



The Future of Zero Trust Applications

Ubiquitous Compartmentalization
SpillProof™ Documents

Nat Bongiovanni – CTO
NTT DATA
Federal Subsidiary

August 2024

© 2024 NTT DATA, Inc.

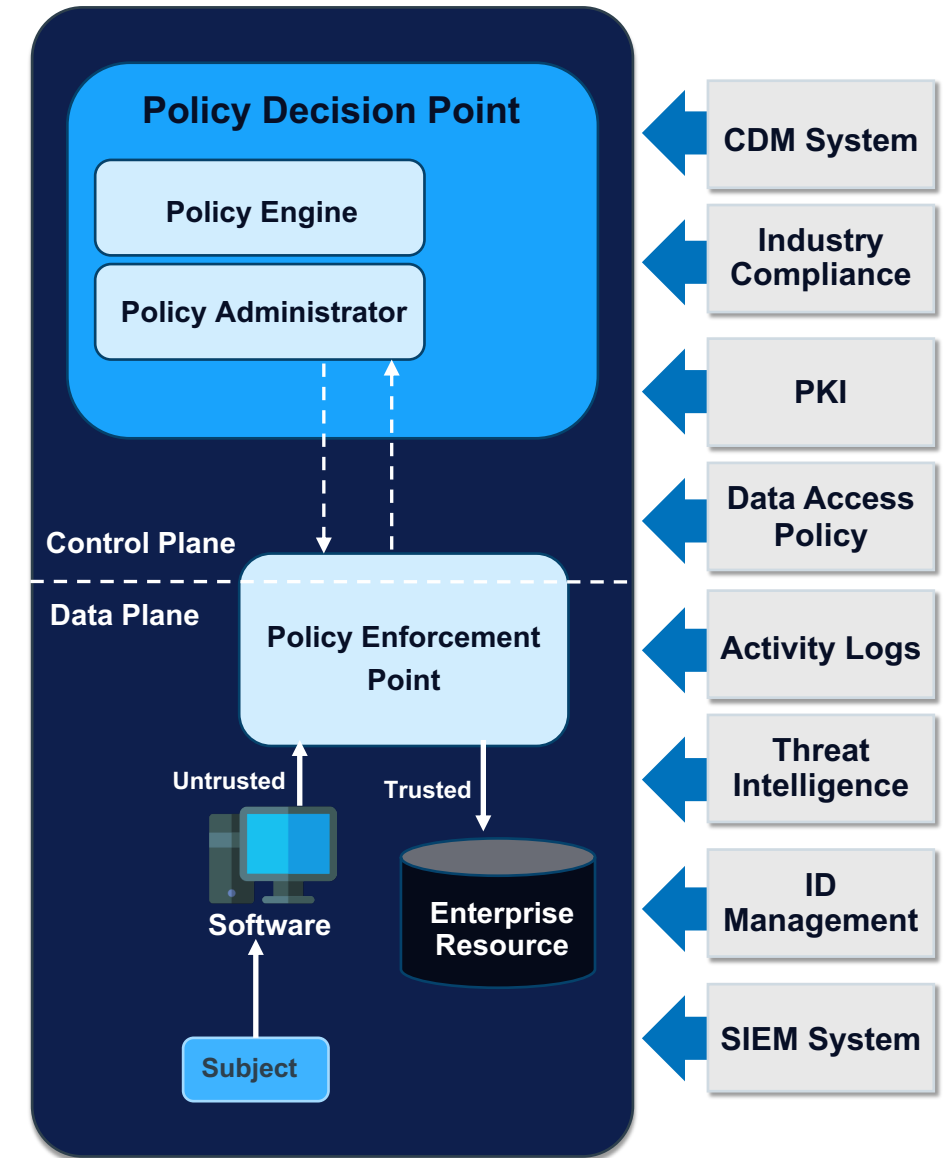


Nat Bongiovanni

Chief Technology Officer
Chief Information Officer
Technology Control Officer

NIST 800-207 – Zero Trust Architecture

- Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary.
- Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.



Core Zero Trust Logical Components

Seven Tenets of Zero Trust Architecture

Authentication

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

Monitoring

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

Authorization

3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

From the National Institute of Standards

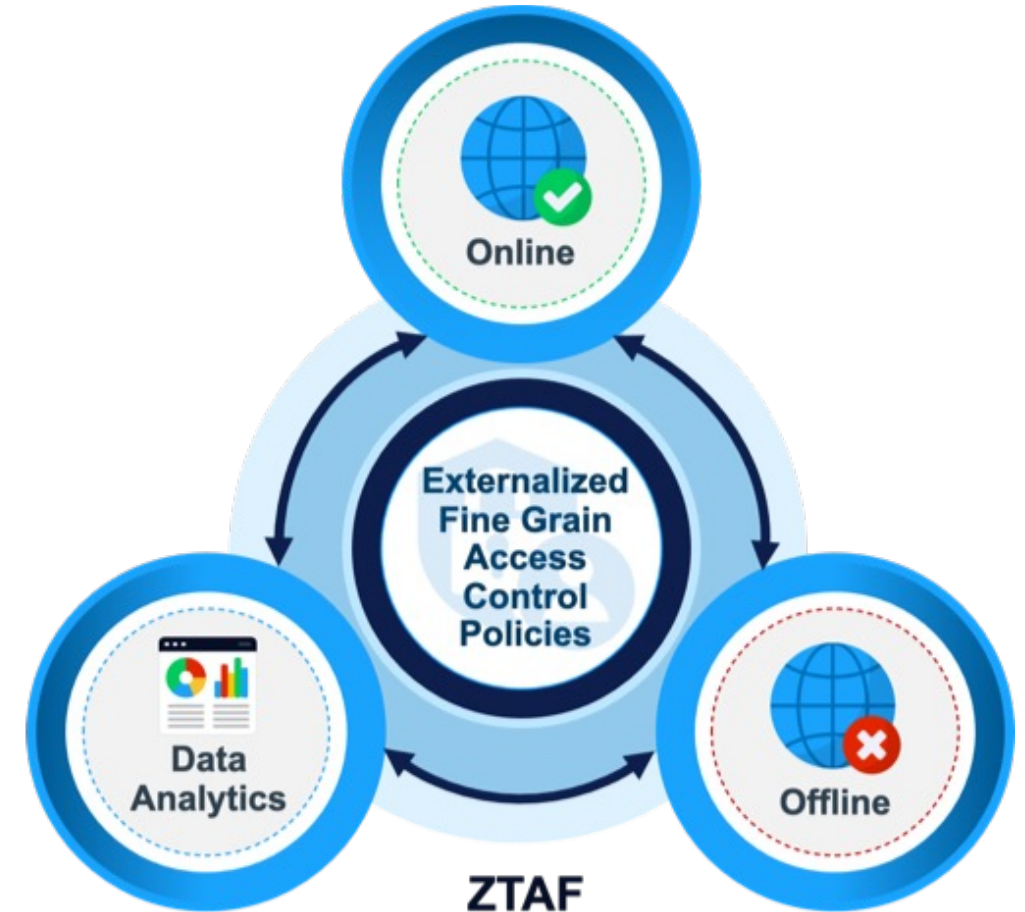
What does a ZTA compliant application look like?

