

OCTOBER 26, 2023

Security essentials of the AVEVA™ PI System™

AVEVA secure by design practices

Bryan Owen PE

AVEVA – Head of Product Security

AVEVA

Cybersecurity

AVEVA advances industrial software assurance with a focus on secure by design

Challenge

- Operational risk of insecure technology is too high, causing excessive cost for defensive measures and regulatory compliance activities.
- Increased criminal use of techniques, once limited to highly resourced nation states, is amplifying cyber risk to legacy operational technology.

Solution

- Enhance the AVEVA PI System security model including modern authentication, hybrid-cloud infrastructure, and industrial edge integration.
- Advance assurance of software development operations and supply-chain integrity.

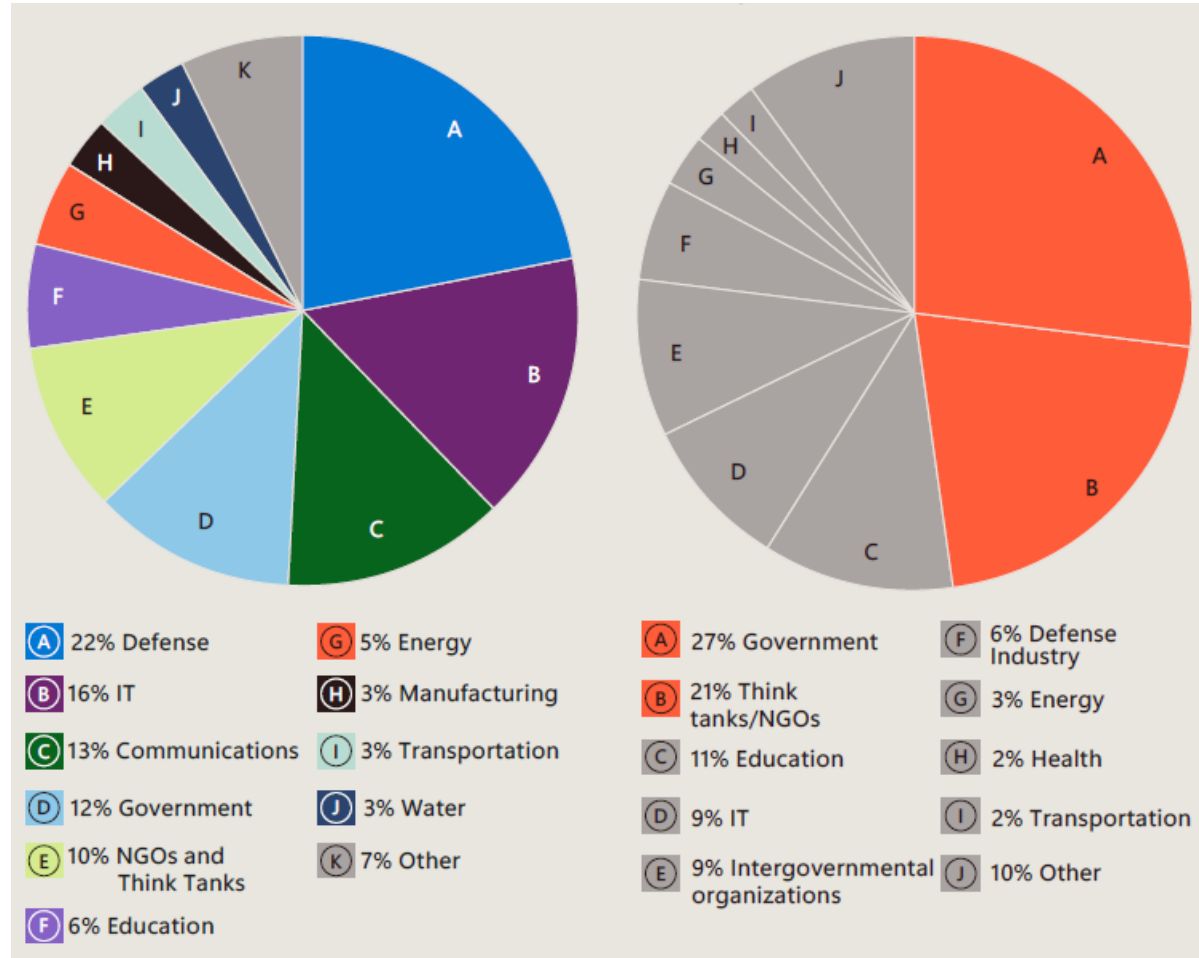
Results

- **Retired use of legacy technology**
- **Designed a path forward to inherently safer technology**
- **Embraced software assurance and compliance directives**



