

NOVEMBER 2022

Four imperatives of a trusted information infrastructure

Mike Lemley

AVEVA

The reality of convergence. Industrial Information Platform.



AVEVA Connect, industrial cloud platform.

Platform Imperatives



GOVERN
Ability to
Align to IT
Security Policy



TRUSTED
Secure
Practices



MANAGED
Information
Platform
Management



HYBRID
Secure Industrial
Solution
Architecture

SUBSCRIBE.

AVEVA Flex

Flexible access to
AVEVA's full portfolio,
whether on the cloud
or on-premises.

One common
subscription program

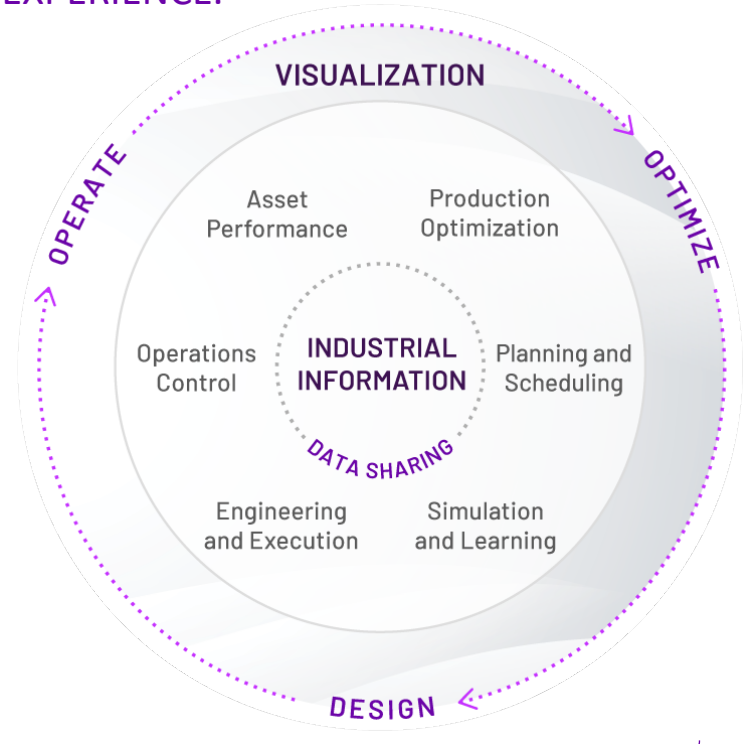
CONSUME.

AVEVA Connect

Cloud platform to
transform faster,
reduce IT cost, and
collaborate securely
across our portfolio.

One industrial
cloud platform

EXPERIENCE.



Full access across one comprehensive
set of portfolio capabilities

AVEVA

Govern Imperative



GOVERN

Ability to Align to
IT Security Policy



TRUSTED

Secure Practices



MANAGED

Information
Platform
Management



HYBRID

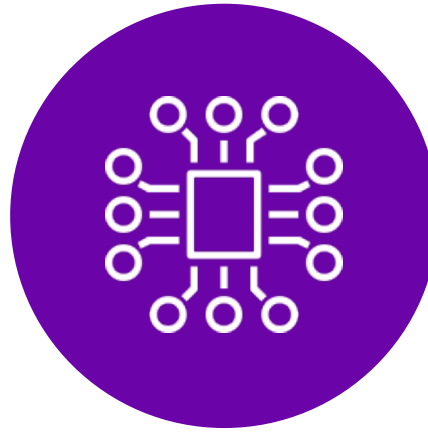
Secure Industrial
Solution
Architecture

- Federate to your Identity
- Use your groups to roles/permissions
- Apply corporate security policies
- Software asset compliance management

Evolution of Security Perimeters



Physical



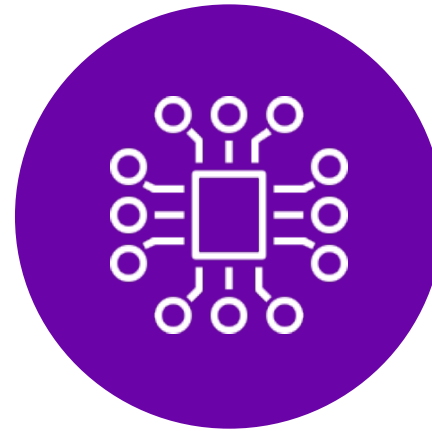
Network



Identity

Network Perimeter

- Phishing
- Credential Theft



Network

Identity Perimeter & Modern 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)

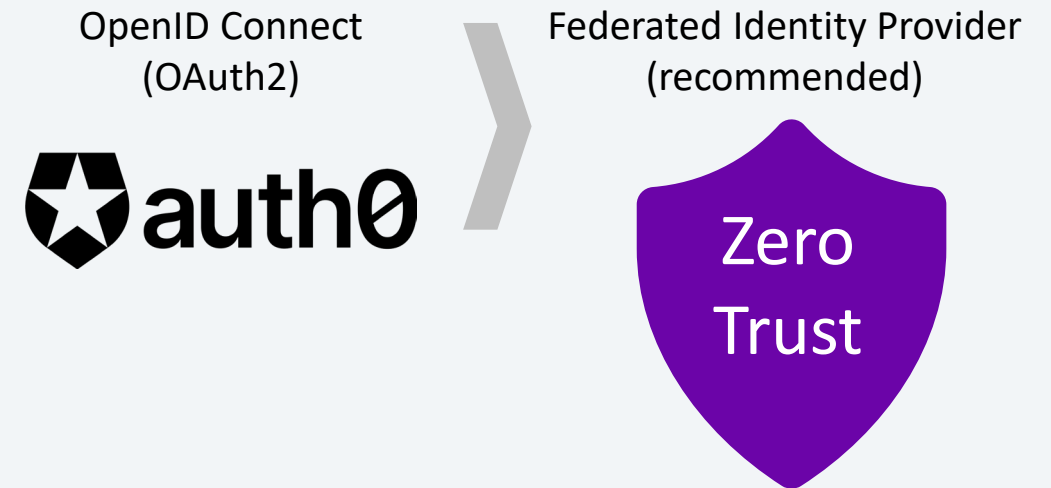
Logical Components of Zero Trust Architecture

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

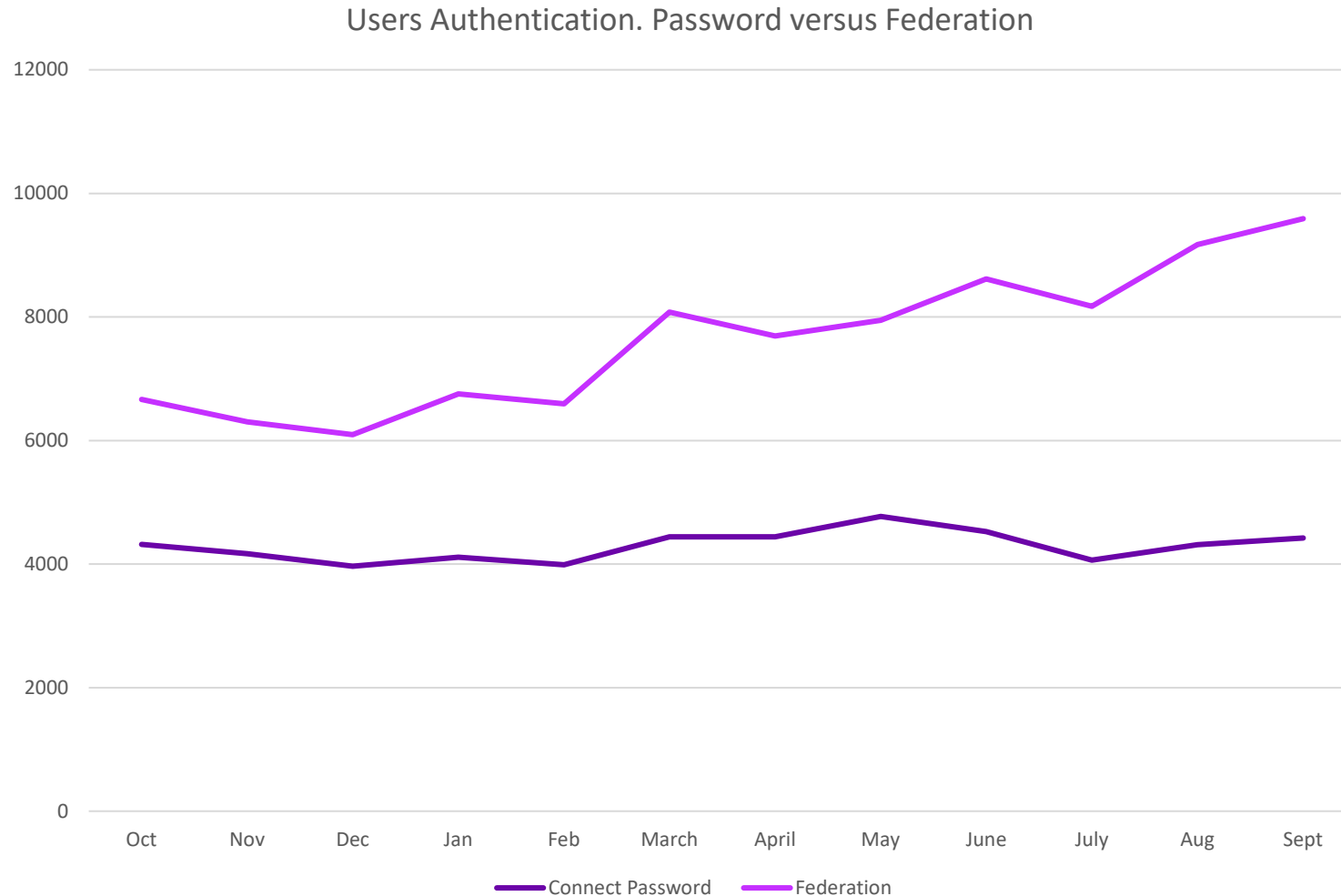


Federate AVEVA Connect

Modern Authentication and Transport Layer Security



AVEVA Connect platform becoming Trusted



AVEVA Connect adoption

- 15,000 monthly active users
- Over 6,000 accounts
- Averaging 100,000+ logins per week

Federating to your company identity provider

- Ability to manage users as part of corporate
- IT Security Policies on users is aligned
- Corporate User Groups are associated with AVEVA Connect Roles/ Permissions

Trusted authentication

- AVEVA Connect IdP can delegate authentication to Identity Providers that support SAML 2, OpenID Connect, ADFS or Azure AD

Software asset management compliance approach

TRACK

UNDERSTAND

MANAGE

Global Empowerment

- Global access and management of AVEVA Software
- Unified Managed across sites, and on premise and SAAS services



One Entitlement

Unit of Measure = AVEVA™ Flex Credits

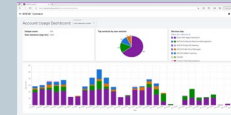
- All offers for a customer are entitled through AVEVA Flex Credits
- Credit consumption is reported as one