- NIST 800-204a - Building Secure Microservices-based Applications using Service-Mesh Architecture
- NIST 800-204b - Attribute-based Access Control for Microservices-based Applications using a Service Mesh
- NIST 800-204c - Implementation of DevSecOps for a Microservices-based

NIST 800-207 – Zero Trust Architecture

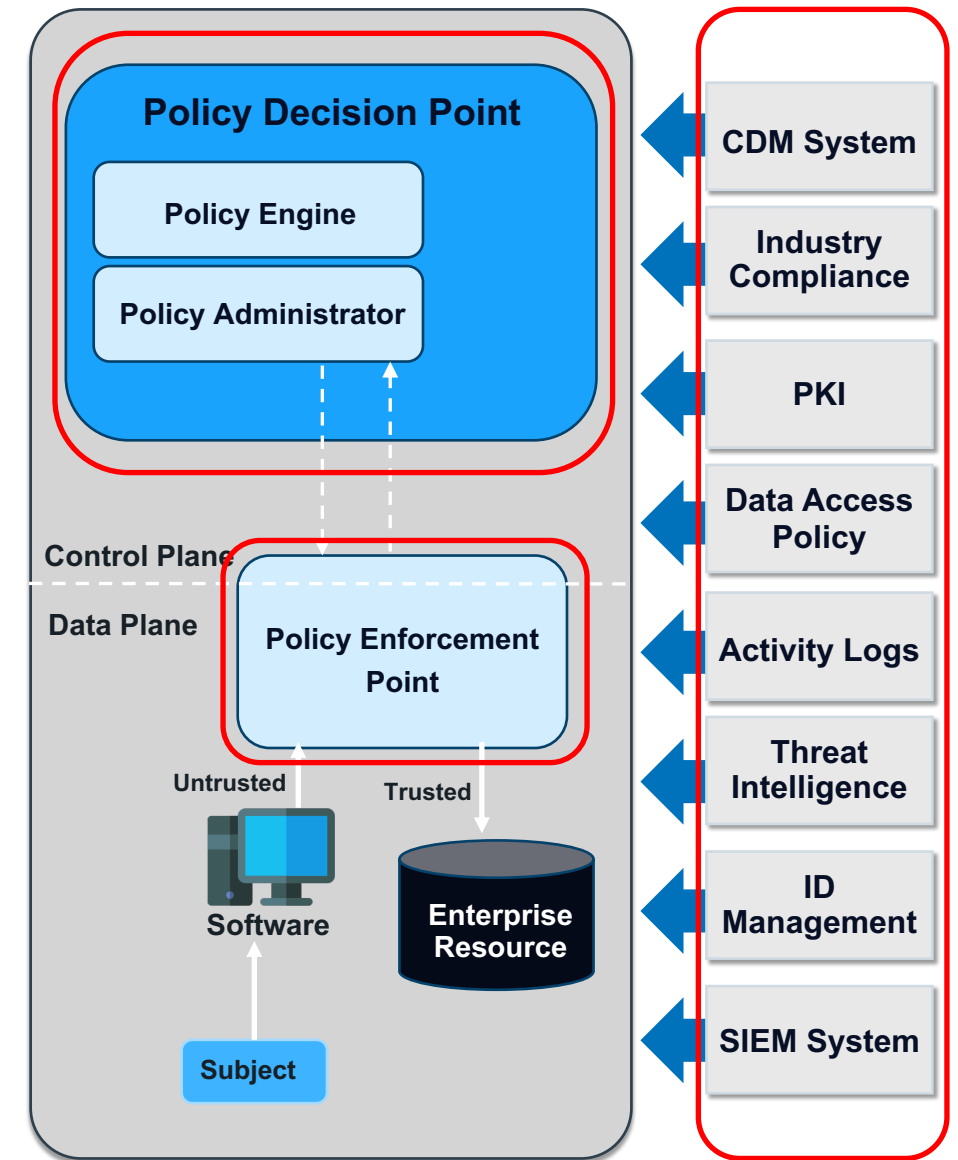
Elements of the Zero Trust Application Framework (ZTAF)

- Focused on meeting all requirements for applications based on:
 - NIST SP 800-207
 - NIST SP 800-204 a, b, c, d
- Provides framework for online, data analytics, & offline files that align with ZTA
- Also provides externalized fine grain access control across the board



ZTAF at a Conceptual Level

- Zero Trust Architecture
 - PDP
 - PEP
 - Inputs
- Enable Ubiquitous Compartmentalization
 - Explanation of Compartments
 - Cartesian Product Example
 - Attributes of Agencies (5), Security Levels (4), Job Roles (2), Countries (49)
 - Potentially 1,960 compartments based on those attributes



