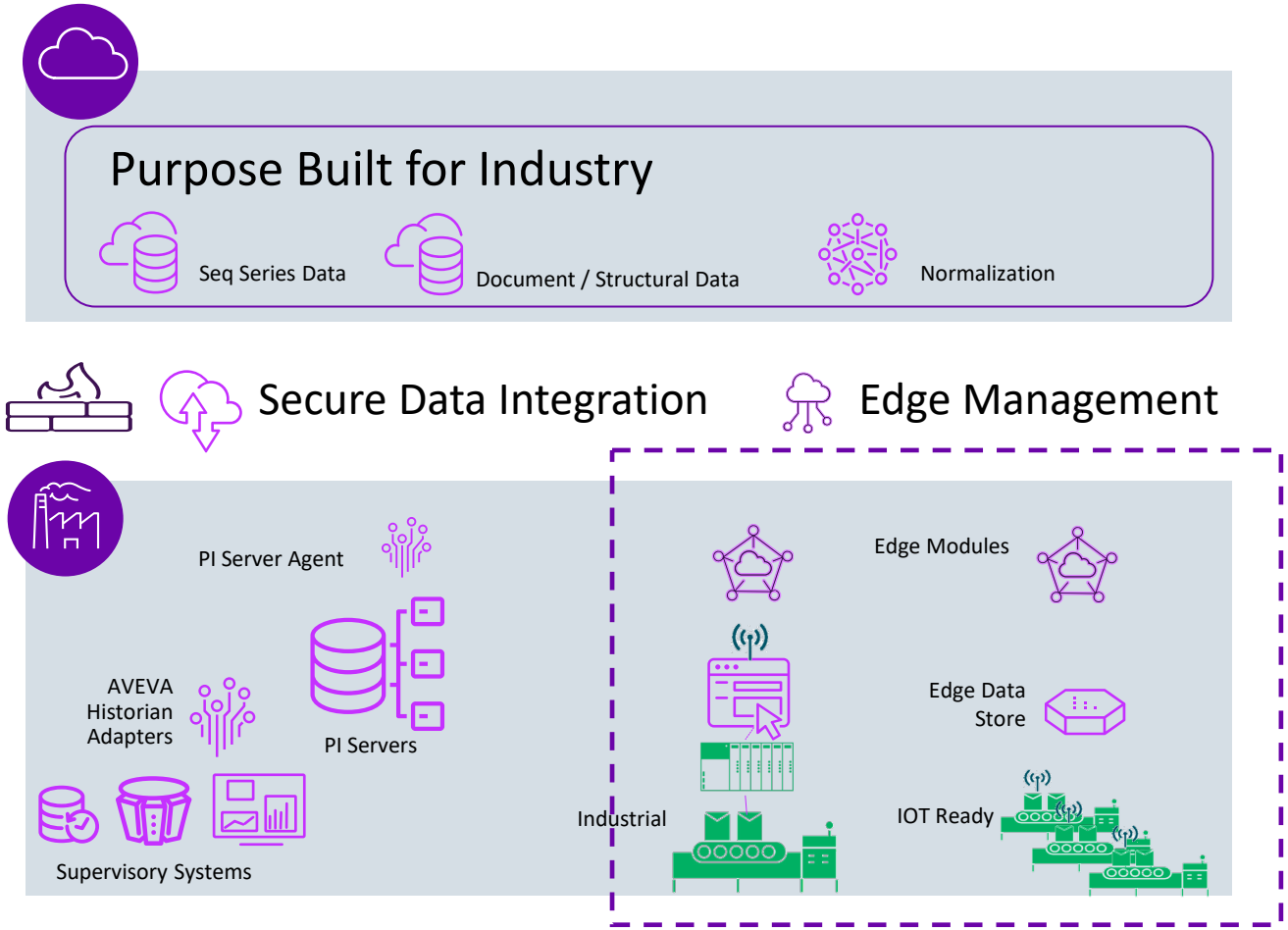
Resiliency of CONNECT data services

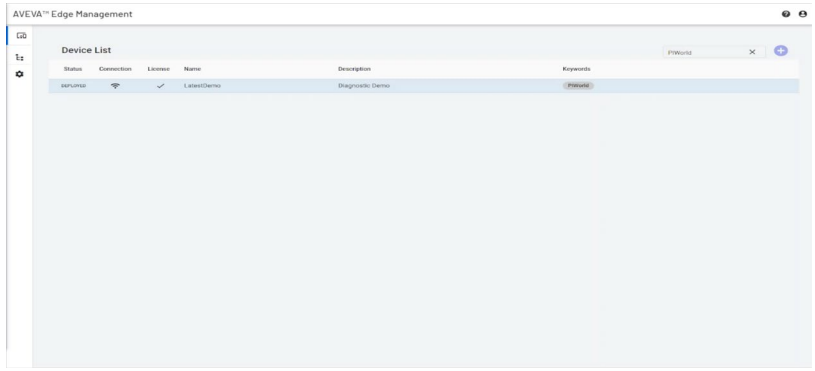
Resiliency

- Consistent, reliable configuration
- Reliable updates (undoable)
- Continuous Testing
- Reliable data

Secure Plant Architectures

- Hybrid Approach





Device health

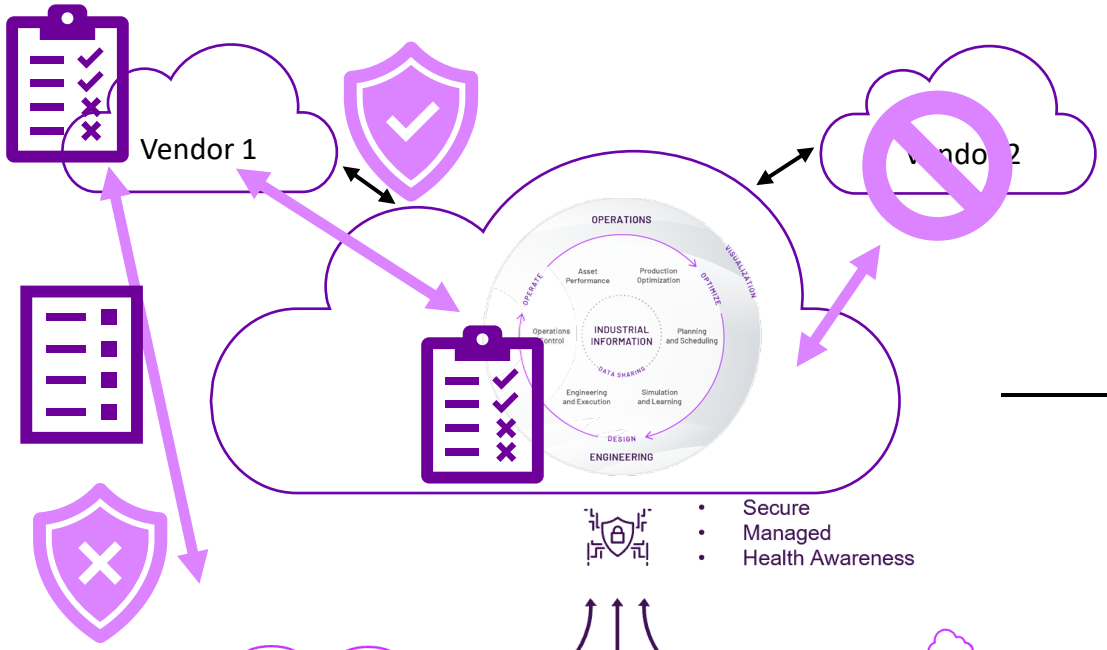
Edge Managed Modules

Secure connection from plant side

Adapter Integration
(e.g. PI Servers, Wonderware)