Insights from Microsoft Digital Defense Report 2023

Sectors most targeted by nation state threats



“As the threat landscape evolves, we are seeing a blurring of lines between cyber operations, espionage, influence campaigns, and destructive attacks.”

John Lambert
Corporate Vice President, Distinguished Engineer, Microsoft Security Research

25%

of OT devices on customer networks use unsupported operating systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats.

41%

of the threat notifications Microsoft sent to online services customers between July 2022 and June 2023 went to critical infrastructure organizations.

Strategy: Secure by design

A global initiative for “built-in” security helps everyone

- Call to action for technology suppliers
- Take ownership of security outcomes
- Embrace radical transparency and accountability
- Build organizational structure to achieve these goals

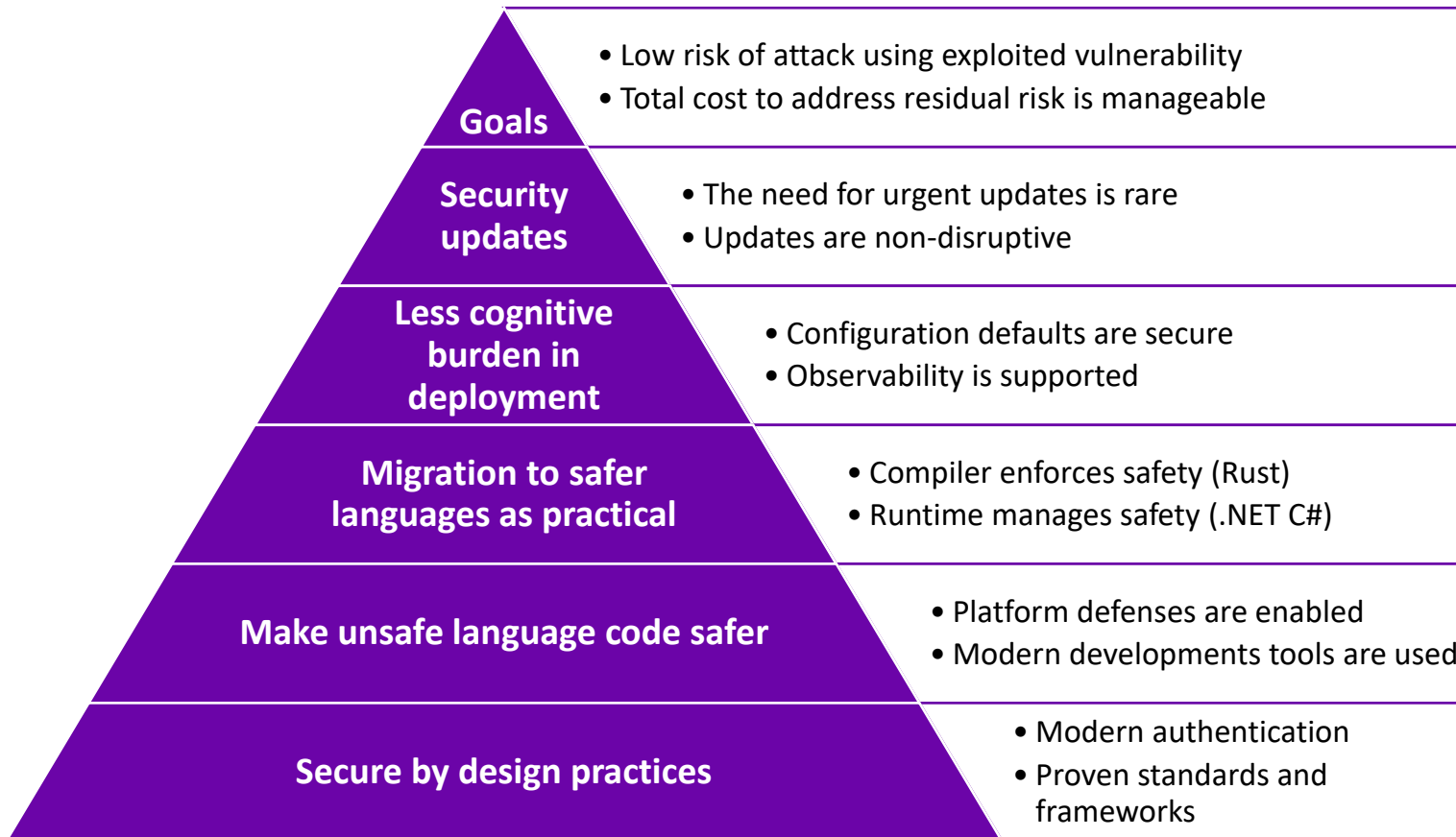


Shifting the Balance of Cybersecurity Risk:
Principles and Approaches for Security-by-
Design and -Default

Publication: April 13, 2023
Cybersecurity and Infrastructure Security Agency
NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Secure by design is foundational

Important concepts for secure by design industrial software



“Consumer safety must be front and center in all phases of the technology product lifecycle— with security designed in from the beginning.”

DIRECTOR JEN EASTERLY

AVEVA uses proven software security standards and frameworks

Microsoft
SDL

- ISO 27034

ISA/IEC
62443

- ISA Secure

NIST SP
800-218

- EO 14028



ISO 9001 Quality Certification

- Quality Management certificate
- Improves product, process and service quality
- Increases customer satisfaction



ISO 27001 Security Certification

- Information Security Management
- Risk-based asset management
- Continuous risk assessments



ISASecure SDLA Certification

- IEC 62443-4-1 standard
- Security Development Lifecycle Assurance
- Secure by design; secure coding, verification and support