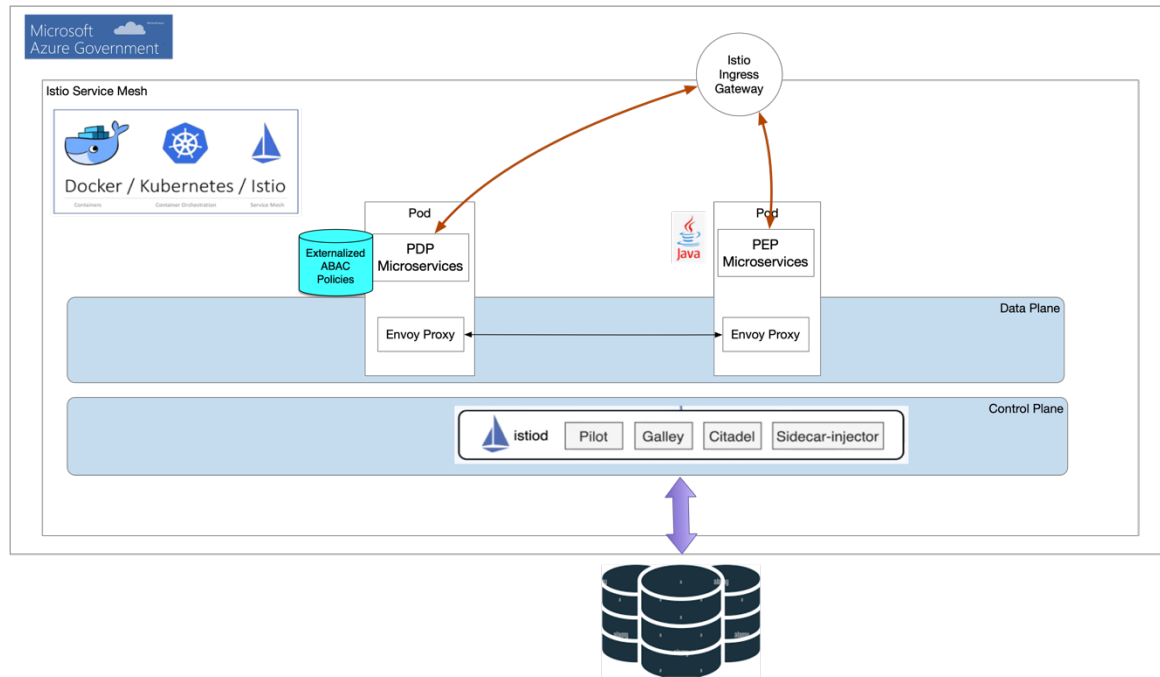
Core Zero Trust Logical Components

Factories mechanize the work of craftsmen

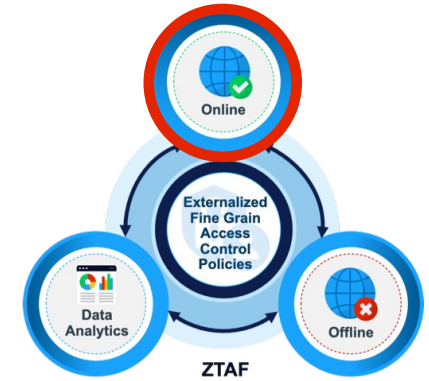
What parts of the factory analogy are we trying to adopt?

ZTAF Instantiated

Think Big, Start Small, Scale Smartly™

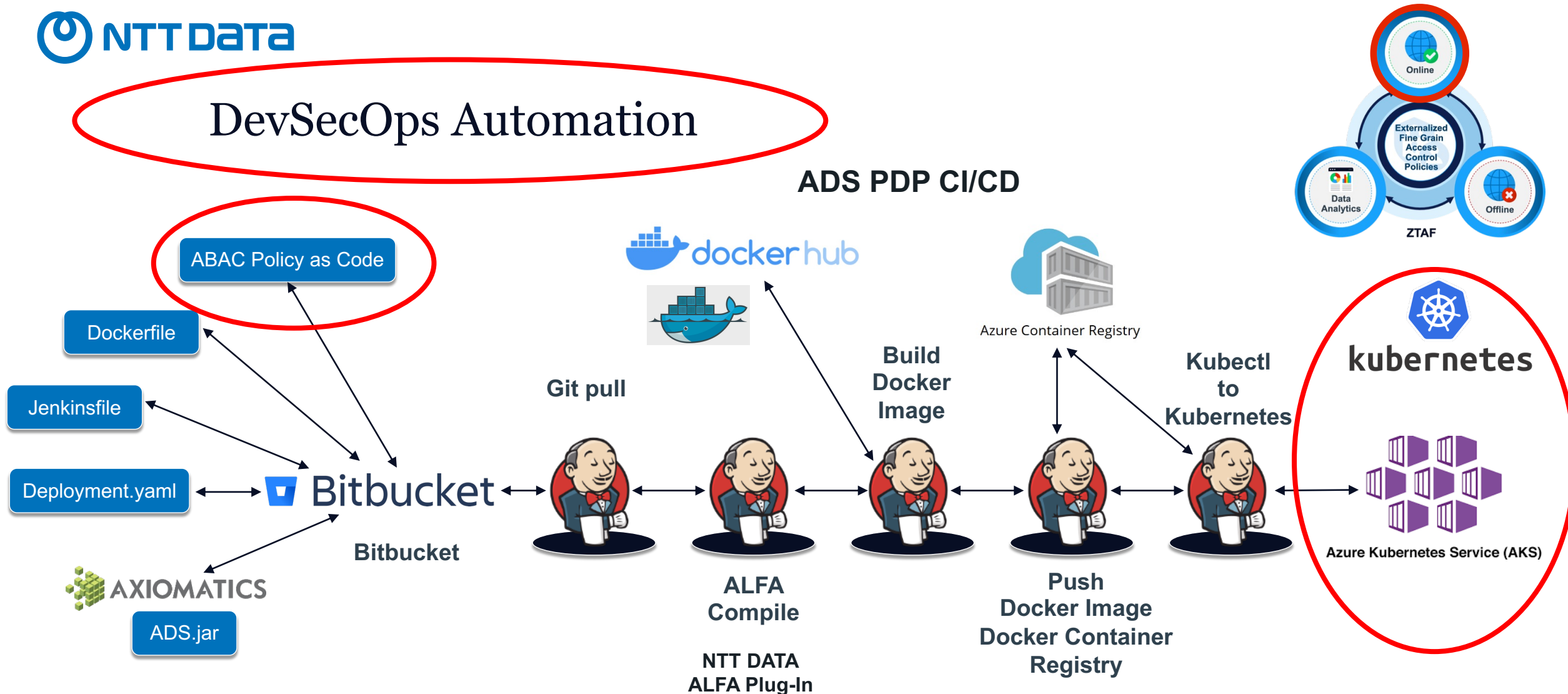


- Cloud Native
 - GovCloud
 - Istio Service Mesh, Ingress Gateway
 - Kubernetes orchestration
 - Docker containers
- Fine Grain Access Control
 - Microservices
 - Policy Enforcement Points (PEP)
 - *Policy Decision Points (PDP)*
 - *For Both APIs and Data Access*
- Modern User Interface Technologies



DevSecOps Automation

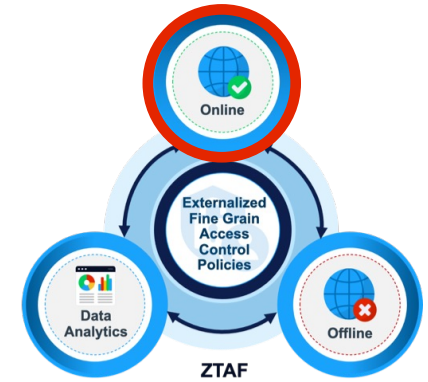
ADS PDP CI/CD



Policy Decision Point (PDP) Continuous Integration(CI)/Continuous Deployment (CD) Pipeline

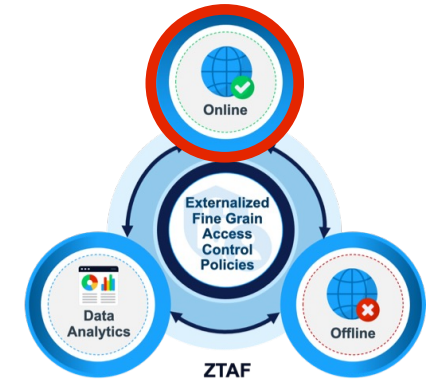
Modernization/Reimagination of a Legacy Applications using ZTAF for Foreign Military Sales (FMS)

