Four Pillars of a Trusted Information Infrastructure

Tim Sowell + Bryan Owen
The reality of convergence. **Industrial Information Platform.**

**Transforming Industrial Landscape**
- **New Work Landscape**
  - Enable collaboration & efficient productivity
  - Empower remote workforce & teams
  - Leverage partner ecosystems
  - Create, acquire & transfer knowledge

- **Secure Industrial Information Thread**
  - Data ownership & protection
  - Increased enterprise data literacy
  - Data Sharing & access management
  - Breakdown information silos

- **Scalability and agility**
  - Increase in deployment speed
  - Flexible application consumption
  - Minimize IT burden & TCO

**Imperatives for an Industrial Information Platform**
- **“Distributed Working”**
- **“Data-Driven Culture”**
- **“Accelerating Change”**

**Expectations for Data Platform**
- **IT Security Compliance**
- **High Available Information Infrastructure**
- **Data/ Information Resilience**
- **Data Governance/ Management**
- **Secure Industrial Data Capture**
- **Secure Managed Information Access**

**AVEVA**
Imperatives for an Industrial Information Platform

- Ability to Federate to corporate identity provider
- Align to IT security groups to roles/permissions
- Ability to apply corporate security policies
- Software asset compliance management
Identity is the key to access your data

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

**AVEVA CONNECT**

Modern Authentication and Transport Layer Security

- OpenID Connect (OAuth2)
- Federated Identity Provider (recommended)
AVEVA Connect platform becoming Trusted

The growth of enterprise users

- Connect Password
- Federation

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

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

**One Entitlement Unit of Measure**
- **= Flex Credits**
  - All offers for a customer are entitled through Flex Credits
  - Credit consumption is reported as one

**Unified Tracking of all AVEVA Software & Services**
- On prem disconnected offers
- On prem “Connected” offers
- On line 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
Imperatives for an Industrial Information Platform

- Ability to Federate to corporate identity provider
- Align to IT security groups to roles/permissions
- Ability to apply corporate security policies
- Software asset compliance management

- Verified SOC 2 trust service criteria
- Certified ISO 27001 information security management system
- Engage industry experts for security risk assessments
- Cloud Operations for platform service availability
Ensuring cloud security

Secure Development

- **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**

Keep our customers secure
- Advance the Security Posture of our products
- Manage supply chain risk
- Provide actionable information about issues (CERT)

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

Increase security awareness
- Collaboration with industry stakeholders
- Ensure Security Requirements are defined
- Build Security into Architectures
Security processes > built using advanced security tools, compliant with international standards and **strongly verified**.
Industrial software as a service > availability is given

AVEVA Global Cloud DevOps provides 24x7 monitoring of all AVEVA solutions and services. Cloud solutions are instrumented for automated deployment and monitoring wherever possible.

Alliances
- Microsoft®
- Cisco®
- Outpost24®
- Splunk®
- Cloud Security Alliance®

Data Retention Approach
- Every 7th backup moved to suitable central backup repository and saved for 28 days
- Central backup repository for other cloud services that don’t use Region B

Structured Data Retention
- 28-day retention
- 90-day retention
- 365-day retention

Security Policies
- Security Monitoring and Alerting
- Network and Domain Monitoring
- Security Logging
- Digital Tracing

© 2022 AVEVA Group plc and its subsidiaries. All rights reserved.
Imperatives for an Industrial Information Platform

GOVERN
Ability to Align to IT Security Policy

MANAGED
Information Platform Management

HYBRID
Secure Industrial Solution Architecture

TRUSTED
Secure Practices

- Ability to Federate to corporate identity provider
- Align to IT security groups to roles/permissions
- Ability to apply corporate security policies
- Software asset compliance management

- Verified SOC 2 trust service criteria
- Certified ISO 27001 information security management system
- Engage industry experts for security risk assessments
- Cloud Operations for platform service availability

- Ability combine data into engaging unified information model
- Data segmentation (residency) management
- Information access management
- Data validation / data trust
Enabling managed industrial solutions

**AVEVA’s Approach**
- Lower the effort
- Lower cost
- Enable Global
- Enable one User Management

**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

**AVEVA Connect Account Provides**
- Trust between services
- User management across services
- Ability to have globally deployed solutions in different regions
- Account API access management
- One entitlement management
- One usage intelligence

- Industrial solutions require multiple capabilities
- They need share data to work as a solution
- They need to aligned
Regionalization management > capability in one account

Enable one account with single global user management
Enable multiple regionals within the same account

Global Account

- NA BU
- EMEA BU
- APAC BU

NA Region

Data segmentation

EMEA BU

European Region

Placing capabilities in regions for performance

APAC BU

APAC Region

Scalable operations data, anywhere

Data Residency

Regional Performance

Divestiture of Digital Twin due to plant sale
Data sharing management

- Smarter, more secure data sharing
- Audit trail of access
- Audit of permission
- Information management sharing
- Allow different access to specific data

Vendor 1

Vendor 2

Advanced analytics (AI/ML)

Business analytics

Enterprise applications

- Secure
- Managed
- Health Awareness

Supervisory Systems

Other System

Remote assets

Other Systems
Secure, Sustainable Data Pipeline
Imperatives for an Industrial Information Platform

- Ability to federate to corporate identity provider
- Align to IT security groups to roles/permissions
- Ability to apply corporate security policies
- Software asset compliance management

- Verified SOC 2 trust service criteria
- Certified ISO 27001 information security management system
- Engage industry experts for security risk assessments
- Cloud Operations for platform service availability

- Ability to combine data into engaging unified information model
- Data segmentation (residency) management
- Information access management
- Data validation / data trust

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

Proven and secure options to unify Industrial Data

- Sustainable Across 1000s of Connects
- Secure from Bottom up
- Data Resilience
- Absorb Change

Connect, device health Updates

Edge Managed Modules

Secure establishment of connection from plant side

Native Secure integration from on-premises systems “adapters” (e.g. PI Servers, Wonderware)
Powerful safeguards to counter destructive malware attacks

Reduce third party access to corporate networks
- Manage ‘data out’ rather than ‘users in’ to sensitive assets

Deploy alternate paths to access critical data streams
- Access to cloud service from BYOD
- Emergency unit operations from autonomous edge

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

**Customer end users**
Responsible for security “at” use

**AVEVA cloud solutions**
Responsible for security “in” the cloud

**Public cloud service provider**
Responsible for security “of” the cloud

- **User management, roles & permissions**
- **Protecting account credentials**

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

**Software**
- Compute
- Storage
- Database
- Networking
  - Global Infrastructure
  - Regions
  - Availability zones
  - Edge locations
THANK YOU
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.
ABOUT AVEVA

AVEVA is a global leader in industrial software, driving digital transformation and sustainability. By connecting the power of information and artificial intelligence with human insight, AVEVA enables teams to use their data to unlock new value. We call this Performance Intelligence. AVEVA’s comprehensive portfolio enables more than 20,000 industrial enterprises to engineer smarter, operate better and drive sustainable efficiency. AVEVA supports customers through a trusted ecosystem that includes 5,500 partners and 5,700 certified developers around the world. The company is headquartered in Cambridge, UK, with over 6,500 employees and 90 offices in over 40 countries.

Learn more at www.aveva.com