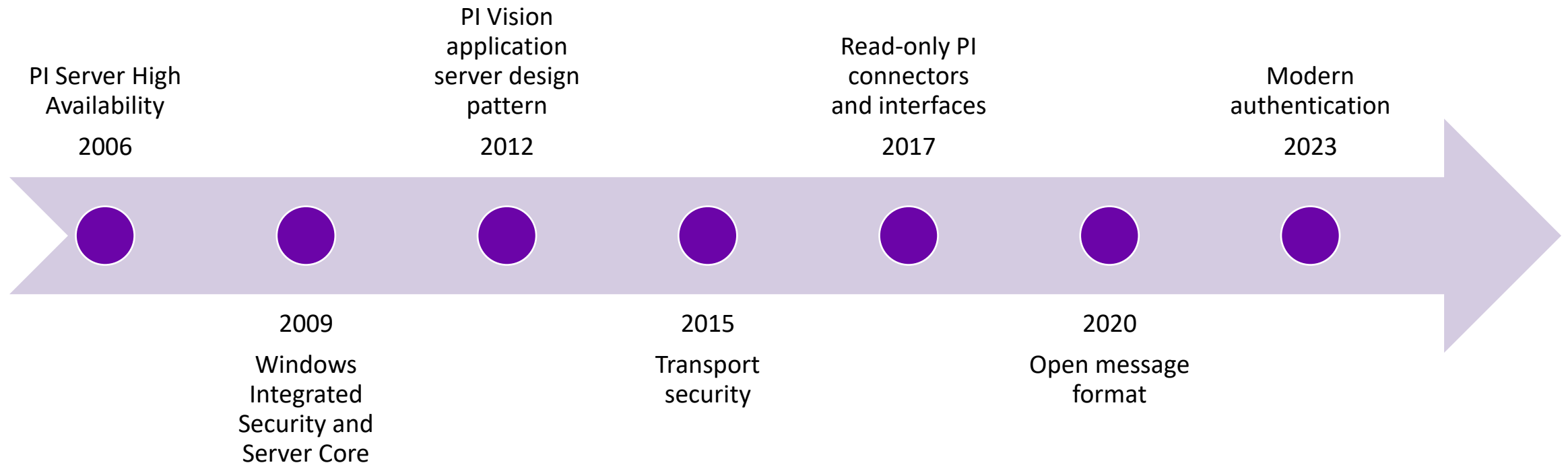


SOC 2 Type 2 Audit

- Security assessment of cloud services
- AICPA Trust Criteria
- Business imperative for AVEVA Cloud

Secure by design architecture

Important AVEVA PI System security architectural milestones



Modern authentication eases MFA adoption

AVEVA™ PI Server 2023 and AVEVA Identity Manager

New with AVEVA PI Server 2023!

- A claims-based approach to verify user and client identities.
- The AVEVA™ Connect identity provider (IdP) can delegate authentication to IdPs that support SAML 2, OpenID Connect, ADFS or Azure AD.