- Legacy Mainframe applications for one Implementation Agency (IA)
- Complex access control policies embedded in the legacy code
 - Hidden everywhere in the Natural COBOL Online, Job Control, Batch Programs
 - No one to maintain it or are too afraid to modernize the system
- Primitive 80 characters CRT user interface
- Need to get to the Cloud, modern architectures and ZTA



Legacy Source Code and UI

Lift and Shift or Code Conversion will result in Legacy UI/UX



```
157 1570INPUT (AD=I)
158 1580/ 'SAMIS' 8X '-' *OUT #WHOLEDATE'TIME:' *OUT #TIME 65T 'MDD:' *OUT +MDD
159 1590/          62T 'OFFICE:' *OUT +OFFICE
160 1600/ '*'(4) 'COMPARISON OF ORIGINAL REQUISITION PRICES TO DELIVERED PRICES'
161 1610  '-' *OUT +QUICK-ACCESS-ID (AD=I) '*'(4)
162 1620// 6T 'ENTER SELECTION PARAMETER:' *OUTIN #SEL-PARM
163 1630/ 9T 'A. COUNTRY, CASE, LINE ITEM'
164 1640/ 9T 'B. COUNTRY, CASE'
165 1650/ 9T 'C. COUNTRY'
166 1660/ 9T 'D. STOCK NUMBER'
167 1670// 6T 'ENTER SELECTION DATA AS NEEDED:'
168 1680/ 6T 'COUNTRY' *OUTIN #COUNTRY 'CASE' *OUTIN #CASE 'LINE ITEM' #LI
169 1690  'STOCK NUMBER' #STK-NR 'RIC' #RIC-IN
170 1700// 6T 'ENTER PRODUCT SEQUENCE:' *OUTIN #PROD-SEQ
171 1710/ 9T '1. STOCK NUMBER, COUNTRY, CASE, LINE ITEM, DOCUMENT NUMBER'
172 1720/ 9T '2. COUNTRY, CASE, LINE ITEM, STOCK NUMBER, DOCUMENT NUMBER'
173 1730// '*' (79)
174 1740// '**ALTERNATE OPTION:' *IN #ALT-OPT
175 1750  'QUICK ACCESS ID OR H-HELP, Q-QUIT, R-RETURN TO TOP**'
176 1760*      GET VALID COMPARISON OF ORIGINAL REQUISITION PRICES TO
177 1770*      DELIVERED PRICES INTERROGATIONS
```

```
MAIN                                IBM i Main Menu                                System:

Select one of the following:

    1. Country, Case, Line Item
    2. Country Case
    3. Country
    4. Stock Number

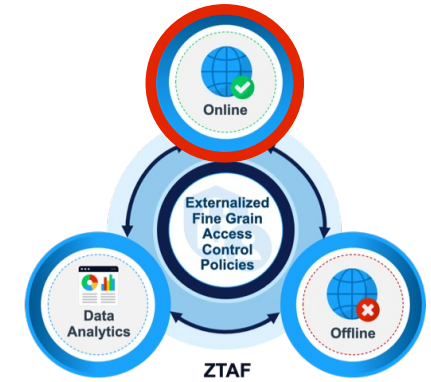
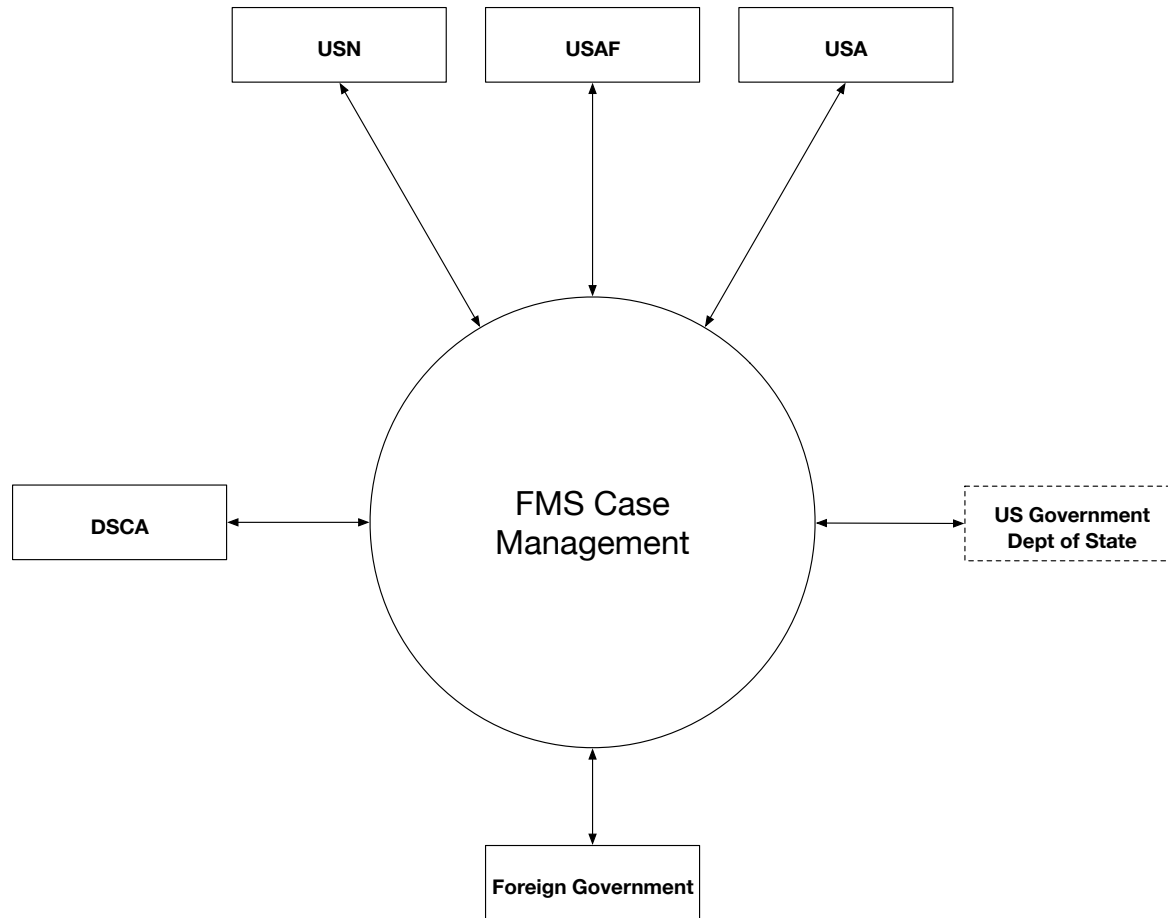
Country: _____
Case:    _____
Line Item: _____
Stock Number: _____

90. Sign off

Selection or command
==> █

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2009.
ONLINE                                M 20,7
```

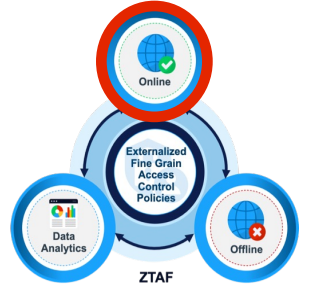
Reimagined based on Application's Ecosystem



- Implementation Agencies have similar functional requirements, can we build one system for all Implementation Agencies?
 - Ecosystem includes
 - Defense Security Cooperation Agency (DSCA)
 - Department of State
 - Foreign Governments (customers)
- Can we include these partners directly into core system?