Unified Tracking of all AVEVA Software & Services

- On-prem disconnected offers
- On-prem “Connected” offers
- Online services

Usage Intelligence

- Self-service usage dashboards
- Understand adoption usage by service
- Ability export usage data for external manipulation



Credit Consumption

- Self-service credit consumption dashboards
- Ability export usage data for external manipulation



Budgets

- Ability to set up monthly usage budgets
- Notifications if usage patterns are exceeded
- Ability understand actual vs targeted usage

Service/ Software Management

- Cloud service availability thru Auth Officer
- Ability to define multiple credit agreements for local management
- Audit Logs

Trusted Imperative



GOVERN
Ability to Align to
IT Security Policy



TRUSTED
Secure Practices



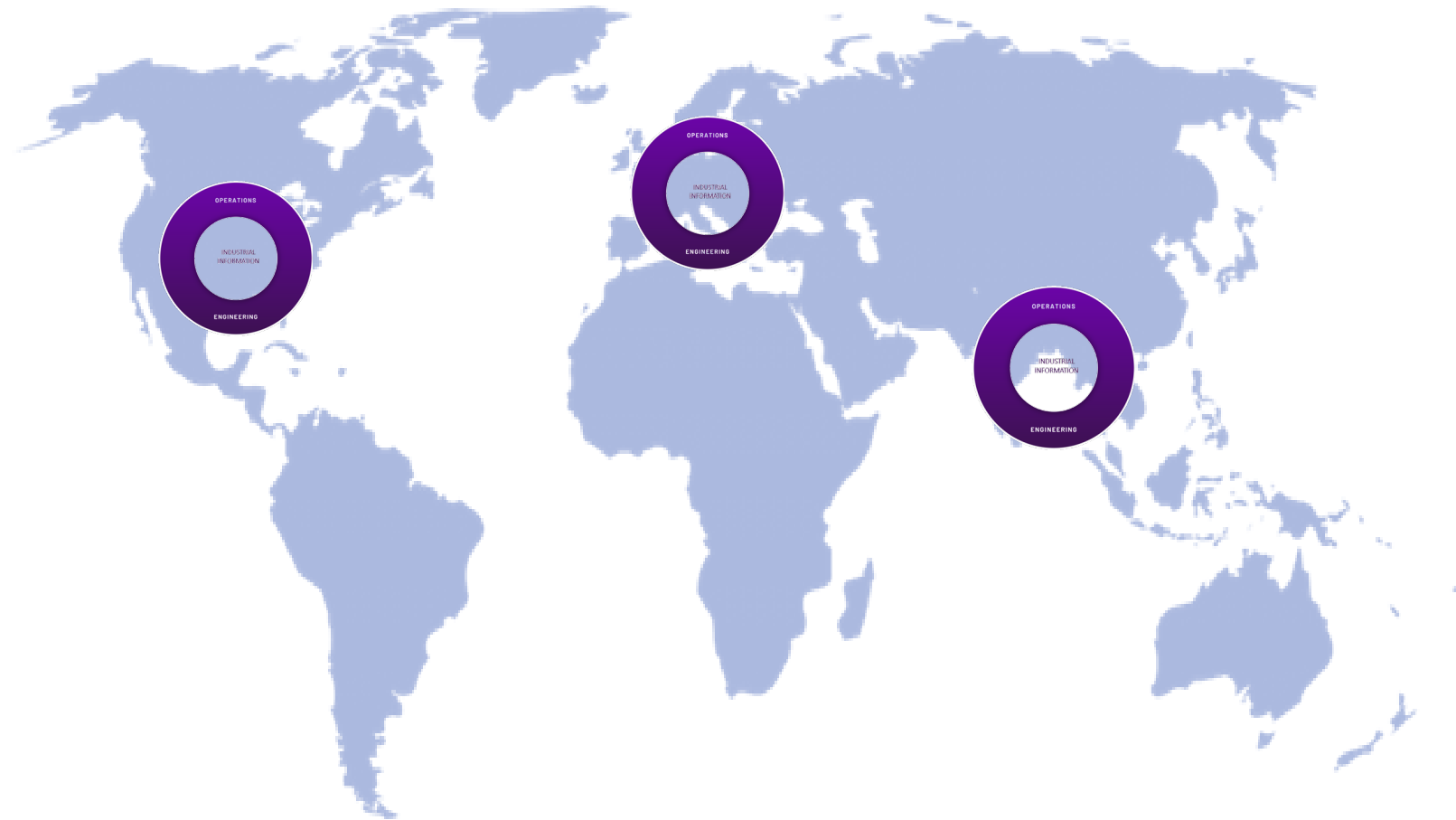
MANAGED
Information
Platform
Management



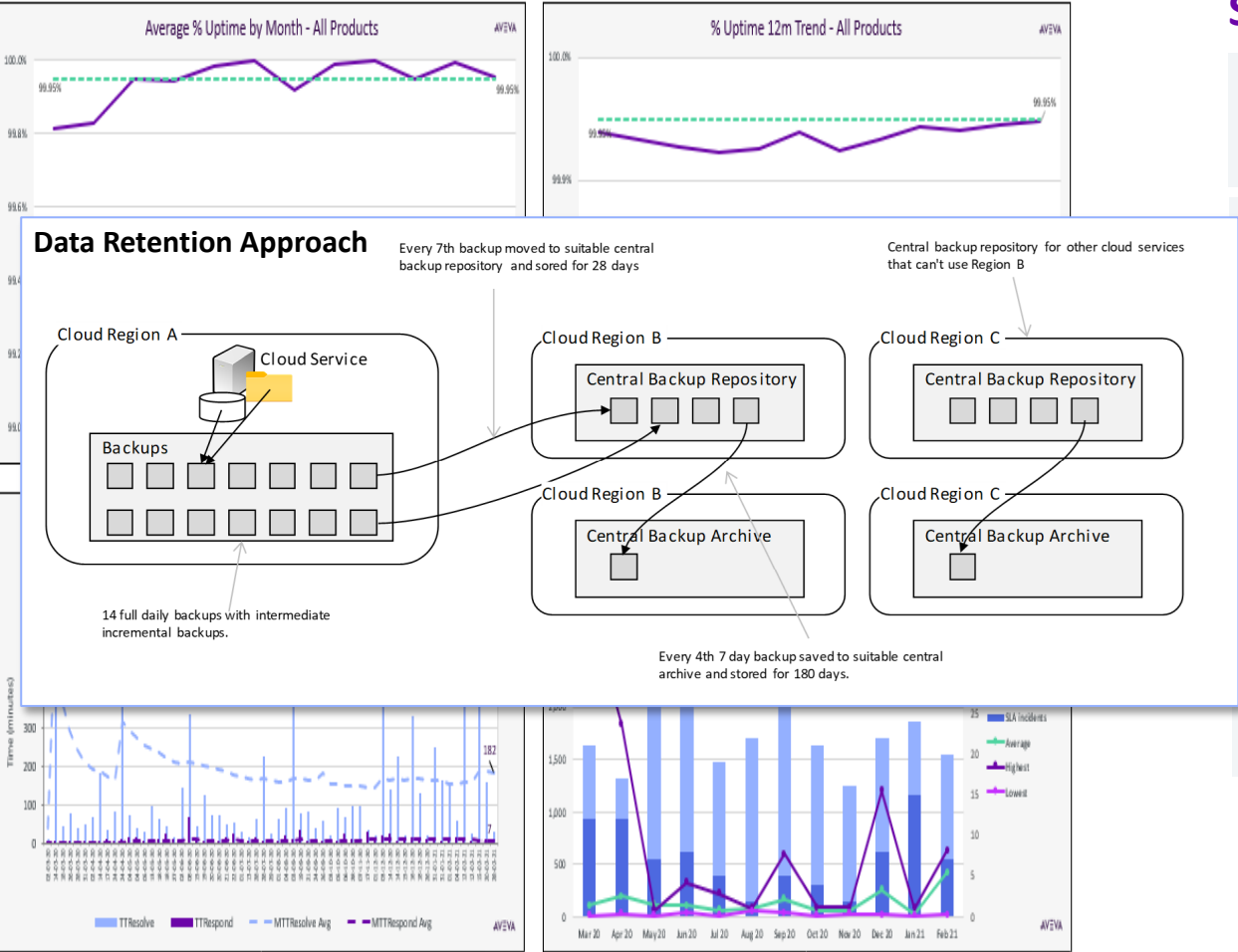
HYBRID
Secure Industrial
Solution
Architecture

- Availability
- Trusted cloud platform
- Certified processes
- Engage industry experts

Availability & Operation



Availability & Operation



SECURE DEPLOYMENT/ SYSTEM MANAGEMENT

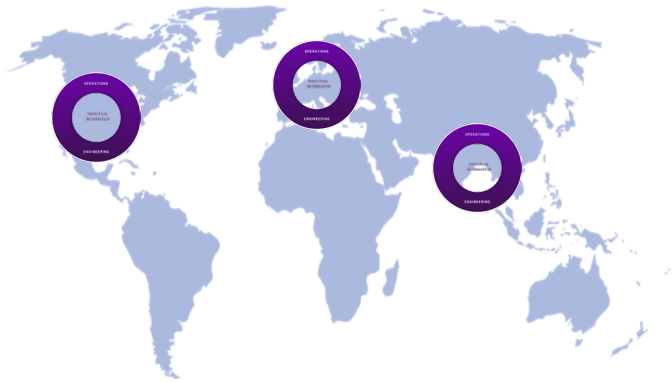
Security Policies

Security Monitoring and Alerting (24x7)

Network and Domain Monitoring

Security Logging & Tracing

Data Retention



Alliances

Microsoft®

Cisco®

Outpost24®

Splunk®

Cloud Security Alliance®

Ensuring cloud security

Security Development Practices

Certifications

ISASecure SDL
ISO 9001
SOC-2
ISO 27001

Industry Bodies

Cloud Security Alliance
Center for Internet
Security

Training

Static Code Analysis
Secure Code Review

Security
Requirements and
Risk Assessment

Verification Testing

Threat Modeling in
Architecture

Security Review
Release Gate

Security Design
Requirements

ISO 30111 for
Incident Response

Products built with security focus

- Keep our customers secure
- Manage supply chain risk
- Provide actionable information about issues (CERT)

Compliance for our process

- Certified ISASecure SDLA processes
- Certified development environment
- Certified Quality Management System (QMS)

Evolve - Increase security awareness

- Collaboration with industry stakeholders
- Ensure Security Requirements are defined
- Build Security into Architectures

Industry Experts

Conforms to international standards and is **strongly verified**.