- The ability to use access tokens and manage TLS certificates through the AVEVA Identity Manager or another certificate management tool.

A recent study based on real-world attack data from Microsoft Entra found that **MFA reduces the risk of compromise by 99.2 percent.**

How effective is multifactor authentication at deterring cyberattacks?

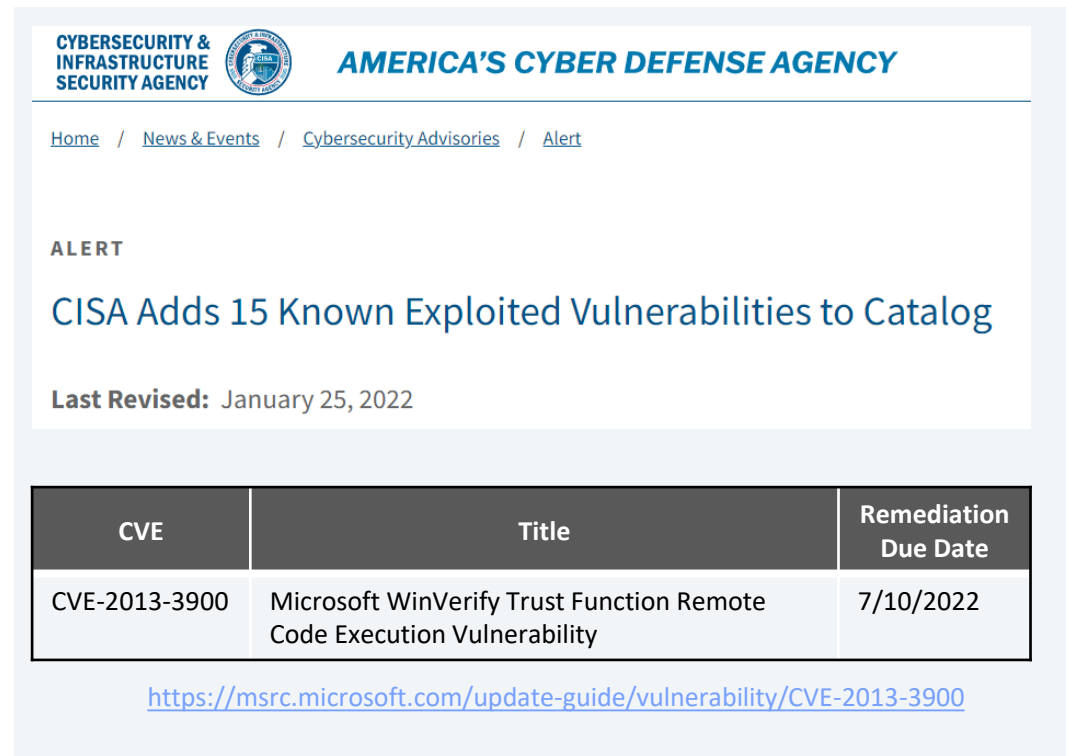
<https://arxiv.org/pdf/2305.00945.pdf>

Modernization of digital signature infrastructure

Alert... Program-level authentication is under exploitation!