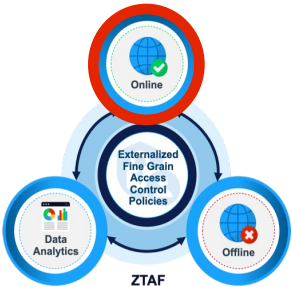
ABAC Policy in English

Externalized Fine-Grain Access Controls



- FMS Case Representatives (CaseReps) can only **view** transactions.
- CaseReps can only access transactions from their own *Implementation Agency* [Army, Navy, USAF] that occurred within the **last** year.
- *Implementation Agency* Officer can **read** and **edit** transactions from their own Implementation Agency.
- Only **active** Subjects should be allowed access to the FMS Portal.
- Defense Security Cooperation Agency (DSCA) CaseRep can **read** all transactions from any of the Implementation Agencies.
- DSCA Officer can **read and edit** all transactions.
- Dept of State can only read all transactions
- Foreign Governments can only read their own cases
- **Subject** can only access Cases with Security Access Level **At or Below** the Subject's Security Access Level assignment

FMS Case Management System - ABAC



NTT DATA FMS Case Tracker		Welcome Officer.DSCA					SIGN OUT	
Army FMS Cases		ARMY	NAVY	AIR FORCE	ENCRYPT	DECRYPT	Search...	
Title	Country	Date	Estimated Cost	Year	Notification Number	Implementation Agency	Security Level	
Australia - Heavy Armored Combat Systems	Australia	29-Apr-2021	\$1,685M	2021	21-40	Army	Yellow	
Australia - AH-64E Apache Helicopters - Change	Australia	3-Jun-1970	\$3,500M	1970	21-42	Army	Red	
Australia - Defense Services Related to Future Stand	Australia	25-Aug-2022	\$350M	2022	21-25	Army	Orange	
Australia - MH-60R Multi-Mission Helicopters, Related	Australia	8-Oct-2022	\$985M	2022	21-61	Army	Orange	
Australia - Hellfire AGM-114R2 Missiles	Australia	20-Dec-2022	\$108M	2022	21-60	Army	Green	
Finland - Extended Range Guided Multiple Launch Rc	Finland	17-Feb-2022	\$91M	2022	21-16	Army	Green	
Georgia - Javelin Missiles	Georgia	3-Aug-2022	\$30M	2022	21-48	Army	Yellow	
Greece - FMSO II, CLSSA Services - Changed	Greece	19-May-2021	\$165M	2021	21-39	Army	Orange	
Israel - CH-53K Heavy Lift Helicopters With Support	Israel	30-Jul-2022	\$3,400M	2022	21-52	Army	Orange	
Kuwait - Heavy Tactical Vehicles	Kuwait	1-Jul-2022	\$445M	2022	20-85	Army	Red	

SpillProof™

What is a SpillProof™ document and how is it encrypted and Decrypted?

- Based on advanced cryptography described by Brent Waters and Ami Sahai in 2005 called **Attribute Based Encryption**
- Access policy is embedded into the encryption
- Multiple keys could exist for a given ciphertext to enable **different users** to access **different parts** of the underlying dataset with attribute-based access control policy. **In essence ABAC inside the file.**

NTT Data Attribute Based Encryption Protected

Spill-Proof Document

Decryption Attributes

Level RED, Implementation Agency: Navy, Country: None

Foreign Military Sales Cases

TOP SECRET

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC

MEMORANDUM FOR DASD (I&S) JUNE 15, 2024

SUBJECT: Security Awareness of Classification Markings

1. [REDACTED]

2. (S) This is paragraph 2 which contains [REDACTED] therefore be marked with the declassification marking (S)

3. (C) This is paragraph 3 which contains [REDACTED] therefore be marked with the declassification marking (C)

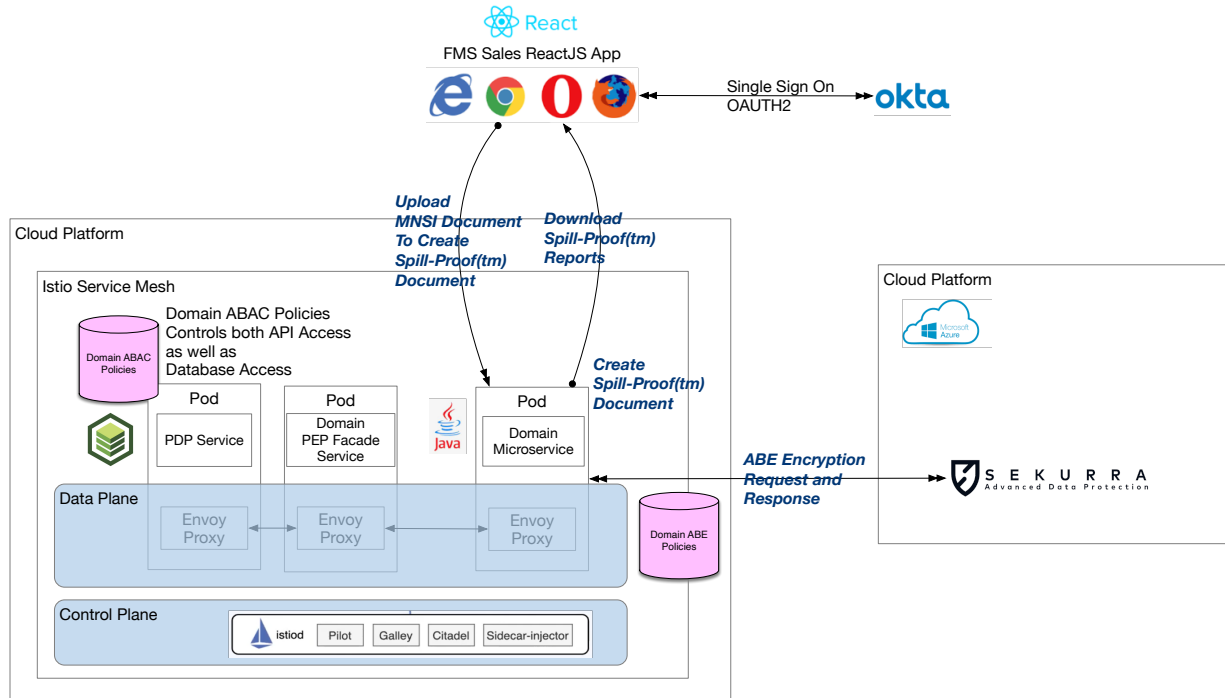
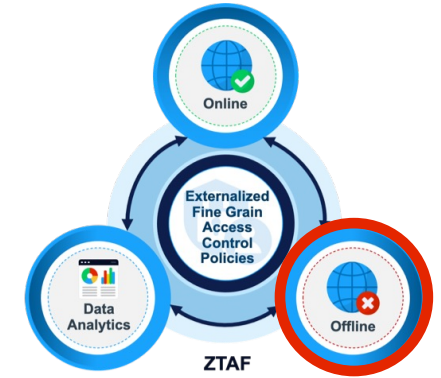
4. (U) This is paragraph 4 which contains [REDACTED] therefore be marked with the declassification marking (U)