Data sharing management

- Communities

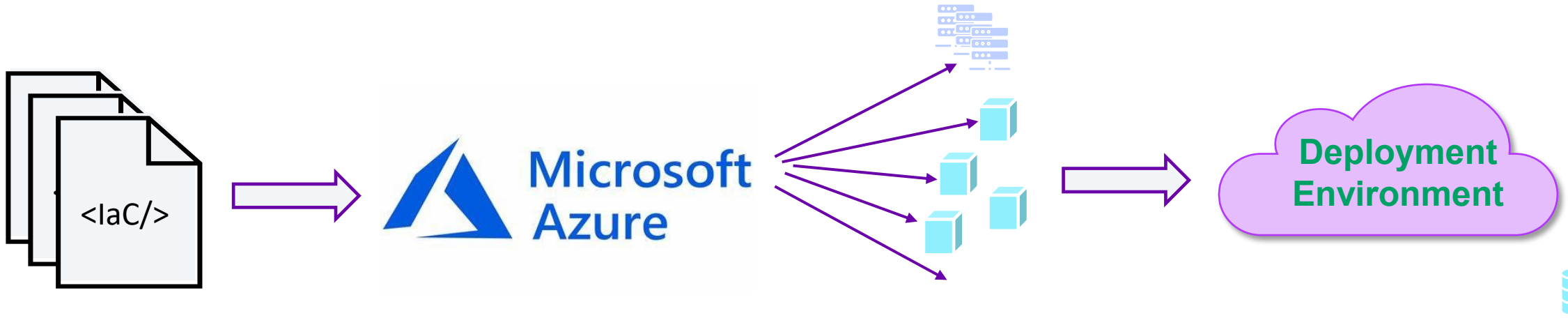


- Advanced analytics (AI/ML)
- Business analytics
- Enterprise applications

- Smarter, more secure data sharing
- Audit trail
- Share management
- Tailor shared data access

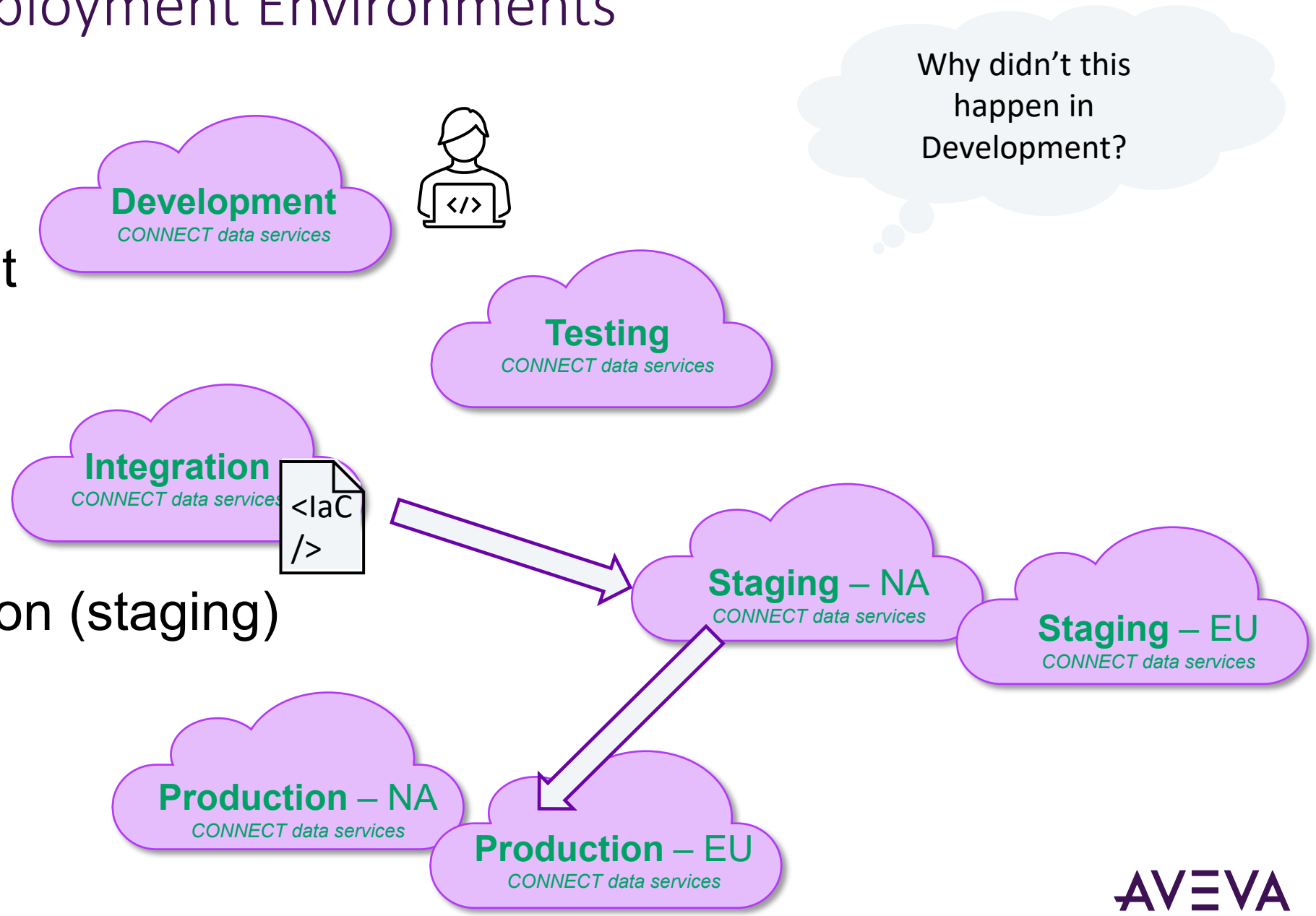
Resilience: Deployment Environment

- Infrastructure as Code
  - Eliminate manual configuration mistakes
- Continuous Updates & Rollback
  - O/S Updates
  - Software patches



Resilience: Deployment Environments

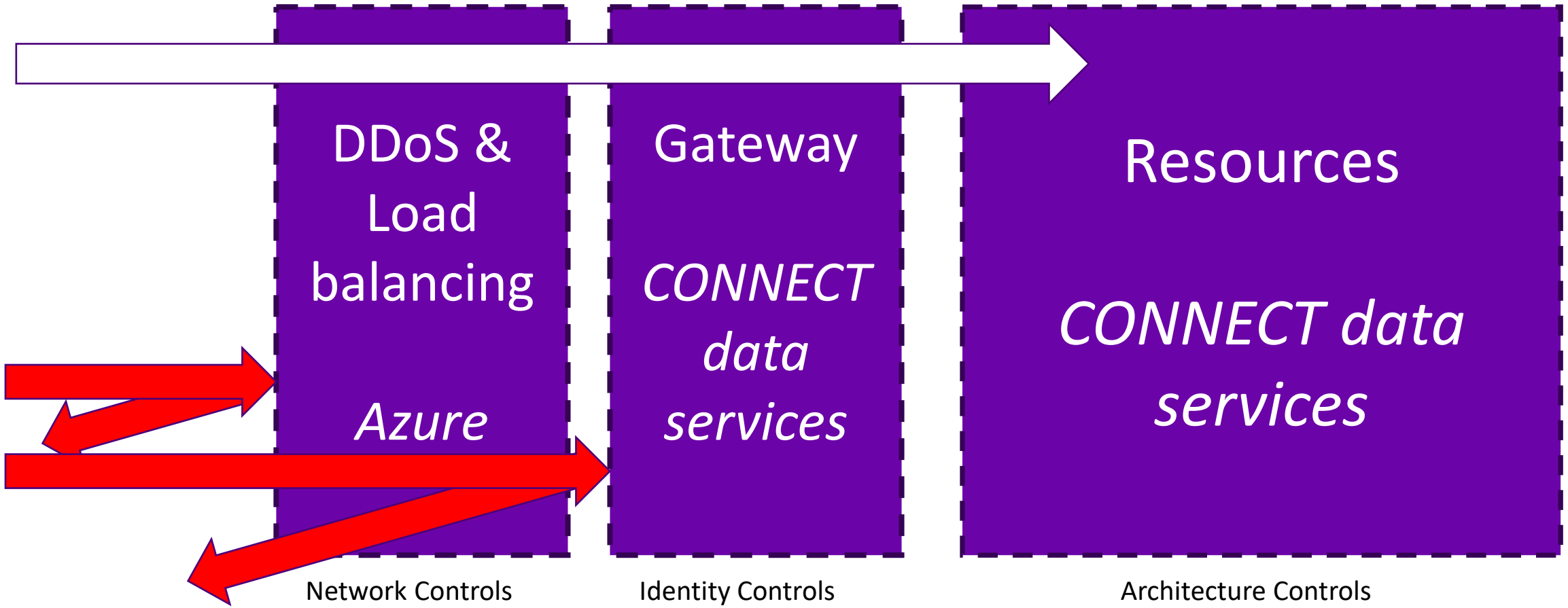
- Development
- Testing
- Integration
- Pre-production (staging)
- Production



Resilience: Is my data available?