Standards and Verification



LRQA
Current issue date: 3 December 2021
Expiry date: 2 December 2024
Certificate identity number: 10410912
Original approval(s): ISO/IEC 27001 - 3 December 2021

Certificate of Approval

This is to certify that the Management System of:
AVEVA Solutions Ltd
High Cross, Madingley Road, Cambridge, CB3 0ET

has been approved by LRQA to the following:
ISO/IEC 27001:2013

Approval number(s): ISO/IEC 27001 - 0003

This certificate is valid only in association with this approval as listed.

The scope of this approval is applicable to:
The provision of Information Security Management Research and Development Centres. The scope includes hosting services in the AVEVA Cloud. Stateside.

David Derrick
David Derrick
Area Operations Manager UK & Ireland
Issued by: Lloyd's Register Quality Assurance Ltd

LRQA Group Limited, its offices and subsidiaries and their UKRA members are independent and shall not be liable to the manufacturer provided, unless that person has agreed a separate liability in accordance with the terms and conditions set out in the issued by Lloyd's Register Quality Assurance Limited, 1 The Quadrant, London EC4A 3DF, UK.



The manufacturer may use the mark:



ISASecure® is a Trademark of ASCI. All rights reserved.
Revision 1.0 Oct. 22, 2019
The certificate is valid until the expiration date of October 1, 2022.

Reports:
AVE 1905010 R001 V1R1
Certification Report

Validity:
This Certificate is restricted to the specified versions of the referenced Security Development Lifecycle set forth in this Certificate.

ISASecure® Chartered Laboratory:
exida
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531



ISO/IEC 17065
PRODUCT CERTIFICATION BODY
81004
T-136, V1R3

**Certificate / Certificat
Zertifikat / 合格証**

AVE 1905010 C001

exida hereby confirms that the process entitled:
Security Development Lifecycle Process
Which is maintained and practiced by
**AVEVA
Lake Forest, CA
USA**

Has been assessed per the relevant requirements of:
**ISASecure® Security Development Lifecycle Assurance (SDLA) Program
Version 2.0.0**

ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements
IEC 62443-4-1:2018 Secure product development lifecycle requirements

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

This certification applies to versions 2.3 or later of "Security Development Lifecycle Process"