Title	Implementation Agency	Security Access Level
Canada - AEGIS Combat System	Navy	Secret
Chile - Standard Missile-2 (SM-2) Block IIIA Missiles	Navy	Secret
Germany - P-8A Aircraft and Associated Support	Navy	Secret
Greece - Multi-Mission Surface Combatant (Hellenic Future Frigate (HF2))	Navy	Secret
Greece - MEKO Class Frigate Modernization	Navy	Secret
India - P-8I and Associated Support	Navy	Secret
India - Harpoon Joint Common Test Set (JCTS)	Navy	Secret
Japan - AEGIS Class Destroyer Support	Navy	Secret

Classified by: Multiple Sources Declared
On: OADR

SpillProof™ Architecture Concept Patent Pending

Leveraging Attribute Based Encryption (ABE) for Offline Resource Protection

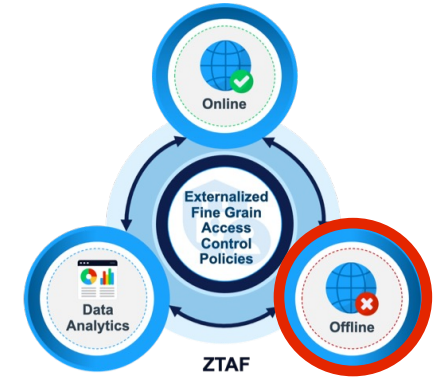


- NTT DATA (Federal Subsidiary)
 - Cloud Native ABAC Based Application
- NTT DATA (Federal Subsidiary)
 - **Cerberus**™: Encryption/Decryption Service
 - Soteria™: ABAC to ABE Policy Manager
- NTT DATA (Commercial)
 - Sekurra™ ABE Service
- NTT Research ABE Encryption Library

Derived ABE Policy as code

We have a demonstration application based on Foreign Military Sales. In that application we can set up policies that use Soteria™ to convert the ABAC policies to ABE policies. From the user perspective it looks something like this:

- Subject's Agency is the same as FMS Case's Agency
- Subject's Security Access Level is higher than or equal to FMS Case's Security Access Level
- Subject's Country Access is defined by a combination of Subject's Agency and Country



FMS Case Management System - ABAC

NTT DATA
Trusted Global Innovator

FMS Case Tracker

Welcome Officer.DSCA

SIGN OUT

Army FMS Cases

ARMYNAVYAIR FORCE

ENCRYPTDECRYPT

Search...

Title	Country	Date	Estimated Cost	Year	Notification Number	Implementation Agency	Security Level
Australia - Heavy Armored Combat Systems	Australia	29-Apr-2021	\$1,685M	2021	21-40	Army	Yellow
Australia - AH-64E Apache Helicopters - Change	Australia	3-Jun-1970	\$3,500M	1970	21-42	Army	Red
Australia - Defense Services Related to Future Stand	Australia	25-Aug-2022	\$350M	2022	21-25	Army	Orange
Australia - MH-60R Multi-Mission Helicopters, Related	Australia	8-Oct-2022	\$985M	2022	21-61	Army	Orange
Australia - Hellfire AGM-114R2 Missiles	Australia	20-Dec-2022	\$108M	2022	21-60	Army	Green
Finland - Extended Range Guided Multiple Launch Rc	Finland	17-Feb-2022	\$91M	2022	21-16	Army	Green
Georgia - Javelin Missiles	Georgia	3-Aug-2022	\$30M	2022	21-48	Army	Yellow
Greece - FMSO II, CLSSA Services - Changed	Greece	19-May-2021	\$165M	2021	21-39	Army	Orange
Israel - CH-53K Heavy Lift Helicopters With Support	Israel	30-Jul-2022	\$3,400M	2022	21-52	Army	Orange
Kuwait - Heavy Tactical Vehicles	Kuwait	1-Jul-2022	\$445M	2022	20-85	Army	Red

Generate ABE Encrypted Microsoft Word Document and Excel Spreadsheet

NTT DATA

FMS Case Tracker

Trusted Global Innovator

Welcome Officer.DSCA

SIGN OUT

Army FMS Cases

ARMYNAVYAIR FORCE

ENCRYPTDECRYPT

Search...

Title	Country	Date	Estimated Cost	Year	Notification Number	Implementation Agency	Security Level
Australia - Heavy Armored Combat Systems	Australia	29-Apr-2021	\$1.685M	2021	21-40	Army	Yellow
Australia - AH-64E Apache Helicopters	Australia						Red
Australia - Defense Services Requirements	Australia						Orange
Australia - MH-60R Multi-Mission Helicopters	Australia						Orange
Australia - Hellfire AGM-114R2 Missiles	Australia						Green
Finland - Extended Range Guided Missiles	Finland						Green
Georgia - Javelin Missiles	Georgia						Yellow
Greece - FMSO II, CLSSA Services - Changed	Greece	19-May-2021	\$165M	2021	21-39	Army	Orange
Israel - CH-53K Heavy Lift Helicopters With Support	Israel	30-Jul-2022	\$3,400M	2022	21-52	Army	Orange
Kuwait - Heavy Tactical Vehicles	Kuwait	1-Jul-2022	\$445M	2022	20-85	Army	Red

Encrypt & Download FMS Cases

Document format:

Microsoft Word (.docx)

Microsoft Excel (.xlsx)

Row By Row

CSV Document

Microsoft Word Template

Microsoft Powerpoint Template

SpillProof™ Document - Word

Remember our easy to read policies
Subject's Agency is the same as FMS
Case's Agency - NAVY

Subject's Security Access Level is higher than or equal to FMS Case's Security Access Level - Red

Subject's Country Access is defined by a combination of Subject's Agency and Country – All (None means no restrictions)