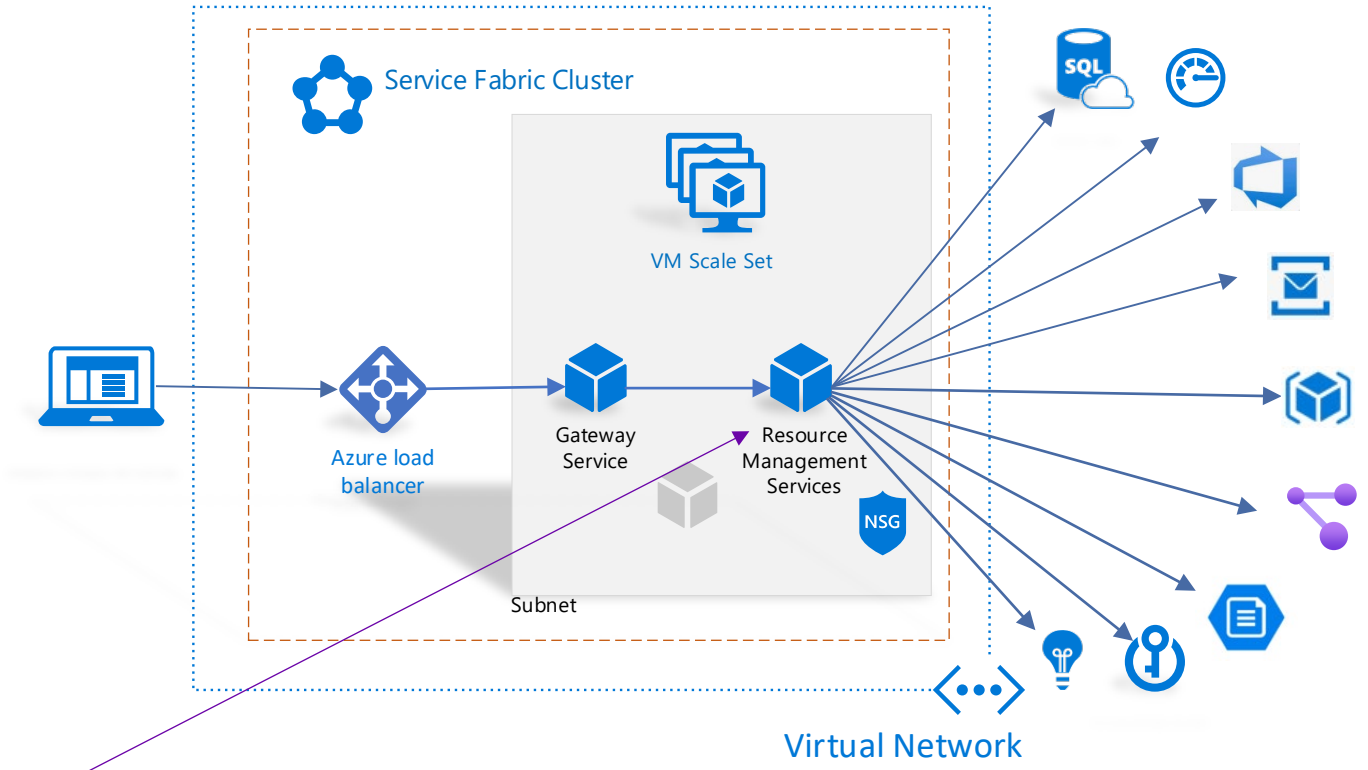
- Distributed Denial of Service protection
- Scalable architecture
  - Increases resources
  - Meets peek demands

Resilience: Layered Defense



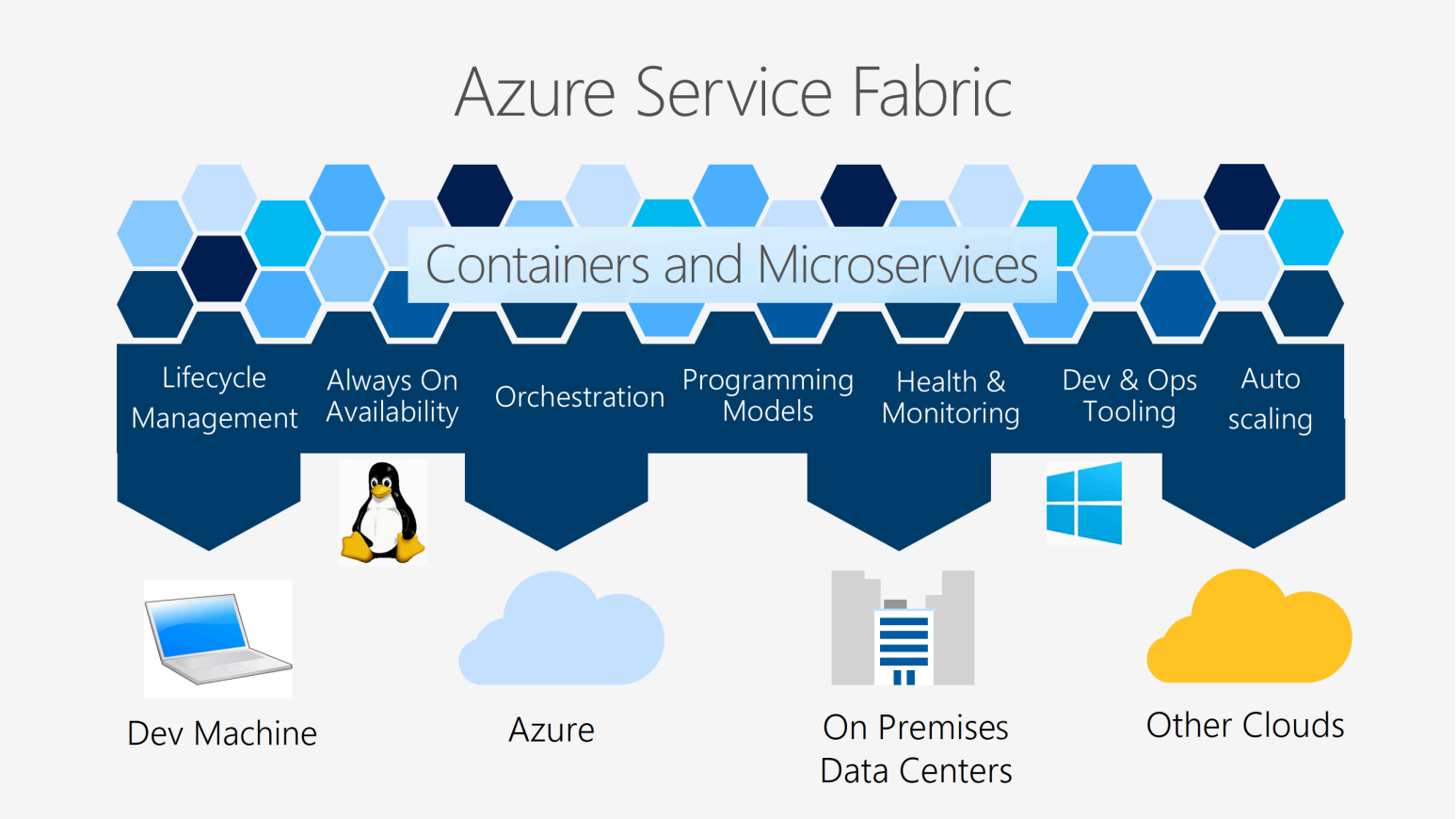
Resiliency of Service

- Governs Scaling
- VM
- Database



Resource Management

Reliance: Orchestration Framework



Is my data safe?