William M. H.
Authorized Representative



Strategic Software Security Suppliers

VERACODE

IOActive



SYNOPSYS



Azure DevOps



Checkmarx

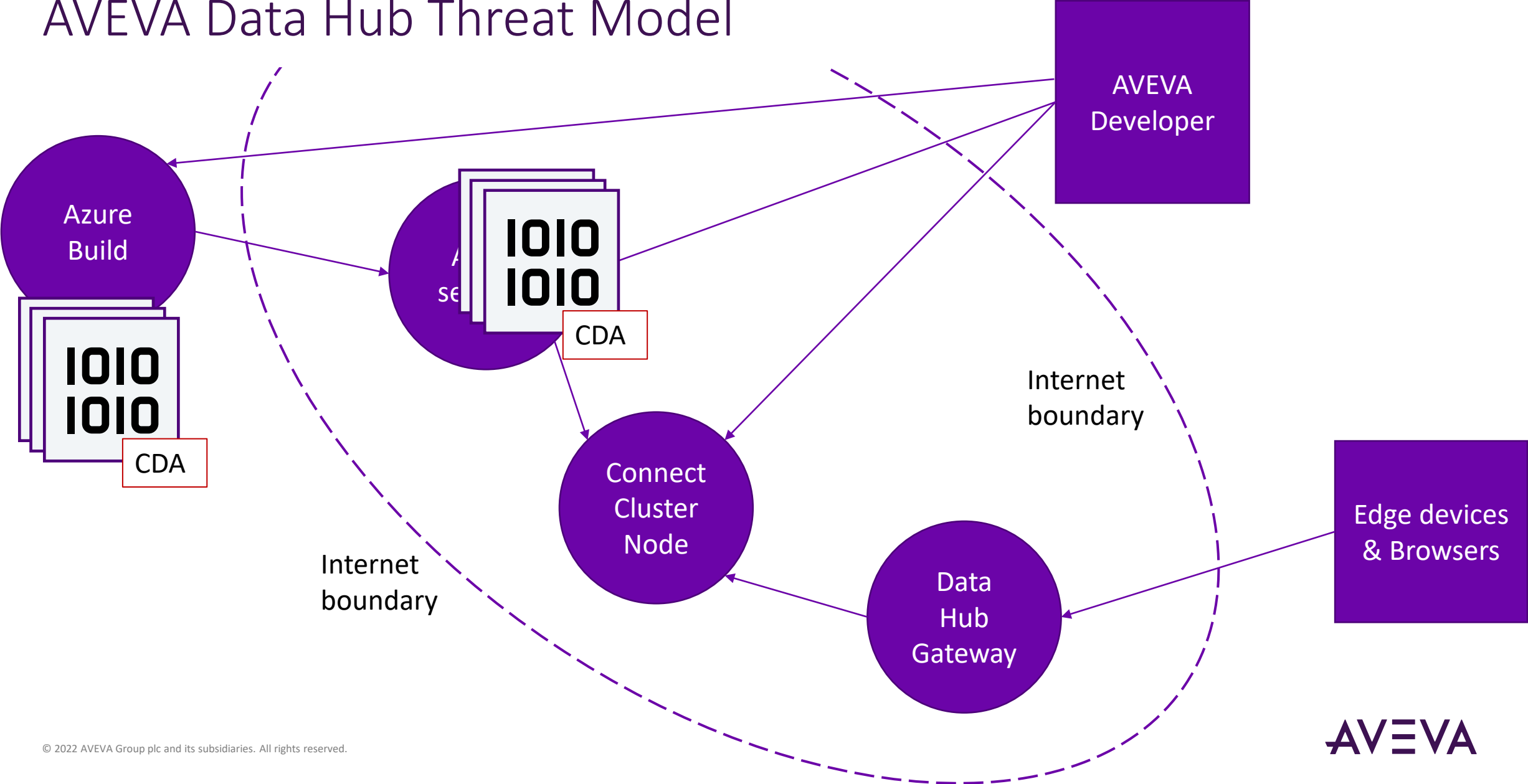


MEND

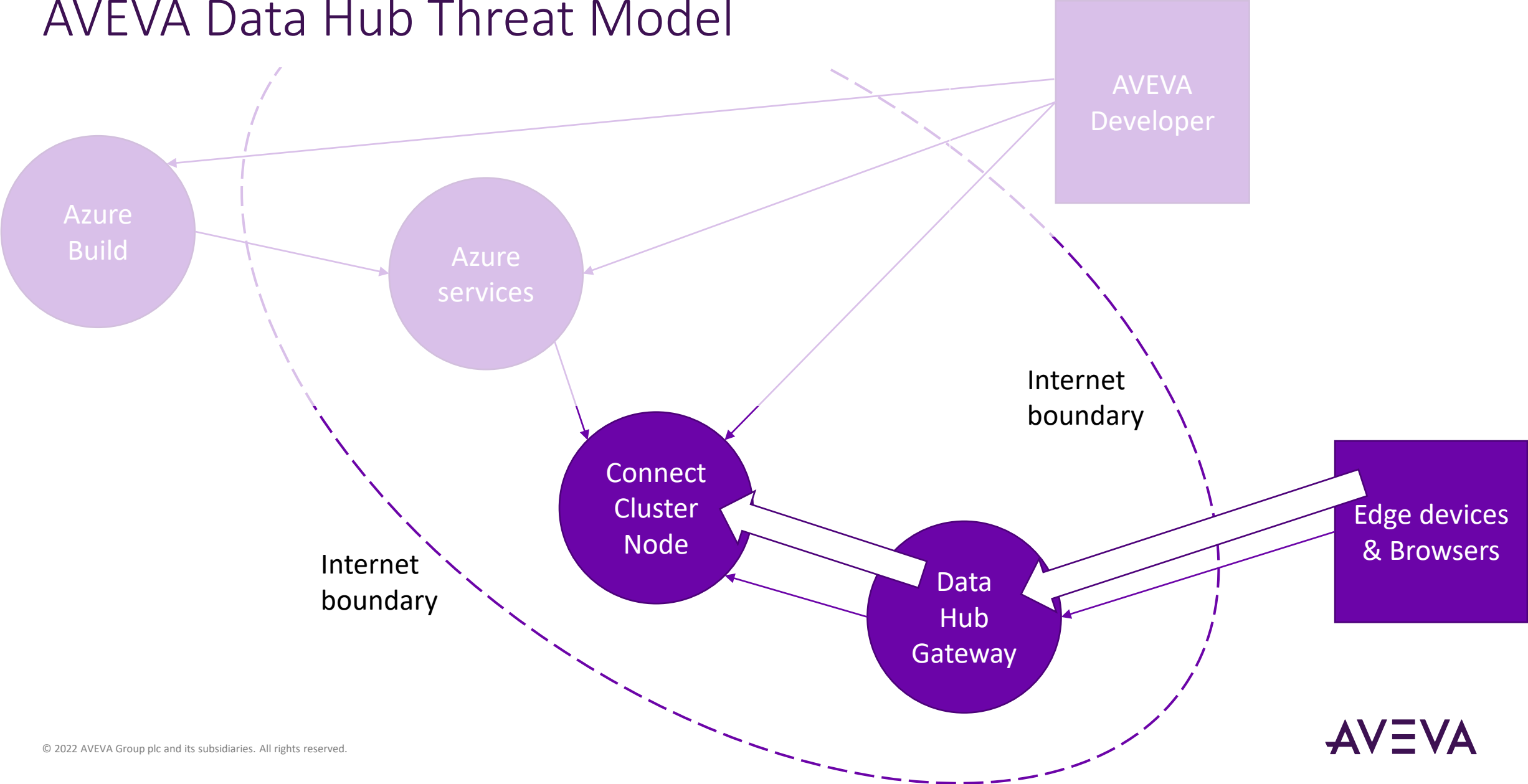
RAPID7

AVEVA

AVEVA Data Hub Threat Model



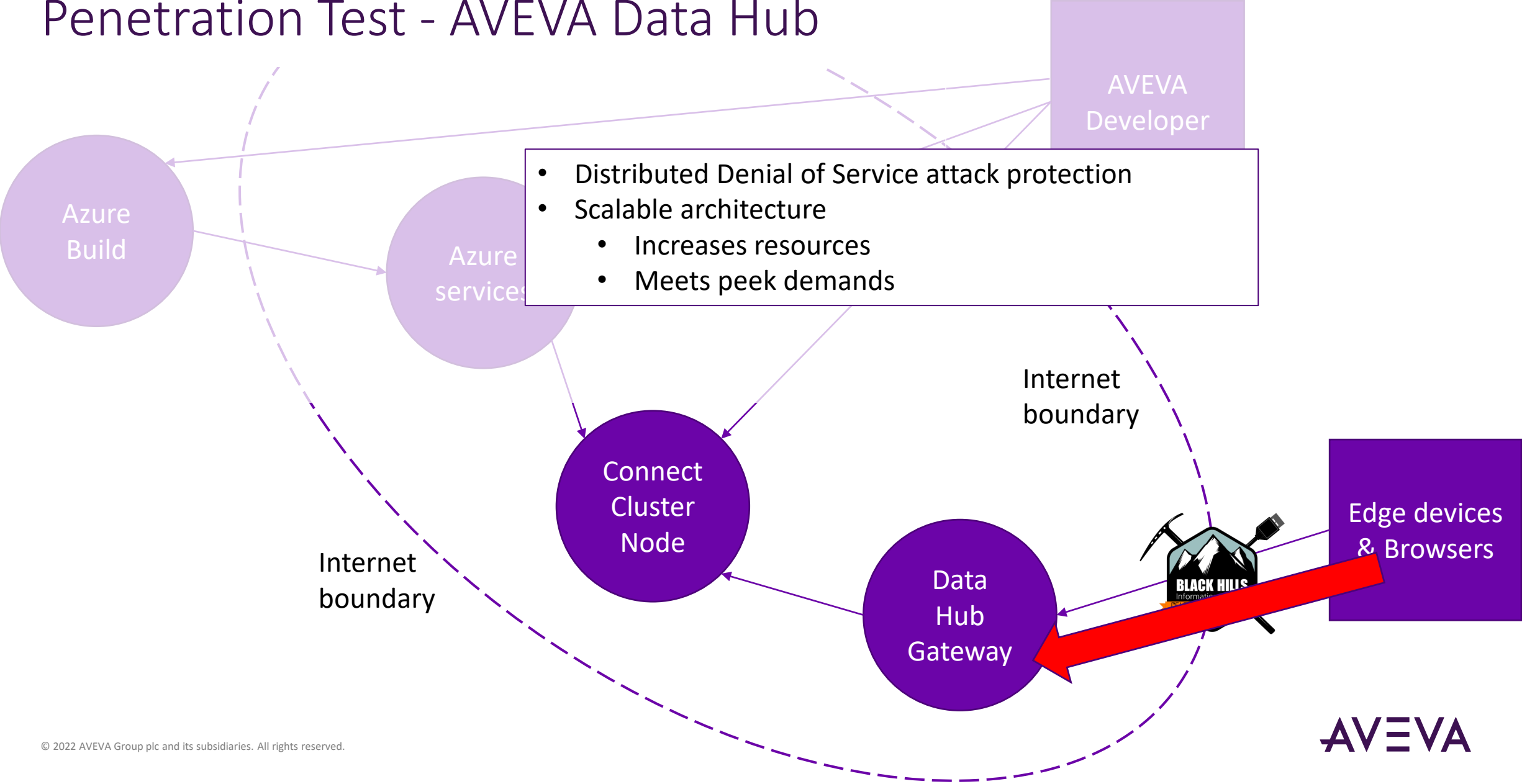
AVEVA Data Hub Threat Model



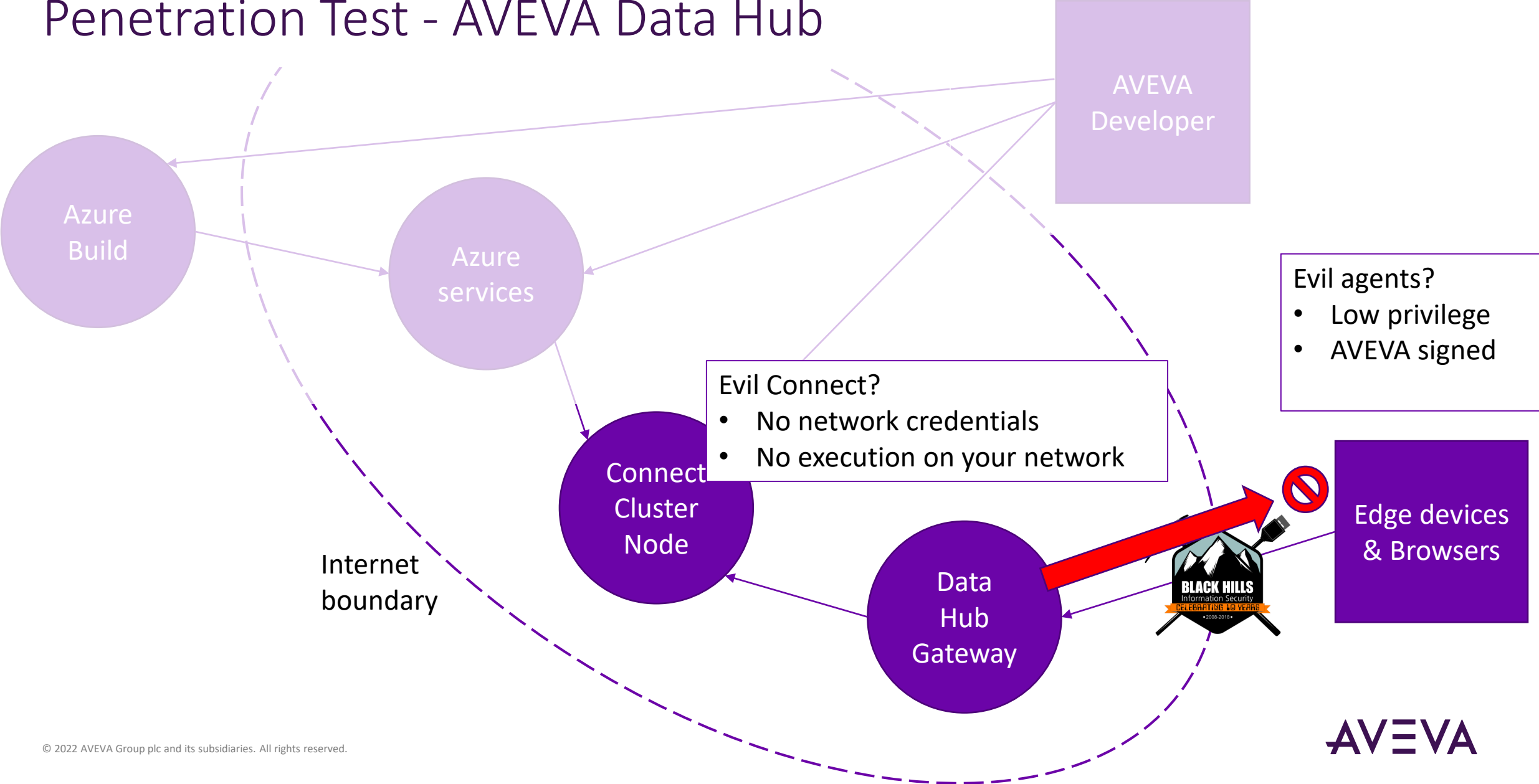
Penetration Testing



Penetration Test - AVEVA Data Hub



Penetration Test - AVEVA Data Hub



Moving Beyond Penetration Testing

- Inside attack
- Developer sabotage
- Developer compromise

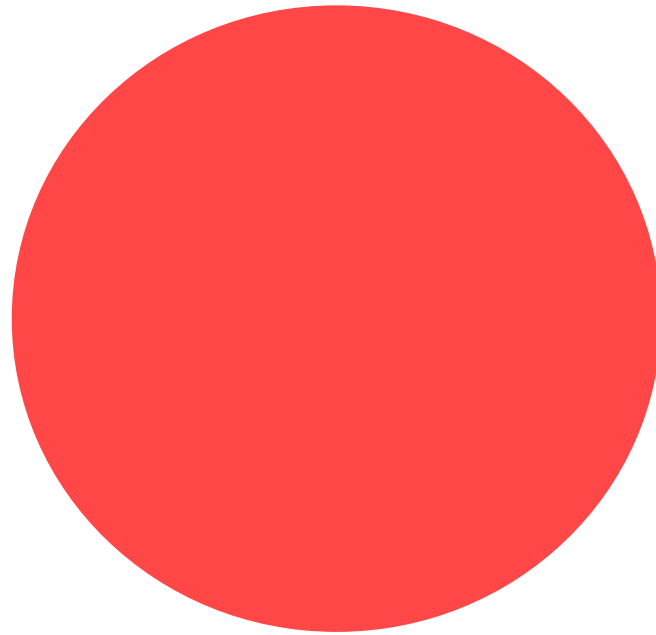


Purple Teaming

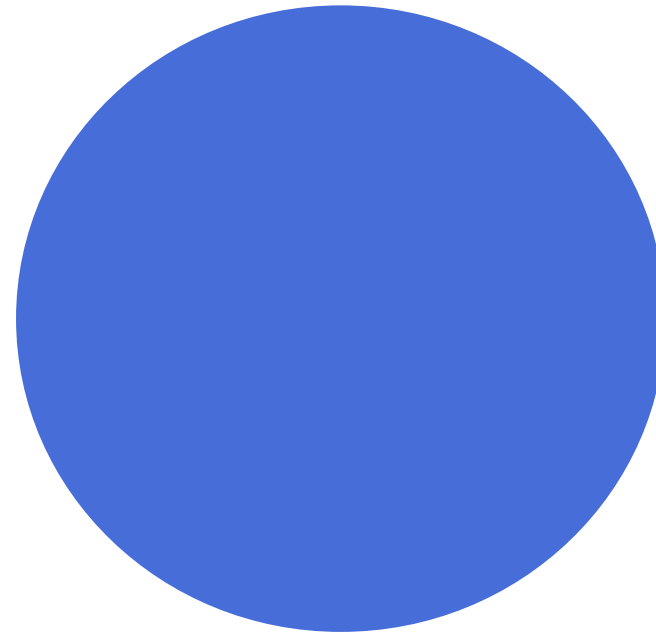
AVEVA



Purple Teaming



Red Team
(attacker) +



Blue Team
(defender)