Army FMS Cases

Title
Australia - Heavy Armored Combat Systems
Australia - AH-64E Apache Helicopters - C
Australia - Defense Services Related to F
Australia - MH-60R Multi-Mission Helicopt
Australia - Hellfire AGM-114R2 Missiles
Finland - Extended Range Guided Multiple
Georgia - Javelin Missiles
Greece - FMSO II, CLSSA Services - Ch

Subject's Country Access is defined by a combination of Subject's Agency and Country – All (None means no restrictions)

Agency	Country	Access
Israel - CH-53K Heavy Lift Helicopters With Support	Israel	30-Jul-2022 \$3,400M 2022 21-52 Army Orange
Kuwait - Heavy Tactical Vehicles	Kuwait	1-Jul-2022 \$445M 2022 20-85 Army Red

NTT Data Attribute Based Encryption Protected

Spill-Proof Document

Decryption Attributes

Level RED, Implementation Agency: Navy, Country: None

Foreign Military Sales Cases

-
-
-
-
-
-
-
-
- (YELLOW) {Navy} Canada - AEGIS Combat System
- (RED) {Navy} Chile - Standard Missile-2 (SM-2) Block IIIA Missiles
-
-
-
-
-
- (RED) {Navy} Germany - P-8A Aircraft and Associated Support
-
-
-
- (RED) {Navy} Greece - Multi-Mission Surface Combatant (Hellenic Future Frigate (HF2))
- (RED) {Navy} Greece- MEKO Class Frigate Modernization
- (ORANGE) {Navy} India - P-8I and Associated Support

SpillProof™ Document - Excel

Original Online

Decrypted
Subject Attributes

NTT DATA FMS Case Tracker

Welcome Officer.D

Army FMS Cases

ARMYNAVY

Title	Country	Date	Estimated Cost
Australia - Heavy Armored Combat Systems	Australia	29-Apr-2021	\$
Australia - AH-64E Apache Helicopters - Change	Australia	3-Jun-1970	\$
Australia - Defense Services Related to Future Stands	Australia	25-Aug-2022	
Australia - MH-60R Multi-Mission Helicopters, Related	Australia	8-Oct-2022	
Australia - Hellfire AGM-114R2 Missiles	Australia	20-Dec-2022	
Finland - Extended Range Guided Multiple Launch Rc	Finland	17-Feb-2022	
Georgia - Javelin Missiles	Georgia	3-Aug-2022	
Greece - FMSO II, CLSSA Services - Changed	Greece	19-May-2021	
Israel - CH-53K Heavy Lift Helicopters With Support	Israel	30-Jul-2022	\$
Kuwait - Heavy Tactical Vehicles	Kuwait	1-Jul-2022	

	A	B	C	
1	NTT Data Attribute Based Encryption Protected			
2	Spill-Proof Document			
3	Decryption Attributes			
4	Level RED, Implementation Agency Navy, Country None			
5	Foreign Military Sales Cases			
6				
7				
8	Title	Implementation Agency	Security Access Level	
9	██	████████████████████	████████████████████	████████
10	██	████████████████████	████████████████████	████████
11	██	████████████████████	████████████████████	████████
12	██	████████████████████	████████████████████	████████
13	██	████████████████████	████████████████████	████████
14	██	████████████████████	████████████████████	████████
15	██	████████████████████	████████████████████	████████
16	██	████████████████████	████████████████████	████████
17	Canada - AEGIS Combat System	Navy	Yellow	
18	Chile - Standard Missile-2 (SM-2) Block IIIA Missiles	Navy	Red	
19	██	████████████████████	████████████████████	████████
20	██	████████████████████	████████████████████	████████
21	██	████████████████████	████████████████████	████████
22	██	████████████████████	████████████████████	████████
23	Germany - P-8A Aircraft and Associated Support	Navy	Red	
24	██	████████████████████	████████████████████	████████
25	██	████████████████████	████████████████████	████████
26	Greece - Multi-Mission Surface Combatant (Hellenic Future Frigate (HF2))	Navy	Red	
27	Greece- MEKO Class Frigate Modernization	Navy	Red	
28	India - P-8I and Associated Support	Navy	Orange	
29	India - Harpoon Joint Common Test Set (JCTS)	Navy	Green	
30	██	████████████████████	████████████████████	████████
31	Japan - AEGIS Class Destroyer Support	Navy	Orange	
32	██	████████████████████	████████████████████	████████

SpillProof™ Documents

- Marking National Security Information (MNSI)

MNSI – Basic Portion Markings Example

TOP SECRET
For TRAINING ONLY

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC

MEMORANDUM FOR DASD (I&S) JUNE 15, 2024

SUBJECT: Security Awareness of Classification Markings

1. (TS) This is paragraph 1 which contains "Top Secret" information. This portion will therefore be marked with the designation "TS" in parentheses.
2. (S) This is paragraph 2 which contains "Secret" information. This portion will therefore be marked with the designation "S" in parentheses.
3. (C) This is paragraph 3 which contains "Classified" information. This portion will therefore be marked with the designation "C" in parentheses.
4. (U) This is paragraph 4 which contains "Unclassified" information. This portion will therefore be marked with the designation "U" in parentheses.

ASD (C31)

Classified by: Multiple Sources Declassify
On: OADR

Single Attributes
For ABE Policies

MNSI – Special Access Required (SAR) Portion Markings Example

UNCLASSIFIED
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

Special Access Program Markings ShortStudent Guide

Portion Markings

Don the Document: Next, we have portion markings, which identify the classification levels of individual sections of a document. Here is one example of what they may look like.

Examples of portion markings

(U) (C) (S) (TS) (U//FOUO) (S//NF/PROPIN)
(C//FRD) (//GBR S) (TS//SI/TK) (S//RD)
(S//REL) (TS//REL TO USA, AUS, CAN, GBR) (S//RD-N)

Here is another example to see how some of the abbreviations are made.

Sample Banner Line	Related Portion Marking
SECRET//SPECIAL ACCESS REQUIRED-TAXI GREY	(S//SAR-TG)
TOP SECRET//SAR-TIN BAKER//WAIVED	(TS//SAR-TB//WAIVED)
SECRET//SAR-BLUE FOG//SAR-MUDDY PATH	(S//SAR-BFG/SAR-MDP)
TOP SECRET//SAR-STAGGER/SAR-TIN BAKER//WAIVED	(TS//SAR-SGR/SAR-TB//WAIVED)
SECRET//SAR-MULTIPLE PROGRAMS	(S//SAR-AB/SAR-DGR/SAR-WZ)
TOP SECRET//SAR-MULTIPLE PROGRAMS//WAIVED	(TS//SAR-BP/SAR-STK/SAR-TG//WAIVED)

In materials that include SAP information, the portion markings include not only the classification level, but also that the information is Special Access Required, which is denoted in the portion by the abbreviation SAR.