Microsoft does not plan to enforce the stricter verification by default.

- Opt-in feature via registry key setting
- Available since December 10, 2013
- AVEVA software development environment is compliant
 - Compatibility for AVEVA PI System and other products is confirmed
 - Recommend coordination with IT to set the registry key
- Goal: enable authentication for each and every program
 - Consider technical enforcement using Windows Defender Application Control



The screenshot shows a webpage from the Cybersecurity & Infrastructure Security Agency (CISA), part of America's Cyber Defense Agency. The page is an alert titled "CISA Adds 15 Known Exploited Vulnerabilities to Catalog", last revised on January 25, 2022. A table below the title lists a specific vulnerability: CVE-2013-3900, titled "Microsoft WinVerify Trust Function Remote Code Execution Vulnerability", with a remediation due date of 7/10/2022. A link is provided at the bottom of the table to the Microsoft update guide for this vulnerability.

CVE	Title	Remediation Due Date
CVE-2013-3900	Microsoft WinVerify Trust Function Remote Code Execution Vulnerability	7/10/2022

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900>

NIST SSDF recommendations to help make unsafe code safer

AVEVA uses modern SaaS based development tool chains including static application security testing and software composition analysis.

- Prepare the Organization (PO)
- Implement Supporting Toolchains (PO.3)
- Produce Well-Secured Software (PW)
- Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality (PW.4)
- Configure the Compilation, Interpreter, and Build Processes to Improve Executable Security (PW.6)



Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>

Enable exploit mitigations to help make unsafe code safer

AVEVA uses BinSkim to verify operating-system-provided mitigations are enabled during build.

BinSkim checks characteristics for each executable file:

- **Use of outdated compiler tool sets** - Binaries should be compiled against the most recent compiler tool sets wherever possible to maximize the use of current compiler-level and OS-provided security mitigations.
- **Insecure compilation settings** - Binaries should be compiled with the most secure settings possible to enable OS-provided security mitigations, maximize compiler errors and actionable warnings reporting, among other things.
- **Signing issues** - Signed binaries should be signed with cryptographically-strong algorithms.

AVEVA BinSkim Checks			
LoadImageAboveFourGigabyteAddress	DoNotMarkImportsSectionAsExecutable	EnableSafeSEH	EnableStackProtector
DoNotIncorporateVulnerableDependencies	EnableStackProtection	DoNotMarkWritableSectionsAsShared	EnableReadOnlyRelocations
DoNotShipVulnerableBinaries	DoNotModifyStackProtectionCookie	DoNotMarkWritableSectionsAsExecutable	UseCheckedFunctionsWithGcc
BuildWithSecureTools	InitializeStackProtection	SignSecurely	EnableSecureSourceCodeHashing
EnableCriticalCompilerWarnings	DoNotDisableStackProtectionForFunctions	EnableSpectreMitigations	EnableShadowStack
EnableControlFlowGuard	EnableHighEntropyVirtualAddresses	EnablePieOnExecutables	EnableMicrosoftCompilerSdlSwitch
EnableAddressSpaceLayoutRandomization	MarkImageAsNXCompatible	DoNotMarkStackAsExecutable	EnableBindNow

<https://github.com/microsoft/bin skim/blob/main/docs/UserGuide.md>

Migration to safer languages – .NET managed code and Rust

Open-source, cross-platform .NET framework is preferred by AVEVA. PI Adapters have started to embrace RUST as protocol libraries come to market.

PI System	C++	.NET	RUST
PI Adapters		✓	✓
PI AF Client		✓	
PI Analysis		✓	
PI Connectors		✓	
PI Data Archive	✓		
PI Interfaces	✓		
PI Notifications		✓	
PI SDK	✓		
PI Vision		✓	
PI WebAPI		✓	

Protocol Libraries

Our libraries are written in **safe Rust** with bindings available for a number of other languages including C/C++, .NET, and Java. They offer both native performance and the security and reliability of a higher-level language.