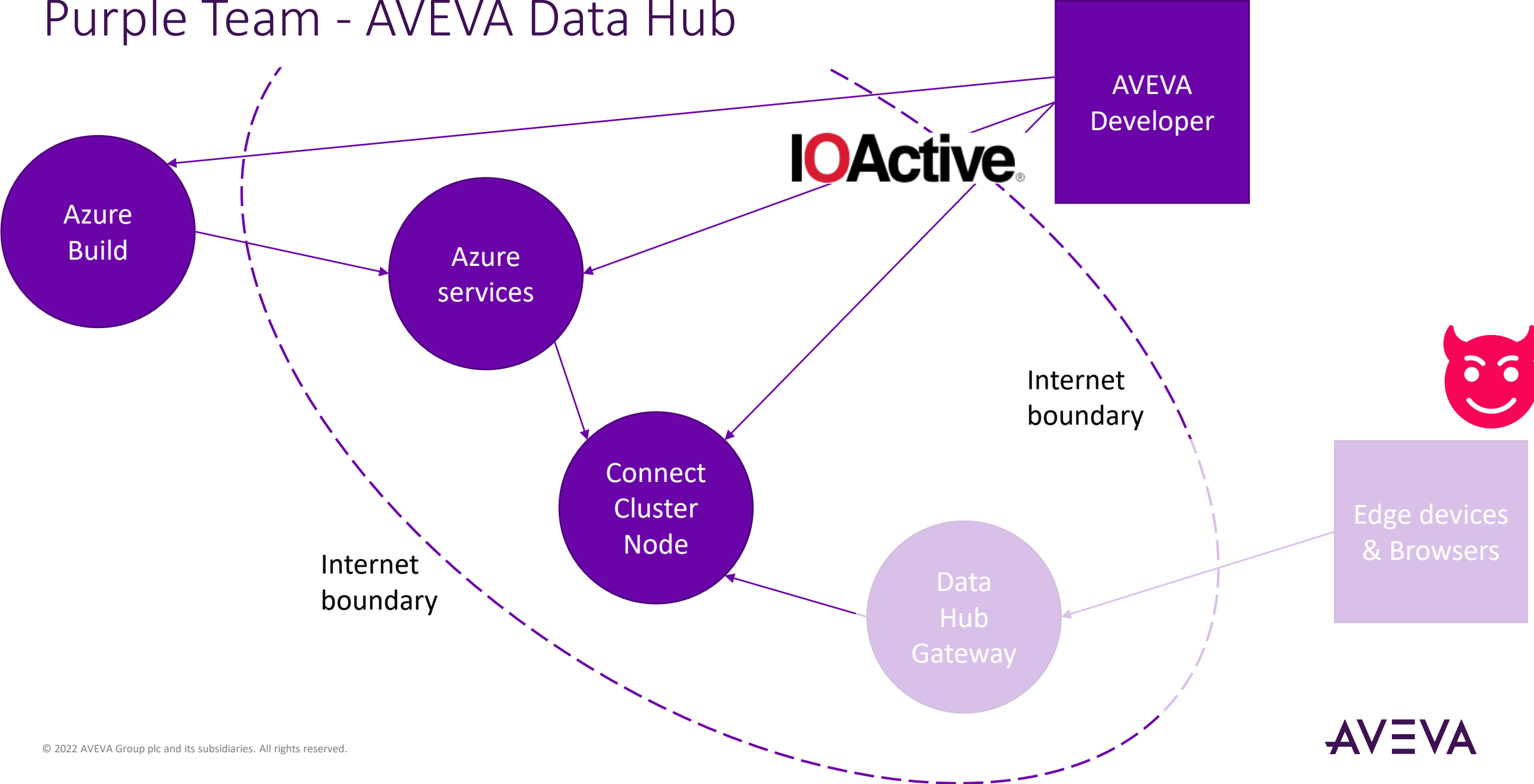




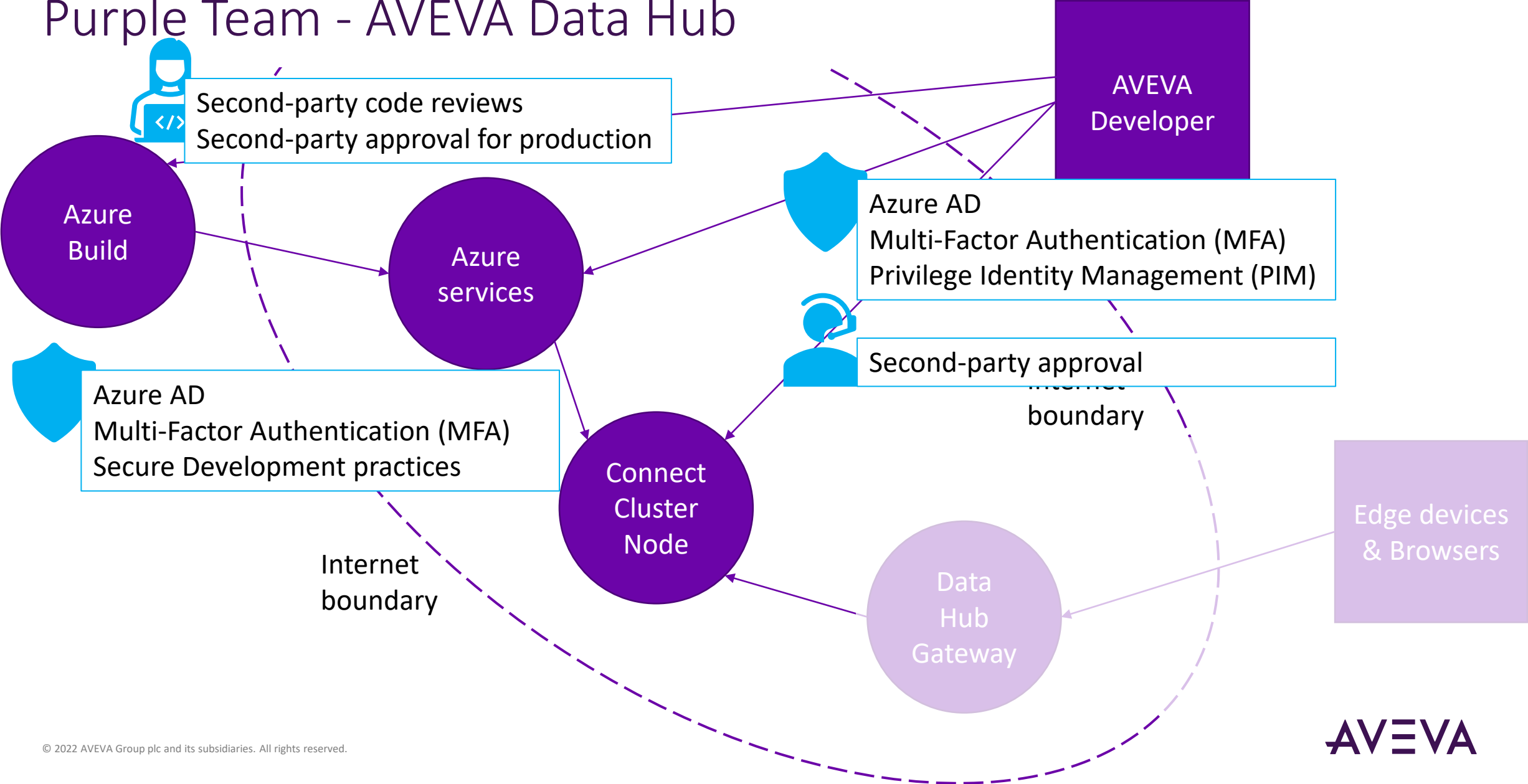
Purple Teaming



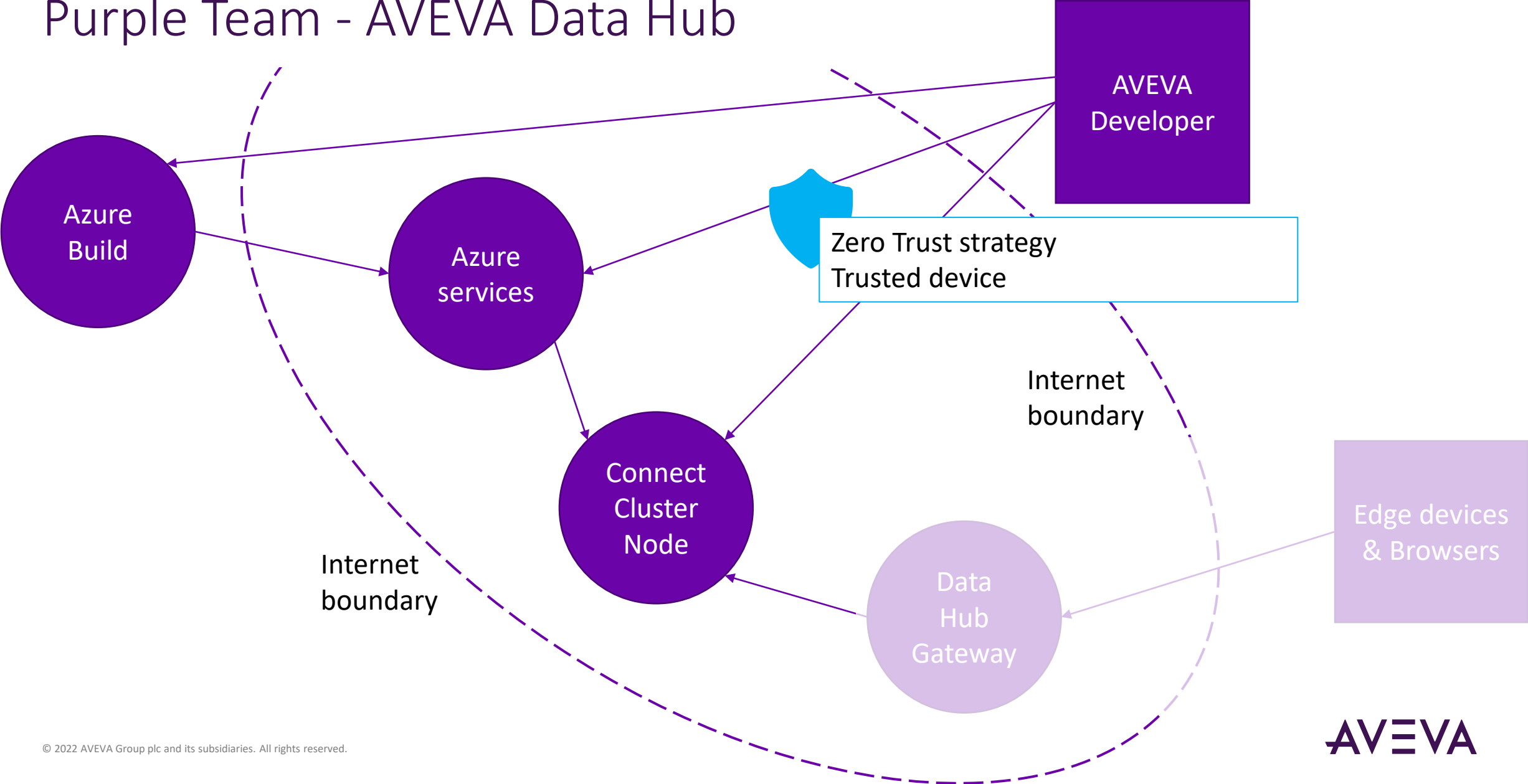
Purple Team - AVEVA Data Hub



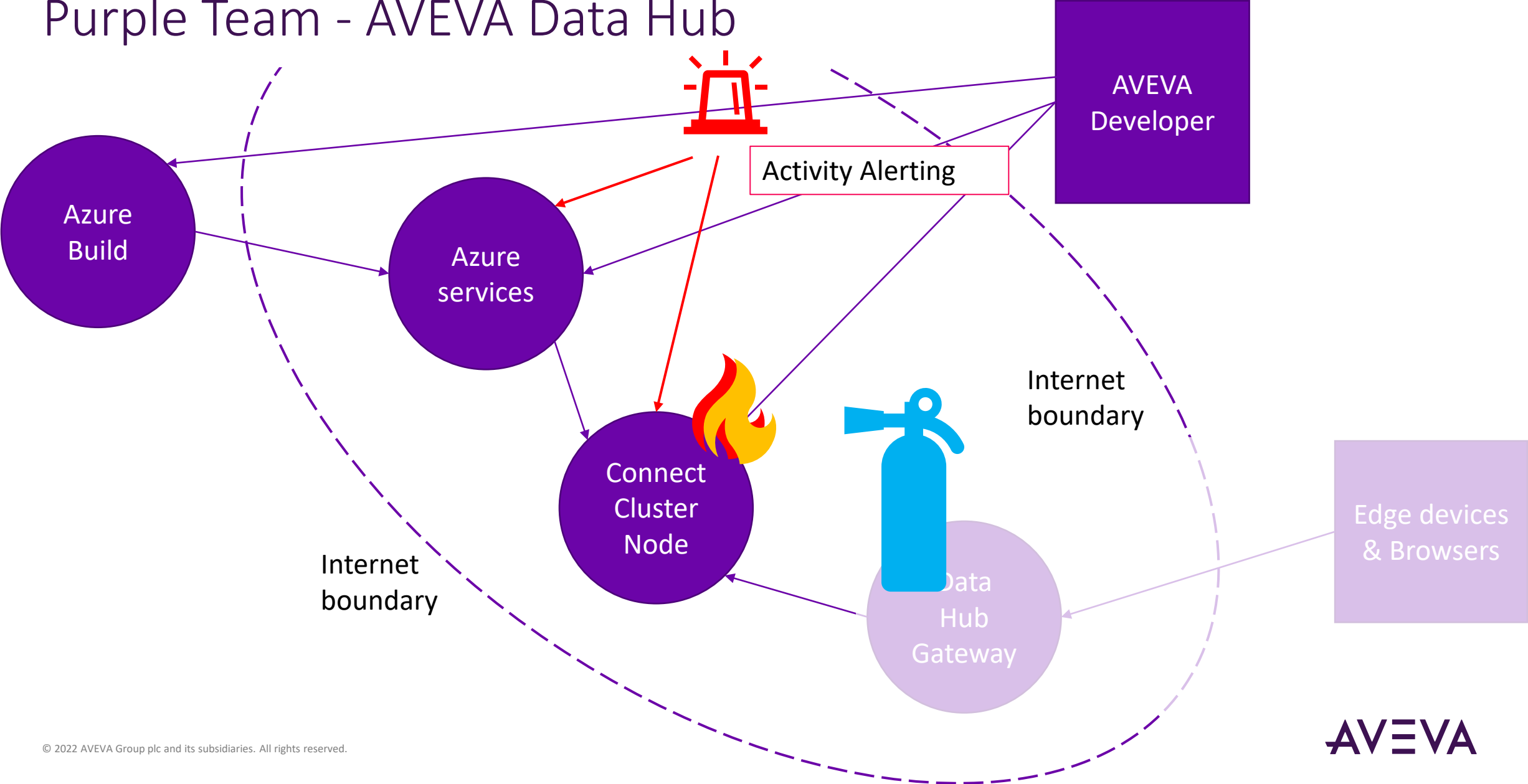
Purple Team - AVEVA Data Hub



Purple Team - AVEVA Data Hub



Purple Team - AVEVA Data Hub



What did we find?



- We learned a lot
- Cross department communication opportunities
 - Attack scenarios cross operational boundaries (IT, Operations, R&D)
 - Don't assume
 - Share perspective
 - Share knowledge