The level of classification in the caveat Special Access Required, or SAR, is separated by a double slash.

The program identifier (PID) for each SAP mentioned must also be cited in the portion marking, regardless of the total number of PIDs. Use a hyphen without spaces to separate the SAR caveat and the PID. When multiple PIDs are listed, list them in alphabetical order and separate

UNCLASSIFIED
CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY

September 2020Center for Development of Security ExcellencePage 4

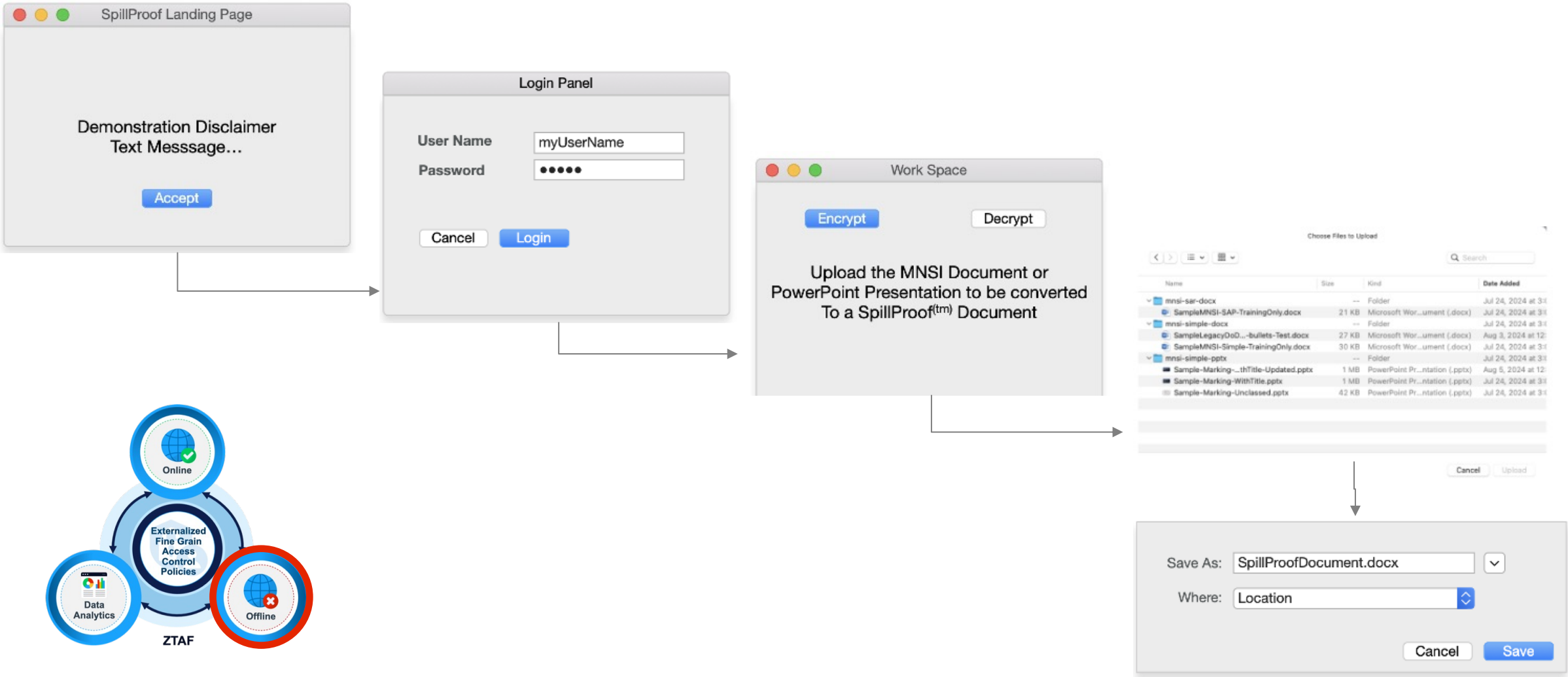
Multiple Attributes
For ABE Policies

© 2024 NTT DATA, Inc.

NTT DATA

How do we transform existing MNSI Documents into SpillProof™ Documents?

Convert Microsoft Word and PowerPoint with MNSI Markings



Microsoft Word with MNST Basic to SnillProof™ Document

TOP SECRET

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC

Original

MEMORANDUM FOR DASD (I&S) JUNE 15, 2024

TOP SECRET

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC

MEMORANDUM FOR DASD (I&S) JUNE 15, 2024

SUBJECT: Security Awareness

1. (TS) This is paragraph 1 which contains information that will therefore be marked with the designation "TS" in parentheses.
2. (S) This is paragraph 2 which contains information that will therefore be marked with the designation "S" in parentheses.
3. (C) This is paragraph 3 which contains information that will therefore be marked with the designation "C" in parentheses.
4. (U) This is paragraph 4 which contains information that will therefore be marked with the designation "U" in parentheses.

ASD (C)

ASD (C31)

Classified by: Multiple Sources Declassify
On: OADR

Classified by: Multiple Sources Declassify
On: OADR

Decrypted

TOP SECRET

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC

MEMORANDUM FOR DASD (I&S) JUNE 15, 2024

SUBJECT: Security Awareness of Classification Markings

1. (TS) This is paragraph 1 which contains information that will therefore be marked with the designation "TS" in parentheses.
2. (S) This is paragraph 2 which contains "Secret" information. This portion will therefore be marked with the designation "S" in parentheses.
3. (C) This is paragraph 3 which contains "Classified" information. This portion will therefore be marked with the designation "C" in parentheses.
4. (U) This is paragraph 4 which contains "Unclassified" information. This portion will therefore be marked with the designation "U" in parentheses.

ASD (C31)

Classified by: Multiple Sources Declassify
On: OADR

Microsoft PowerPoint with MNSI Basic to SpillProof™ Presentation

Sample Marking PPTX

1. [REDACTED]
2. (S) This is Bullet 2 which contains "Secret" information. This portion will therefore be marked with the designation "S" in parentheses.
3. (C) This is Bullet 3 which contains "Classified" information. This portion will therefore be marked with the designation "C" in parentheses.
4. (U) This is Bullet 4 which contains "Unclassified" information. This portion will therefore be marked with the designation "U" in parentheses.

Spill-Proof™ Document: Decrypted with Secret (S) Access Level

Why do we need SpillProof™ Documents?

- Protecting National Security Information
- Ubiquitous Compartments based on "Need to Know" –
- Protects from Insider Threats like:
 - Jack Teixeira
 - Chelsea Manning
- Sharing of Information Across Domains/Organizations
- Sharing sensitive information in other organizations such as
 - Electronic Health Records
 - Manufacturing schematics/designs with sensitive components
 - Etc.