[Read More](#) [About Rust](#)

Modbus [View](#)

DNP3 [View](#)

Source: STEP FUNCTION I/O
<https://stepfunc.io>



Observability is provided by integrated security infrastructure

AVEVA™ PI System™ observability strategy leverages security infrastructure and partner solutions while providing action indicators for application-level activity.

- Network activity
 - Documented ports and services
 - AVEVA PI System 'aware' firewalls (e.g. Palo Alto App-Id)
- Identity-based activity
 - Active directory
 - Claims-based identity provider
- Application activity
 - Built-in health indicators
 - REST API / PI powershell for integration
 - AVEVA PI System 'aware' solutions (e.g. Dragos Platform)

Health and Diagnostics

Health

Device status

Next health message expected

Diagnostics

System

Stream count

IO rate

Error rate

Egress

Health and Diagnostics

<https://docs.aveva.com/bundle/pi-adapter-dnp3/page/main/shared-content/health/health-and-diagnostics.html>

Configuration defaults are secure

Community engagement is needed to identify the best ideas for effective default configuration.

- New deployment
 - Posture: Balanced
 - More flexibility to pursue secure defaults
- Major upgrade
 - Posture: Proportionate
 - Limited to areas with breaking changes
- Long-term service branch
 - Posture: **Highly Risk Adverse**
 - Introduce no breaking changes

Description	Long-Term Servicing Channel	Annual Channel
Recommended scenarios	General purpose file servers, Microsoft and non-Microsoft workloads, traditional apps, infrastructure roles, software-defined Datacenter, and hyper-converged infrastructure	Containerized applications running on container hosts benefiting from faster innovation
New releases	Typically 2–3 years	Typically 12 months
Support	5 years of mainstream support, plus 5 years of extended support	18 months of mainstream support, plus 6 months of extended support
Activation	All Windows Server activation keys	Windows Server Datacenter activation keys
Licensing	All licensing programs [↗]	Software Assurance customers only [↗]
Get media	All distribution channels	Volume Licensing Service Center (VLSC) and Visual Studio Subscriptions only
Installation options	Server Core and Server with Desktop Experience	Server Core for a container host only

Windows Server Servicing Channels

<https://learn.microsoft.com/en-us/windows-server/get-started/servicing-channels-comparison>

Updates are non-disruptive

AVEVA PI Server High Availability and long-term servicing branch are key enablers.

- Testing is still appropriate for critical operations
 - AVEVA PI System deployment sample helps with baseline testing
- Consider shifting the balance with ADH
 - AVEVA is responsible for cloud service updates!

The AVEVA PI System Deployment Sample for Azure installs core AVEVA PI System components such as Data Archive and Asset Framework.

The template deploys an AVEVA PI System that includes the following with an option for High Availability (HA) for the components indicated:

- Domain Controller (HA)
- SQL Server (HA)
- RDS box for remote access
- [PI Data Archive server](#) (HA)
- [PI AF server](#) (HA)
- PI Analysis Service
- [PI Vision](#) (HA)

PI System on Azure

https://github.com/AVEVA/sample-pi_core-deployment_azure-powershell/blob/main/README.md

The need for urgent updates is generally rare

Most urgent issues to date are primarily OS related

The AVEVA PI System is designed for deployment on Windows server core

- Reduced attack surface
- Fewer updates

Commitment to ethical disclosure of software vulnerabilities is central to our values

- Routine security updates
- Actionable defensive measures

The need for urgent updates can still emerge

- When in doubt, patch!

Windows Update compatibility testing completed successfully.

Microsoft periodically (usually the second Tuesday of the month) provides security updates, or patches, for their products. You can access details about these patches directly from Microsoft's [Security Update Guide](#).

Each month OSISOFT applies the newest patches to its test environment for targeted testing of the most current release of PI Data Archive and PI Asset Framework with the most recent Windows Server operating systems in wide use by our customers.