- Remote Desktop access is a risk we didn't need
- Always more to do

Managed Imperative



GOVERN
Ability to Align to
IT Security Policy



TRUSTED
Secure Practices



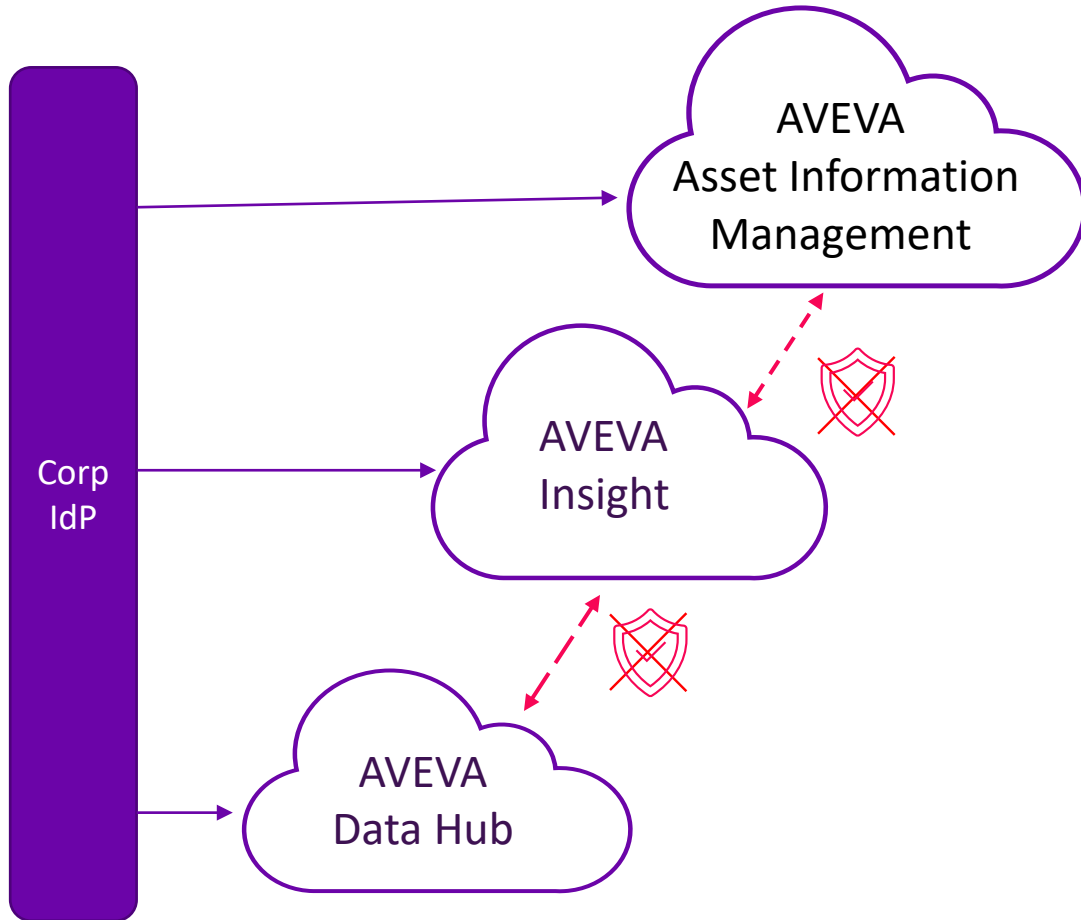
MANAGED
Information
Platform
Management



HYBRID
Secure Industrial
Solution
Architecture

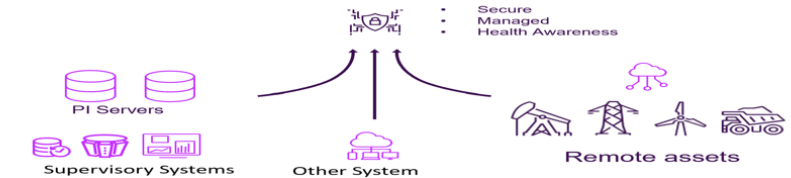
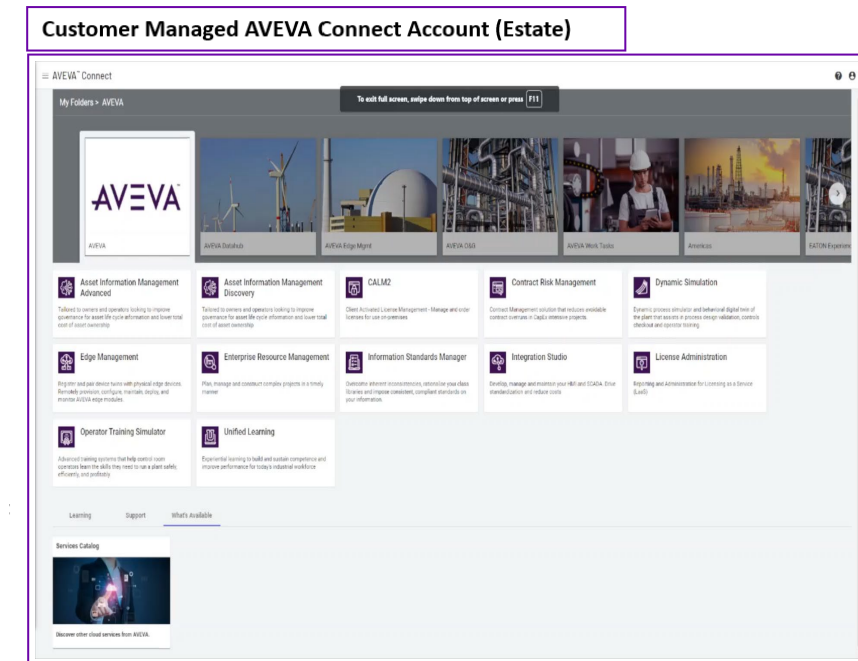
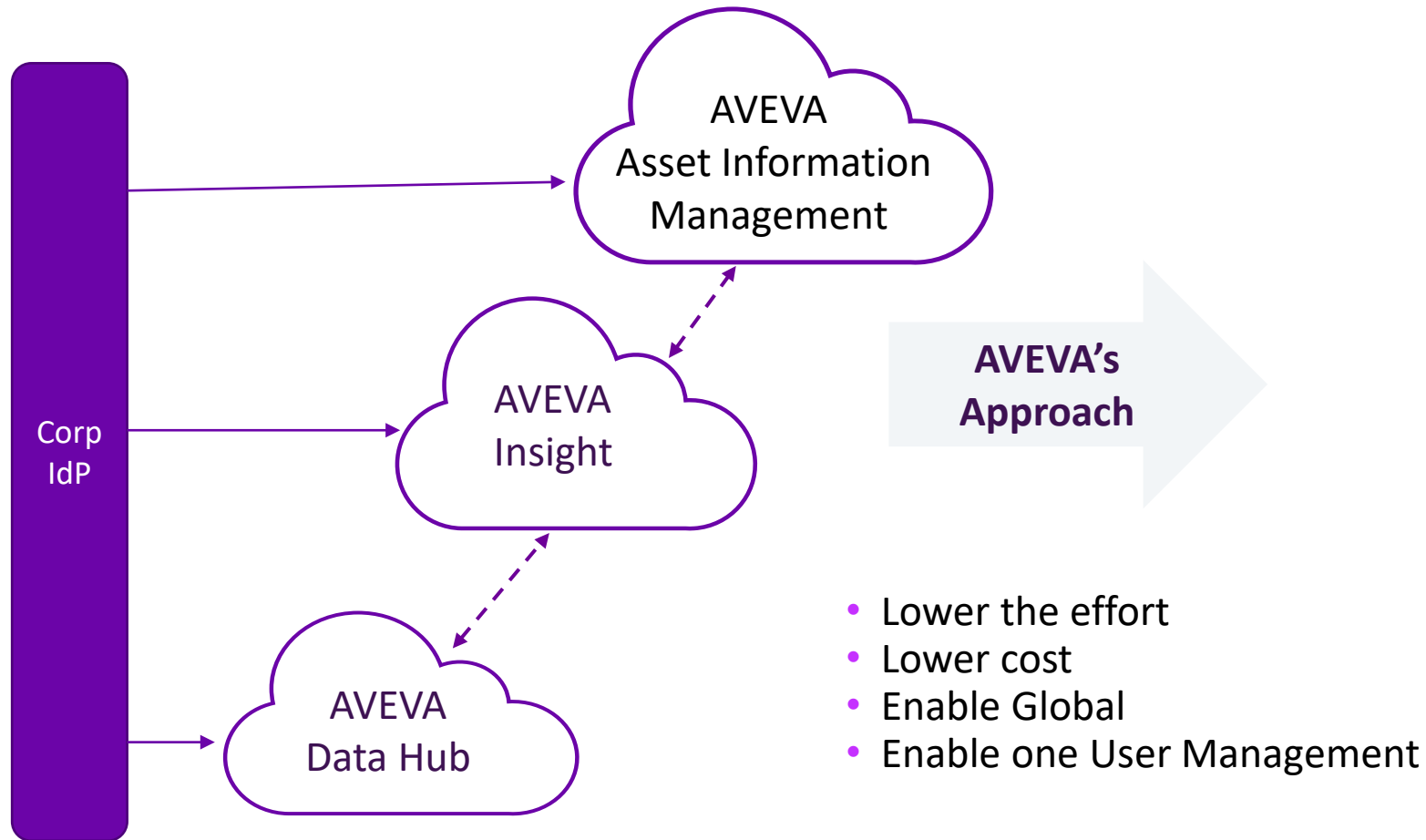
- Unified information model
- Data residency
- Access management
- Data validation & trust