Theft and Tampering

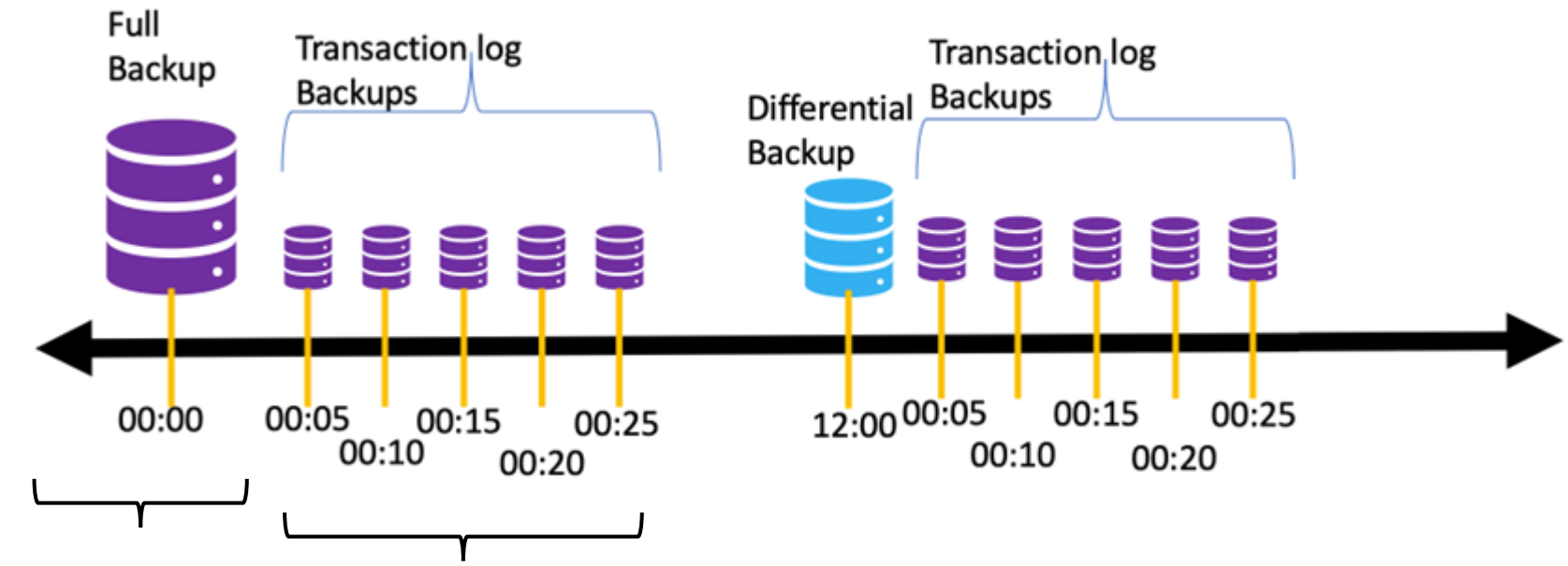
Resiliency of Data

- Control Access
  - Support latest identity standards
  - You control authentication
  - Architect to leverage the evolving identity industry

- Encrypted at rest

Backup: Azure SQL

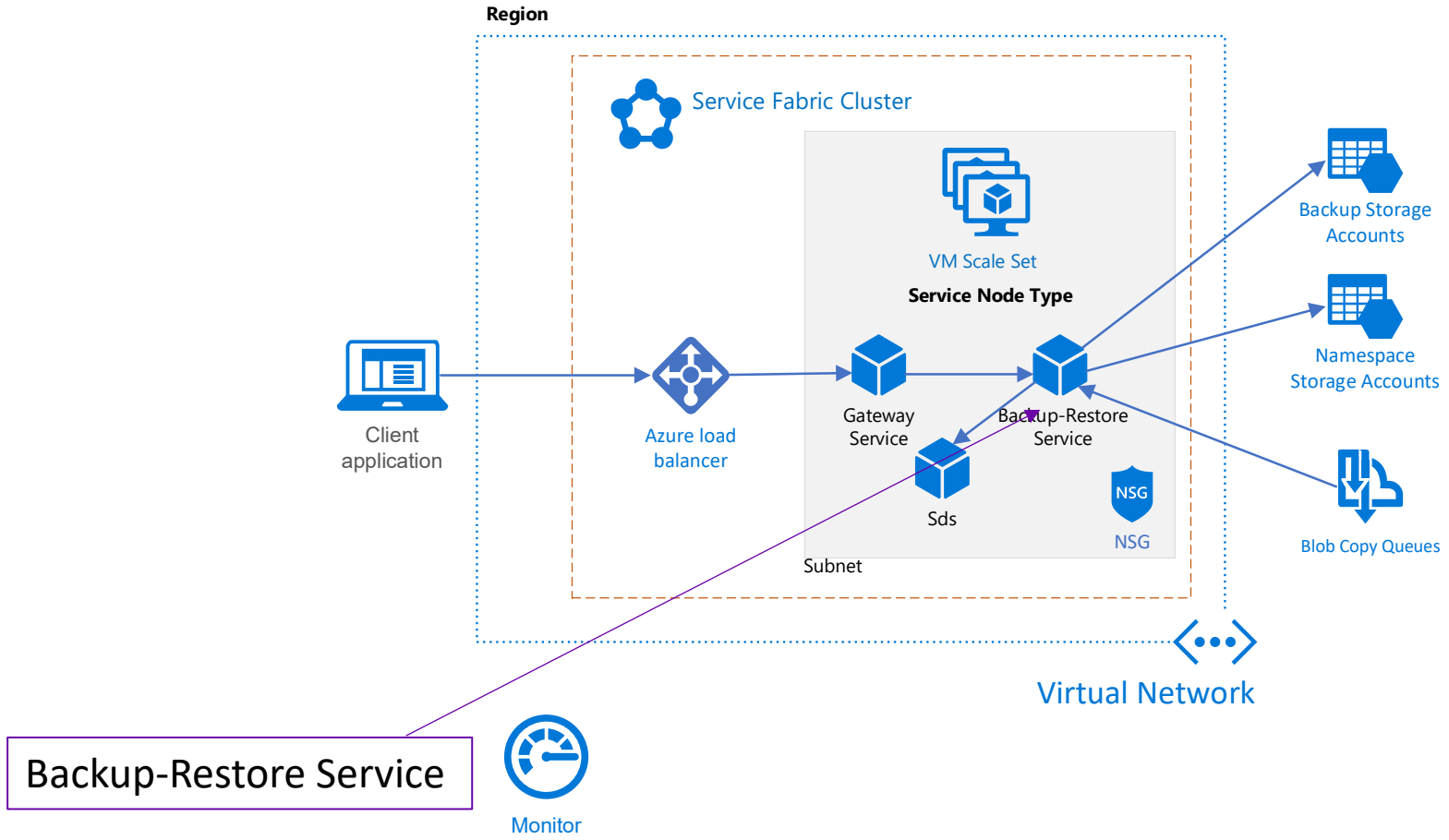
Resiliency of Data



Backup: Sequential Data Store (SDS)

Resiliency of Data

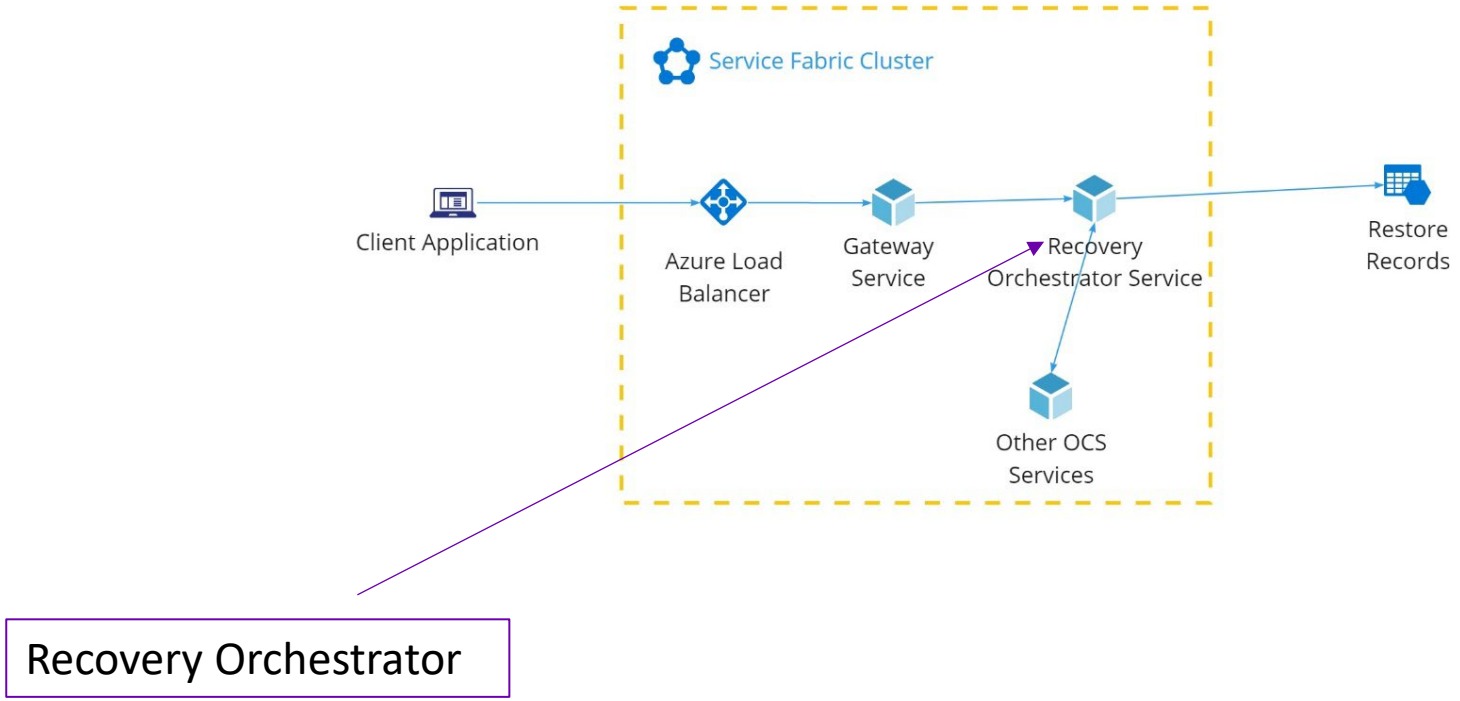
- Backups
  - Weekly
  - Daily
  - Transaction logs