Currently, these are **Windows Server 2016** through **Windows Server 2022**.

In addition, OSISOFT incorporates all the supported Windows operating systems into our *daily* development and test environments.

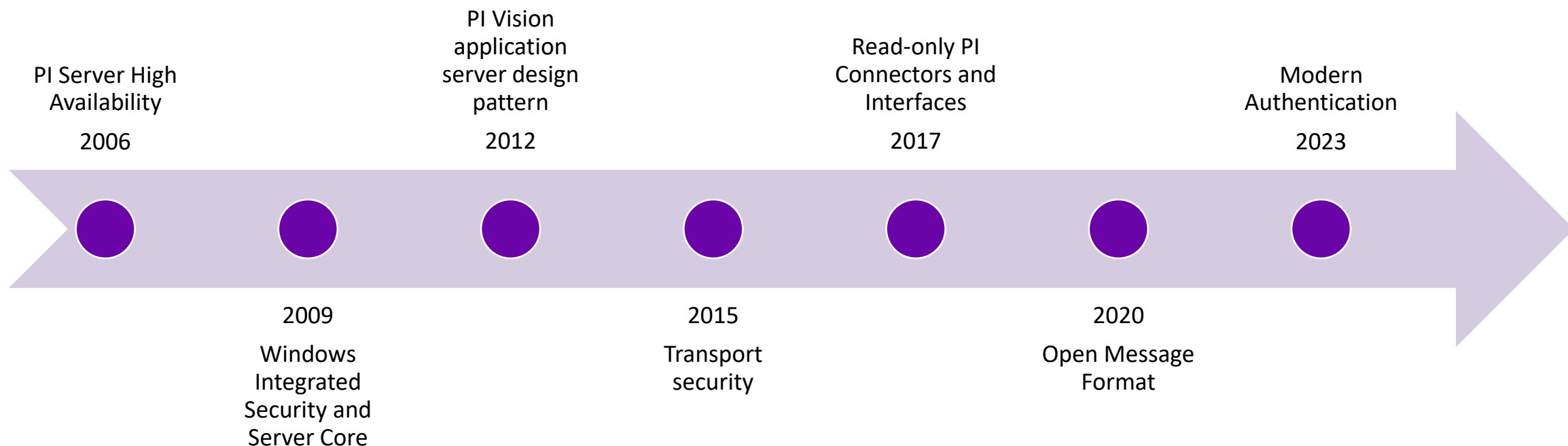
If any of our testing detects any compatibility issue with PI Server software resulting from a Microsoft security patch, OSISOFT will alert customers within 72 hours of discovering the issue. It is worth noting that, since 2008, PI Server software has been Windows Certified for Server Core mode. Server Core significantly reduces the number of applicable security updates and provides extra reliability because it includes only well-tested operating system features. No issue has yet been detected from testing PI Server compatibility with Microsoft security patches.

Microsoft Security Patch Compatibility

<https://customers.osisoft.com/s/knowledgearticle?knowledgeArticleUrl=MS-Security-Patch-Compatibility>

Goal summary

Secure by design initiatives are worth the effort. Risk of attack is lower and cost to address residual risk is lower. We will continue with secure by design innovations.



Call to action

Reminder to discuss mitigation for this known exploited issues with your IT leaders

- **CVE-2013-3900** WinVerifyTrust Signature Validation Vulnerability
- Windows update is insufficient, opt-in registry setting is required for protection
- Subscribe to KEV bulletins from CISA
- Most concerning known exploited issues are operating system and security device related

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

[Home](#)

Known Exploited Vulnerabilities Catalog



Bryan Owen PE

Head of Product Security

- AVEVA
- bryan.owen@aveva.com

Engineers' Creed: As a Professional Engineer, I dedicate my professional knowledge and skill to the advancement and betterment of human welfare. I pledge: To give the utmost of performance; To participate in none but honest enterprise; To live and work according to the laws of man and the highest standards of professional conduct; To place service before profit, the honor and standing of the profession before personal advantage, and the public welfare above all other considerations.

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!

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 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