Enabling managed industrial solutions



- Industrial solutions require multiple capabilities
- They need share data to work as a solution
- They need to align

Enabling managed industrial solutions



Enabling managed industrial solutions

AVEVA Connect Account Provides

- Trust between services ✓
- Manage ✓
 - Across services ✓
 - Global deployment ✓
 - Access ✓
 - Entitlement ✓
- Usage intelligence across services ✓

Account Capabilities

Account Structure

SSO- Idp fed

User Management

Solution Management

Edge Deployment Mgmt

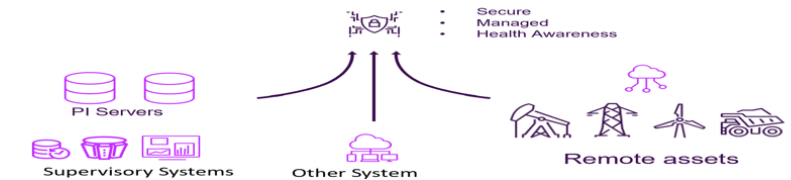
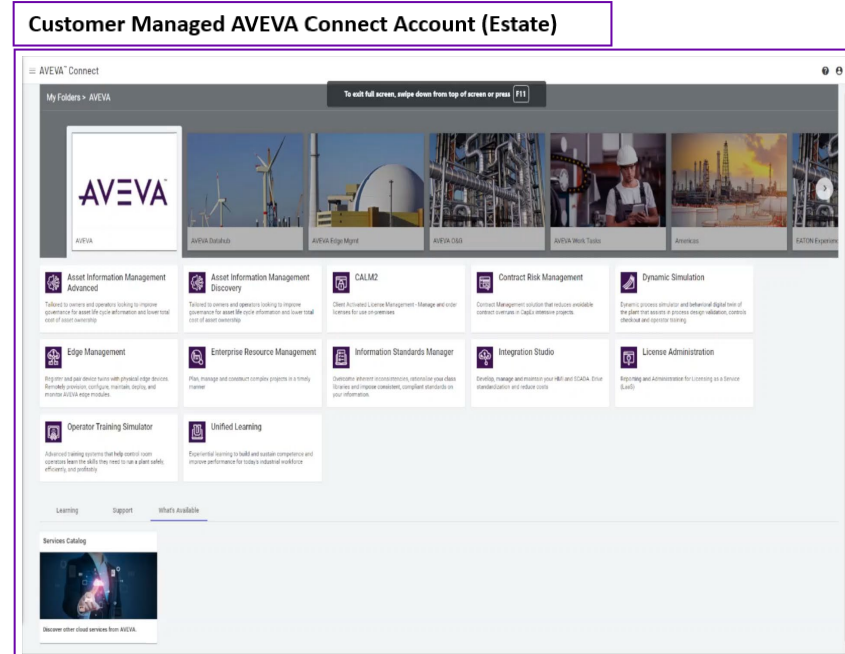
Usage Intelligence