Disaster Recovery

Resiliency of Services

- Orchestrate recoveries across multiple services.
- Augmented with playbooks.



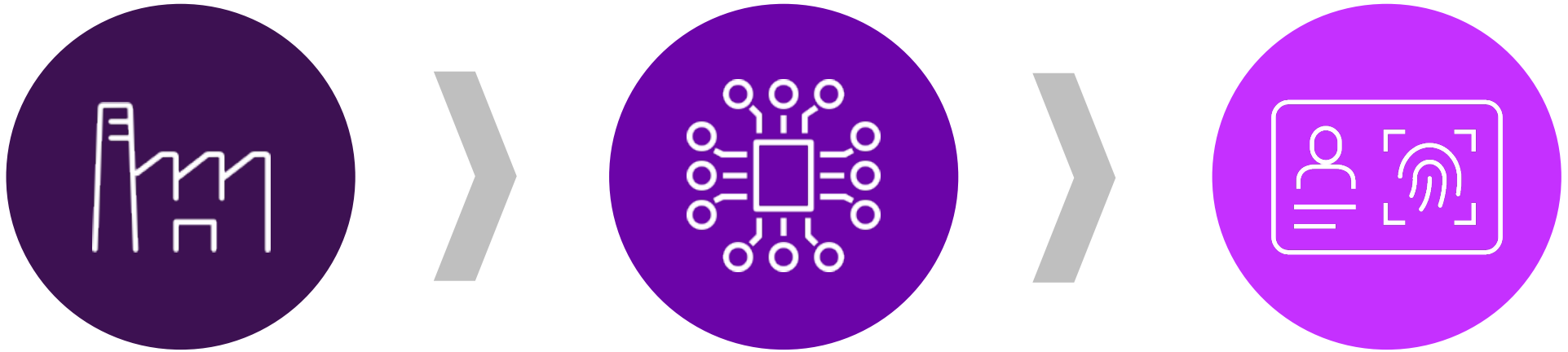
Reliance: Penetration Tests and Assessments

CONNECT data services

- Black Hill: 2019, 2021
- IO Active: 2022
- VERACODE: 2023
- AVEVA Product Security: 2023

Identity

Evolution of Security Perimeters



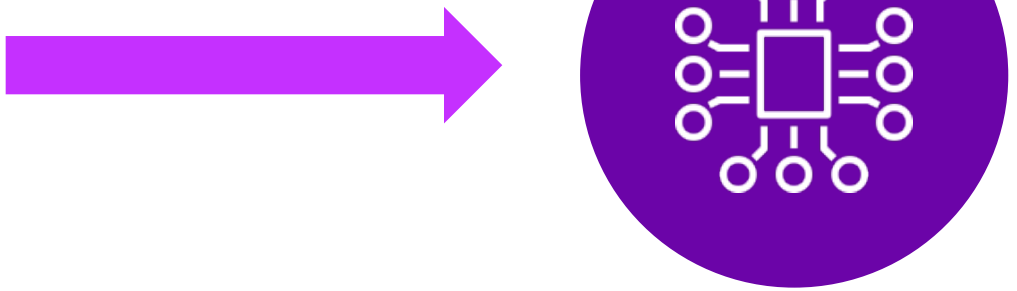
Physical

Network

Identity

Network Perimeter

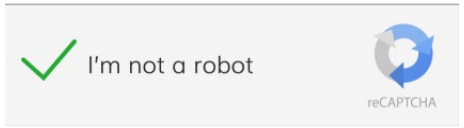
- Phishing
- Credential Theft



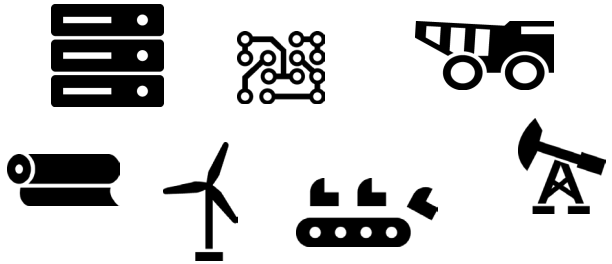
Network

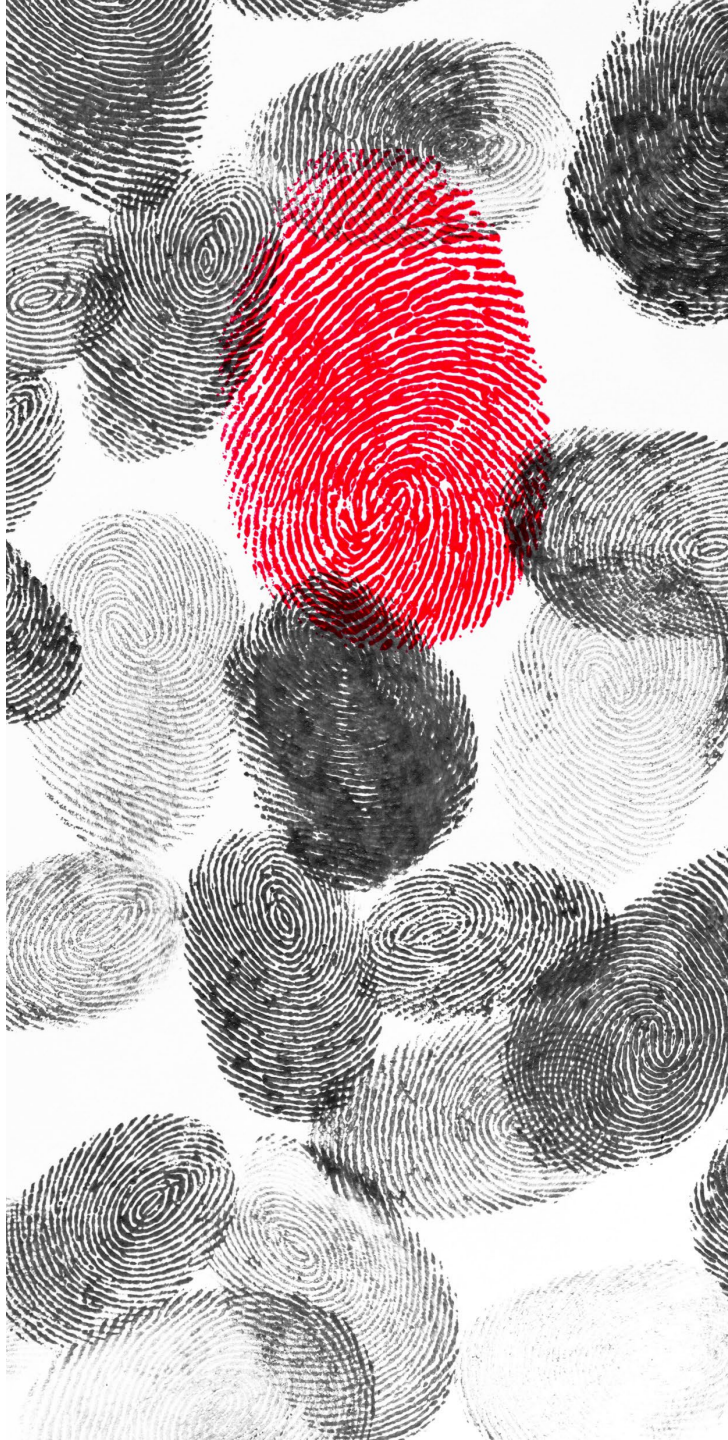
Different Identity types

- Humans – Interactive



- Machines – Silent





Machine Identity

- client ID and secret.

- Theft protections/defenses
  - HTTPS only
  - Credential revocation
  - clientID has limited access
  - No access to your network
  - Secret expiration
  - Secret: 32 byte (256 bit) cryptographically random

AVEVA

Human Identity

Zero Trust

- Trusted devices
- Geolocation fencing
- Multifactor Authentication (MFA)
- Privilege Identity Management (PIM)
  - Just In-Time Authorization (JIT)
  - Second party approval

- Risk-based access verification and challenges
  - Unusual activity
  - Impossible travel
  - Compromised password

Identity

Identity Perimeter

Your journey towards **zero trust architecture** starts with strong proof of identity

STANDARDS (NIST SP 800-207)

Logical Components of Zero Trust Architecture

- Enhanced Identity Governance
- Micro-Segmentation
- Software Defined Perimeters

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Federate AVEVA Connect

Modern Authentication and Transport Layer Security

OpenID Connect (OAuth2)

auth0

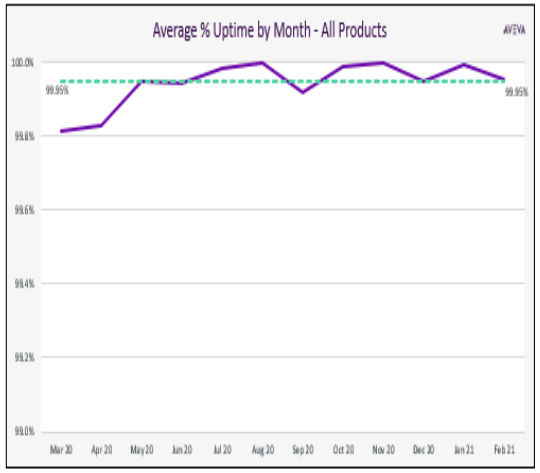
Federated Identity Provider (recommended)

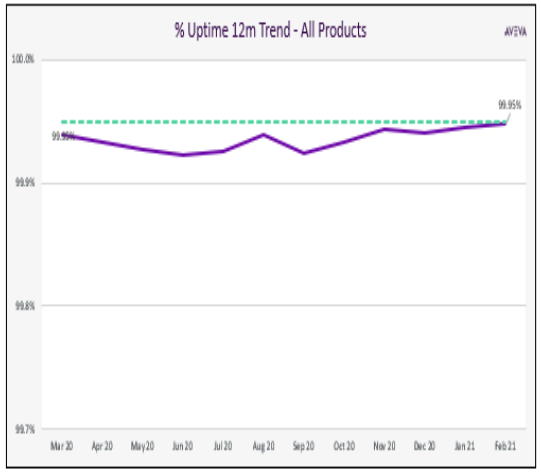
Zero Trust

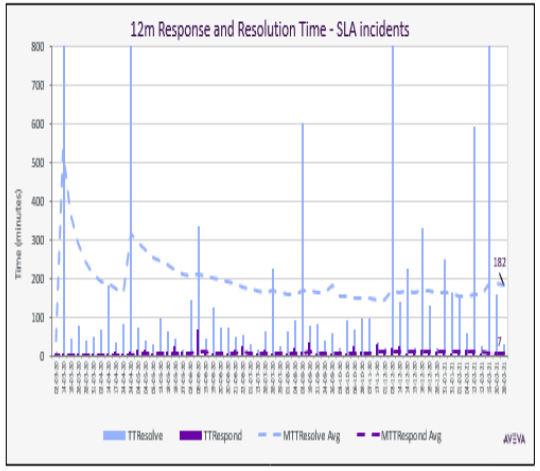
AVEVA

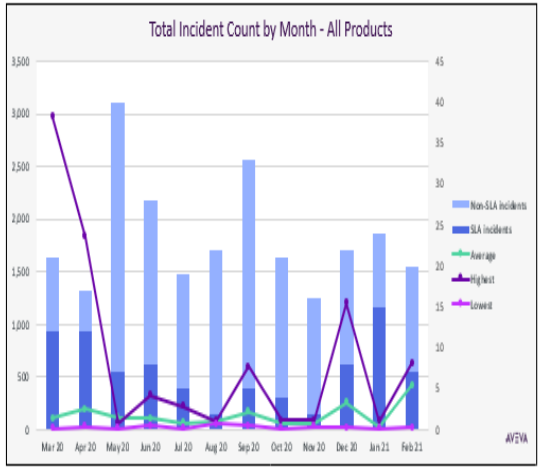
Operational countermeasures

Availability & Operation: Cloud DevOps



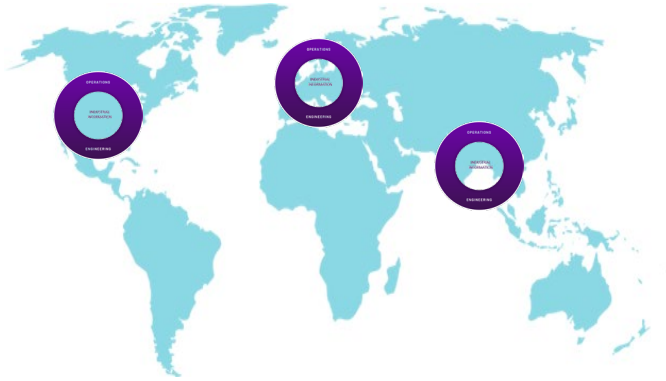






SECURE DEPLOYMENT/ SYSTEM MANAGEMENT

Security Monitoring and Alerting (24x7)