Entitlement Mgmt

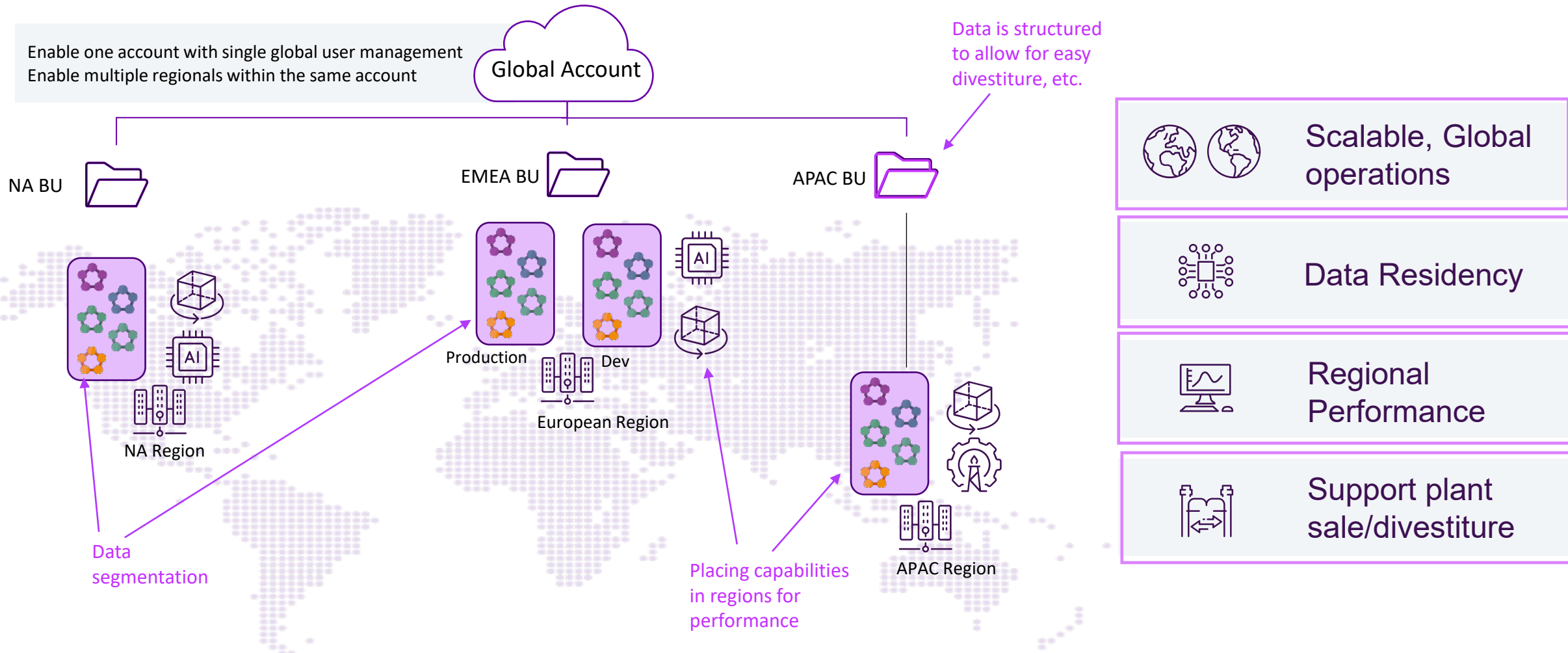
On Premise License Mgmt

Trust Mgmt

API Access Mgmt

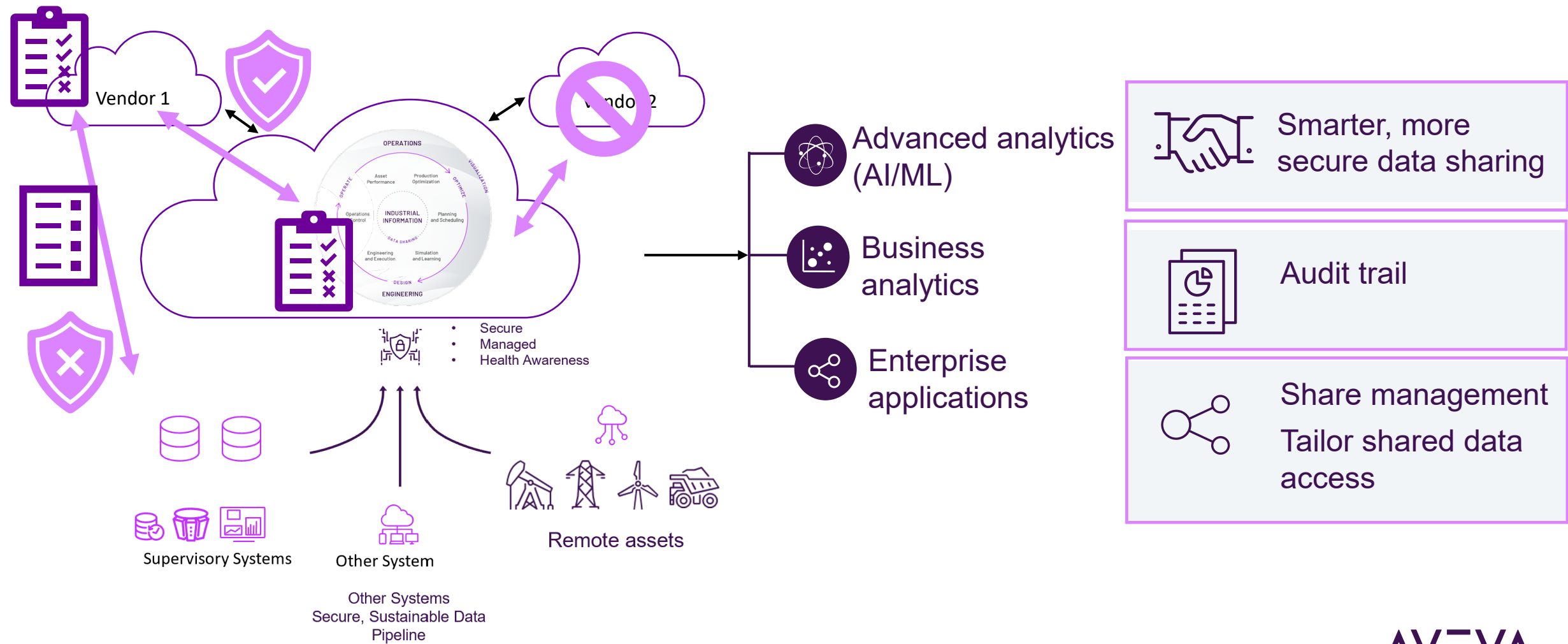


Regionalization management > capability in one account



Data sharing management

Communities



Hybrid Imperative



GOVERN
Ability to Align to
IT Security Policy



TRUSTED
Secure Practices



MANAGED
Information
Platform
Management



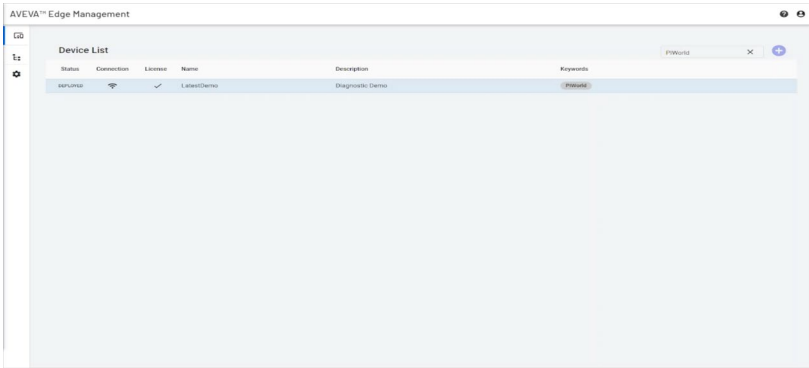
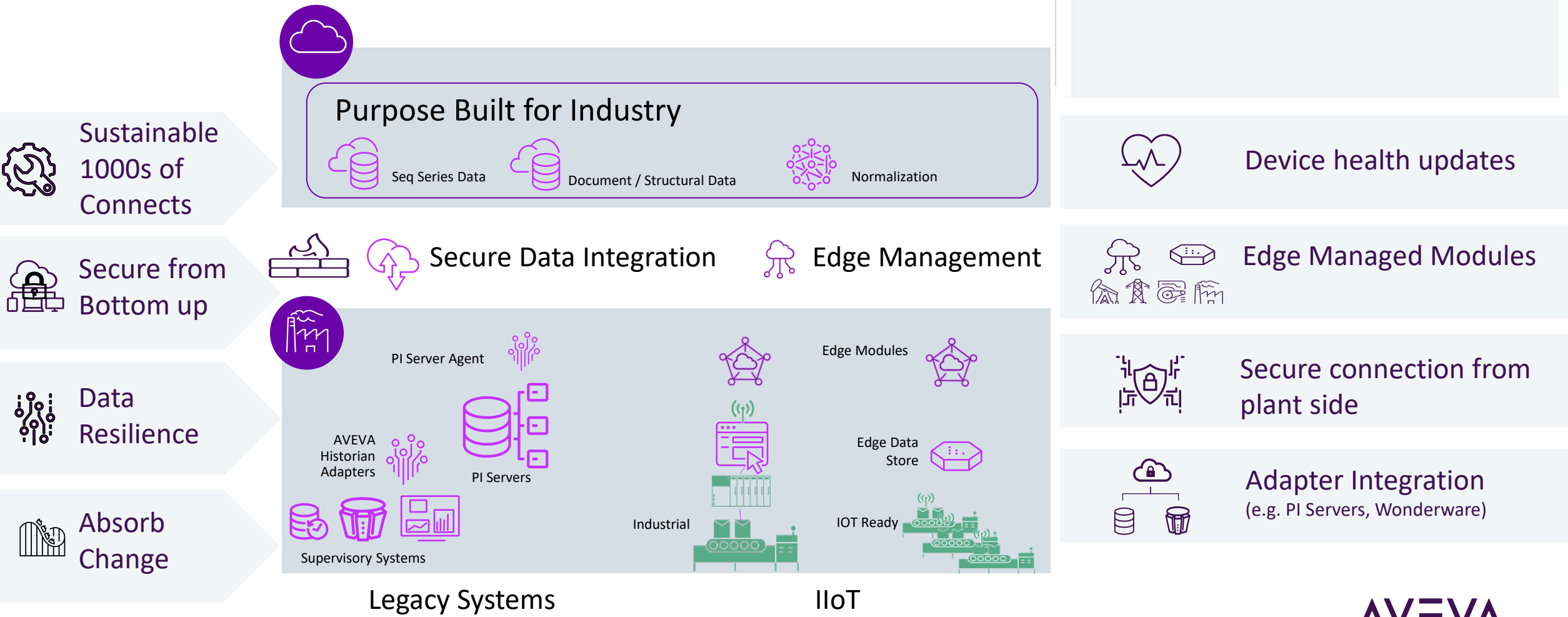
HYBRID
Secure Industrial
Solution
Architecture

- Managed Plant floor/
industrial capture
- Resilient autonomous services
- Secure plant data connectivity
- Data quality



Secure Plant Architectures

Hybrid Approach



Powerful safeguards to counter destructive malware attacks

Protect Assets

Reduce access to corporate networks

- Manage "data out" rather than "users in" to sensitive assets

Sustain Operations

Deploy alternate paths to access critical data streams

- Access to cloud service from BYOD
- Emergency unit operations from autonomous edge

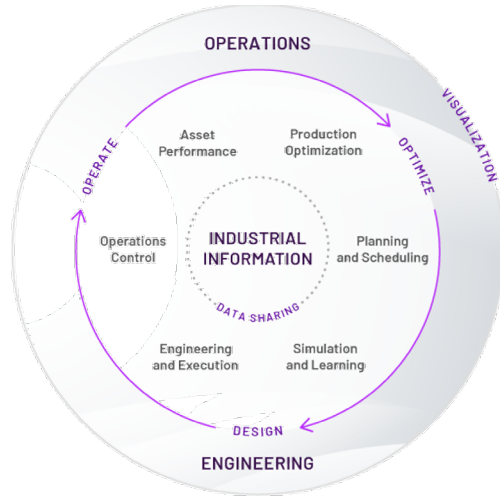
Recover Rapidly

Use the "3-2-1 rule" for critical operations data

- Three backups of your data
- Two different storage types
- One+ offsite backup – industrial cloud!



Industrially trusted > increasing shared responsibility



**AVEVA is your Industrial
Information Platform
Partner**

**Responsible
for security
“at” use**



Customer end users

- User management, roles & permissions
- Protecting account credentials

**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

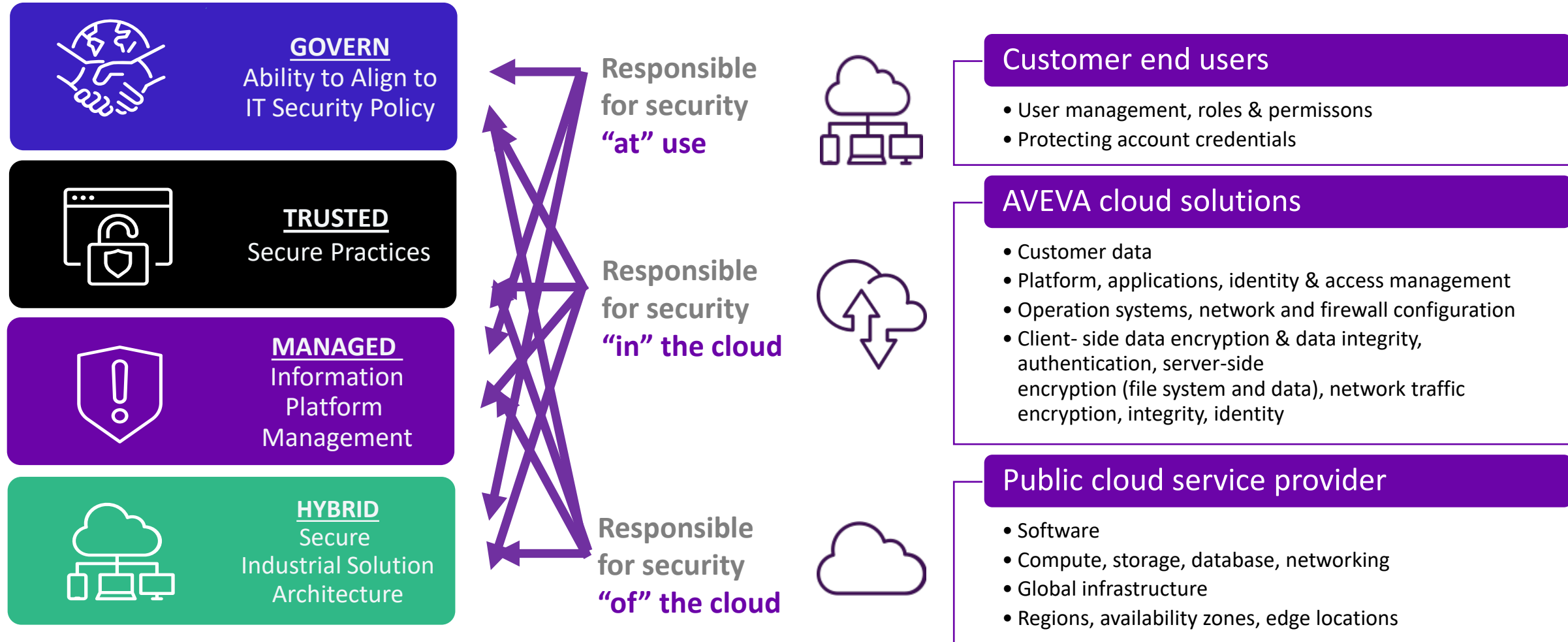
**Responsible
for security
“of” the cloud**



Public cloud service provider

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

Industrially trusted > increasing shared responsibility





Mike Lemley

Product Security Architect

AVEVA

mike.lemley@aveva.com

Questions?

Please wait for the microphone
State your name and company



Please remember to...

Navigate to this session in the mobile
app to complete the survey.




Thank you

AVEVA

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

 [linkedin.com/company/aveva](https://www.linkedin.com/company/aveva)

 [@avevagroup](https://twitter.com/avevagroup)

ABOUT AVEVA

AVEVA is a global leader in industrial software, sparking ingenuity to drive responsible use of the world's resources. The company's secure industrial cloud platform and applications enable businesses to harness the power of their information and improve collaboration with customers, suppliers and partners.

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. With operations around the globe, we are headquartered in Cambridge, UK and listed on the London Stock Exchange's FTSE 100.

Learn more at www.aveva.com