Alliances

Microsoft®

Cisco®

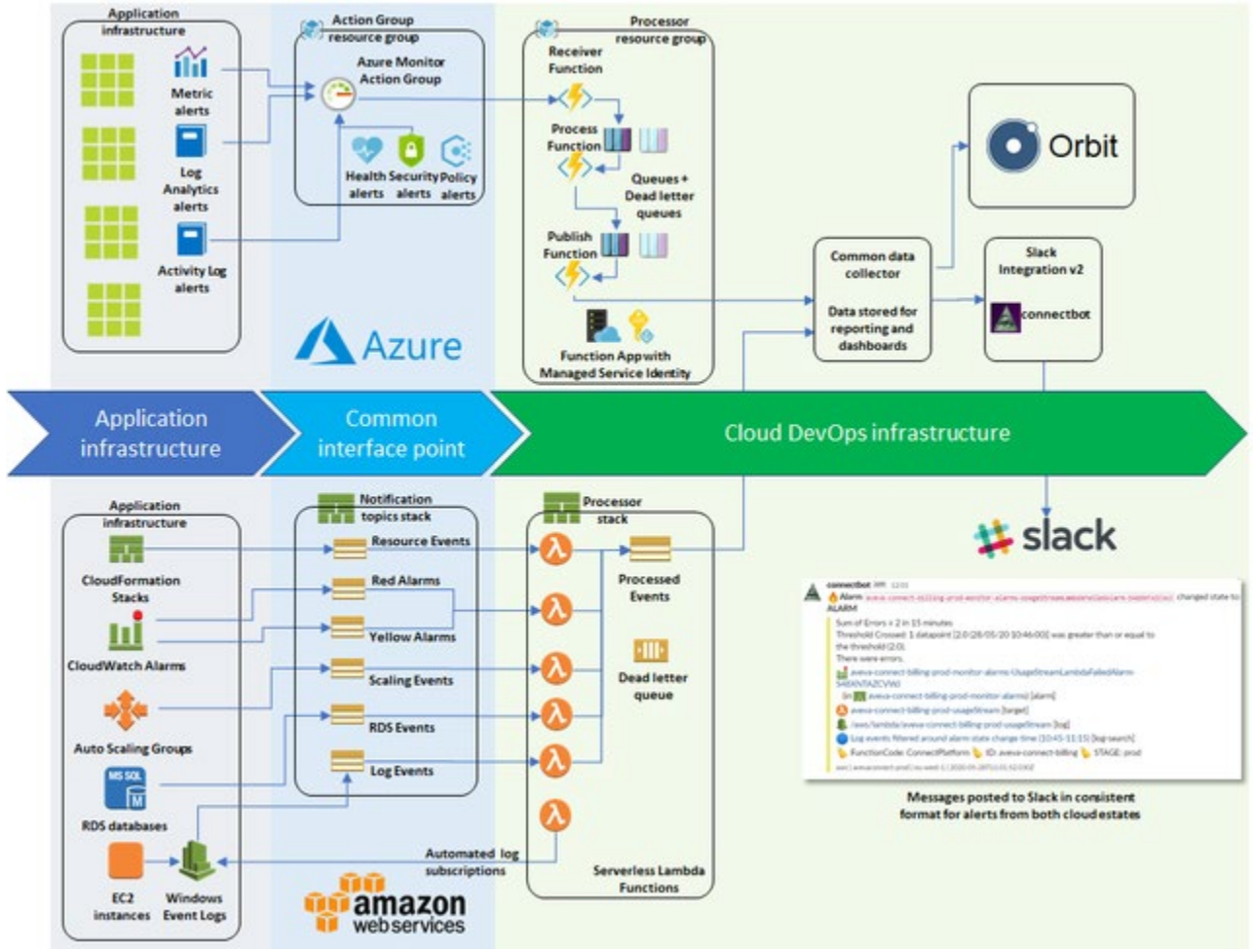
Outpost24®

Cloud Security Alliance®

BitSite®

Detectify®

Monitoring: Cloud DevOps



Monitoring: Cloud DevOps

Microsoft Azure Tools

- Microsoft Defender for Cloud for Hosted Services
  - Recommendations vs. Alerts
- Azure Policy Compliance
  - Azure and AVEVA policies
- Azure Monitor Agent
  - Security event logs -> Sentinel
- Microsoft Defender for Endpoint
- Azure Resource Graph
  - O/S Patch updates

Response: Global Security Operations

24/7 Monitoring

Dedicated team ensures constant vigilance, swiftly identifying and responding to potential threats. Safeguard operations around the clock, providing peace of mind in an ever-evolving digital landscape.

Detection Engineering

Detection engineering integrates advanced methodologies with SIEM, SOAR, UEBA, and security controls to enhance proactive threat detection and streamline incident response

Delivery Services

Delivery Services manage projects from start to finish, ensuring alignment with goals and stakeholder engagement.

Vulnerability Management

Systematic identification, assessment, and prioritization of vulnerabilities, offering tailor-made solutions to reinforce digital defenses.

Threat Intelligence & Hunting

Anticipate and neutralize threats ahead of time, leveraging advanced insights to safeguard digital landscape. Vigilant approach that surpasses mere detection, ensuring resilient against evolving cyber threats.

Red Team

Proactive and Reactive Red Team initiative is at the forefront of offensive security assessments, diligently identifying and countering potential threats to fortify the security posture.

Digital Forensic & Incident Response

Leverages state-of-the-art methodologies, offering meticulous analysis and investigation to uncover critical insights.

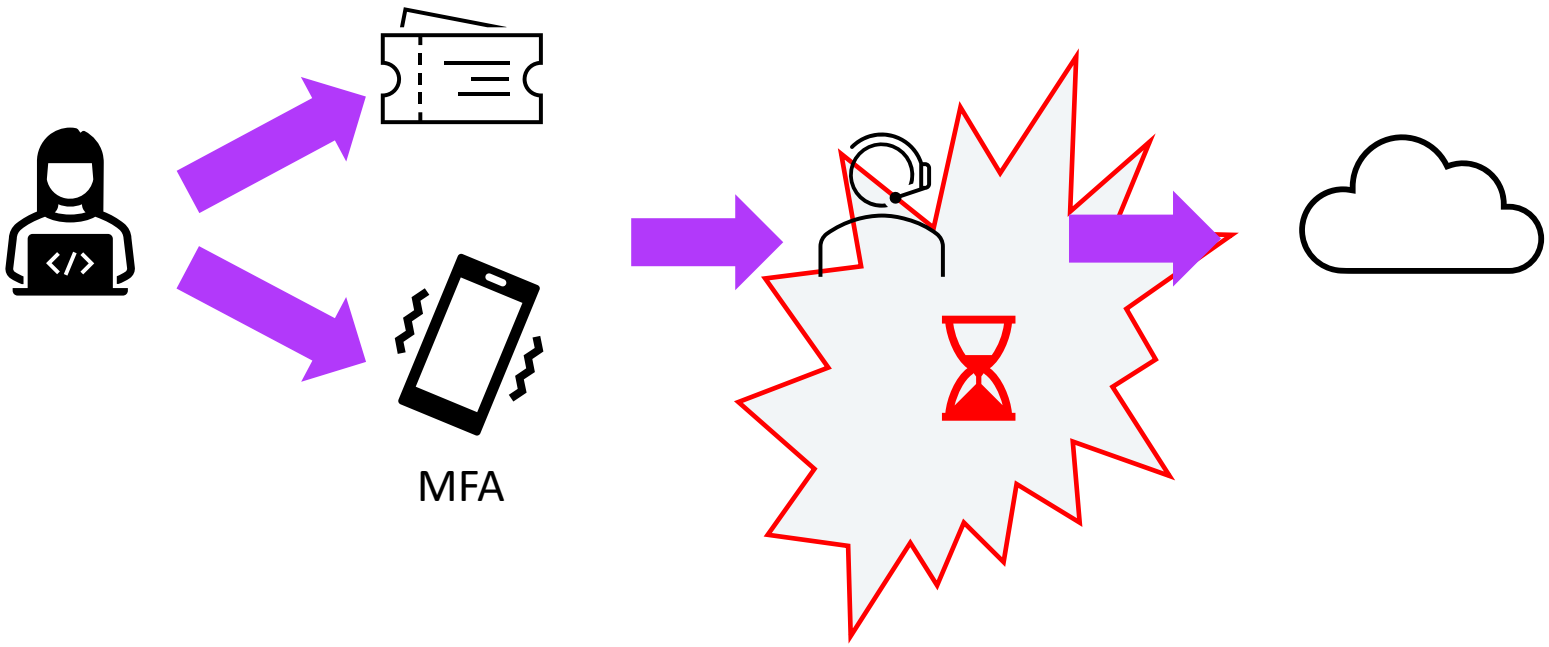
Security Incident Management

Swiftly and effectively manage cyber threats, ensures a rapid and strategic response, minimizing impact and restoring security with precision.

AVEVA

Response: Access to Production

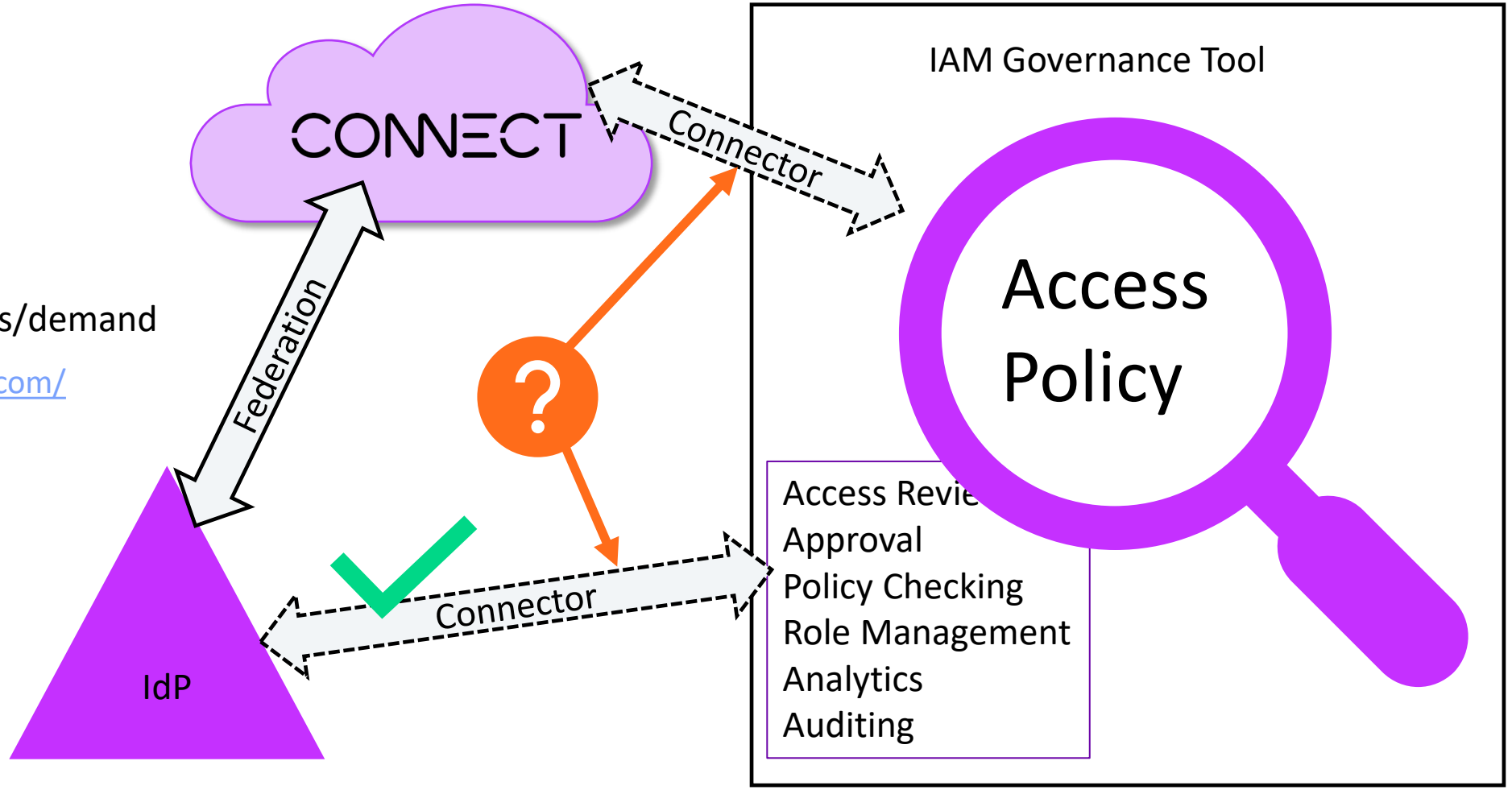
Privileged Identity Management (PIM)



Future

Future: Identity Access Management (IAM) Governance

- Audit options
  - Identity Provider
  - Resource
- Identify customer needs/demand
  - https://feedback.aveva.com/
  - Regulations you face?



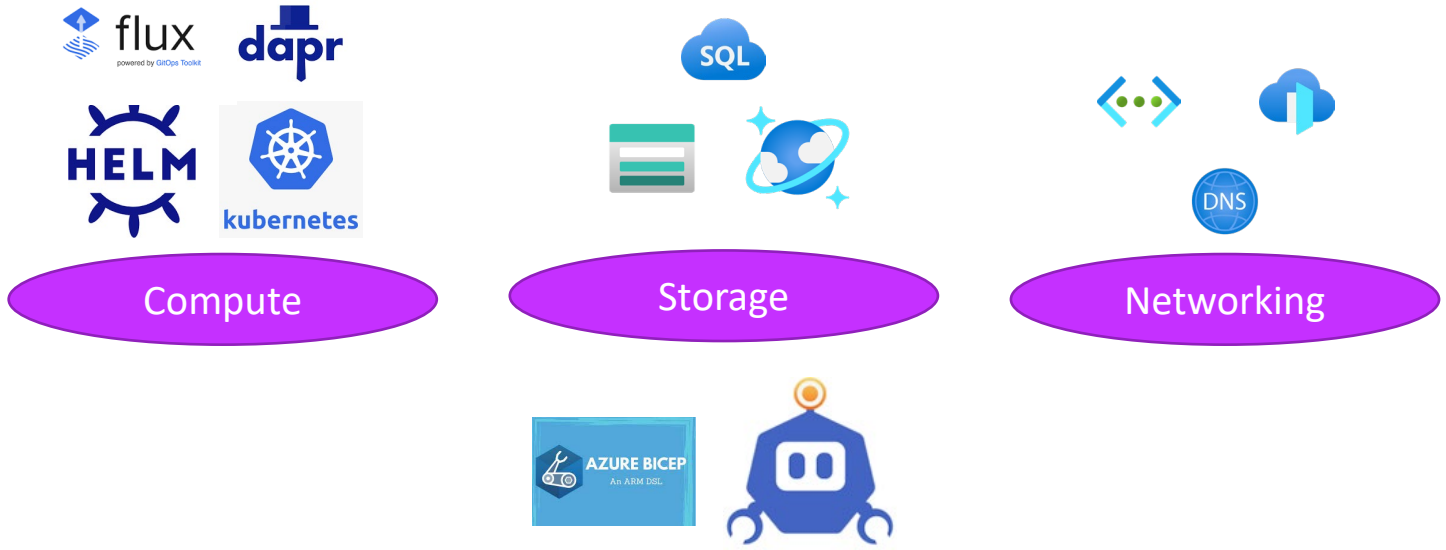
Future: Software Bill of Materials

Ingredients of your software

- Software Bill of Materials (SBOM)
  - CycloneDX
  - Vulnerability Exchange (VEX)
- Regulation
  - EU Cyber Resilience Act
  - EU Network and Information Security (NIS2)
  - CISA Software Transparency in SaaS Environments
  - US Executive Order 14028 on Improving the Nation’s Cybersecurity

Future: CONNECT v2

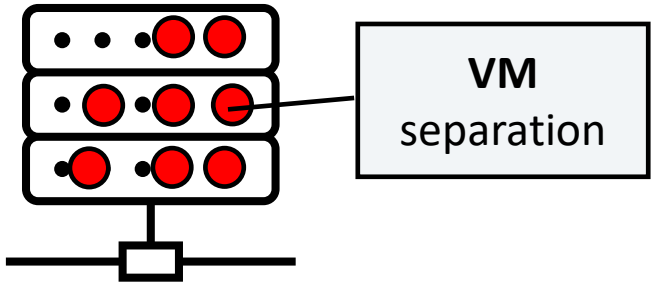
- Service to service mTLS
- Improved secrets management
- Faster deployment
- Secure by default services
- Data residency improvements



Subscription vs. Tenancy Isolation

Subscription Isolation

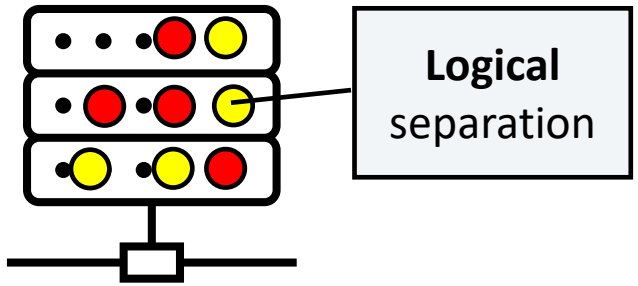
- Hypervisor isolation



- What problem trying to solve?
  - Regulations?
  - Company policy?

Tenancy Isolation

- Cost Management
  - Shared “backbone” resource costs
  - Shared operations costs
- Performance



Tenant 1

Tenant 2

AVEVA

Conclusion

Visit us at the CONNECT Booth

- Federate IdP to CONNECT
  - Identity is the new perimeter
  - Federate with OIDC – for your company’s zero-trust strategy
  - SAML is dead
- Regulations/Policies
- Security tool integrations
- Something else?

Questions?

Mike Lemley

Product Security Chief Architect

THINK SECURE

AVEVA

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a world leader in industrial software, providing engineering and operational solutions across multiple industries, including oil and gas, chemical, pharmaceutical, power and utilities, marine, renewables, and food and beverage. Our agnostic and open architecture helps organizations design, build, operate, maintain and optimize the complete lifecycle of complex industrial assets, from production plants and offshore platforms to manufactured consumer goods.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. The company is headquartered in Cambridge, UK.

Learn more at www.aveva.com