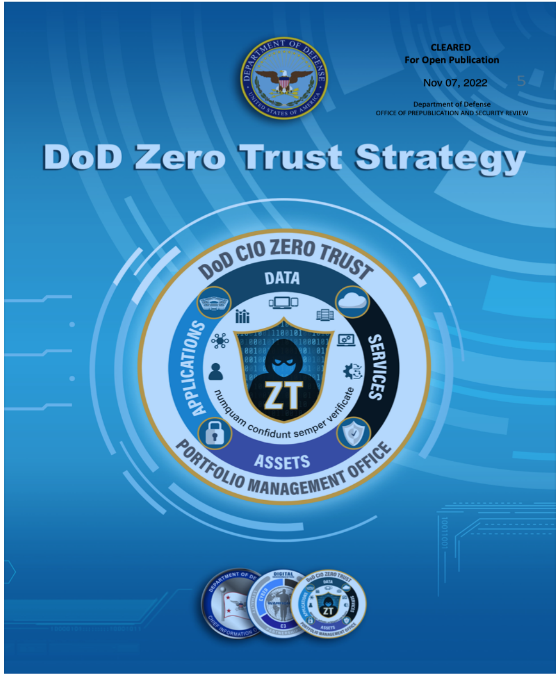
Introduction To Zero Trust Data

New Security Architecture From The
US Department Of Defense

Presented By Junaid Islam

What Is Zero Trust Data?



CLEARED
For Open Publication

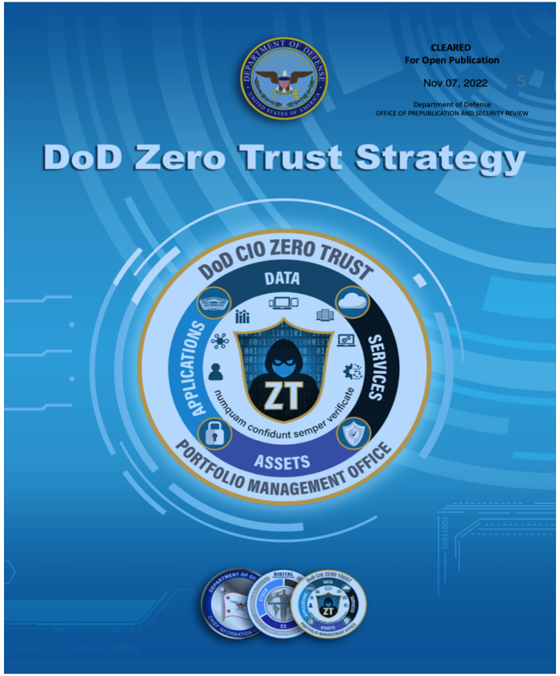
Nov 07, 2022

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Zero Trust Strategy

DoD CIO ZERO TRUST
DATA
SERVICES
ASSETS
APPLICATIONS
ZT
numquam confidunt semper verificate
PORTFOLIO MANAGEMENT OFFICE

What Is Zero Trust Data? REVOLUTIONARY!!!



CLEARED
For Open Publication

Nov 07, 2022

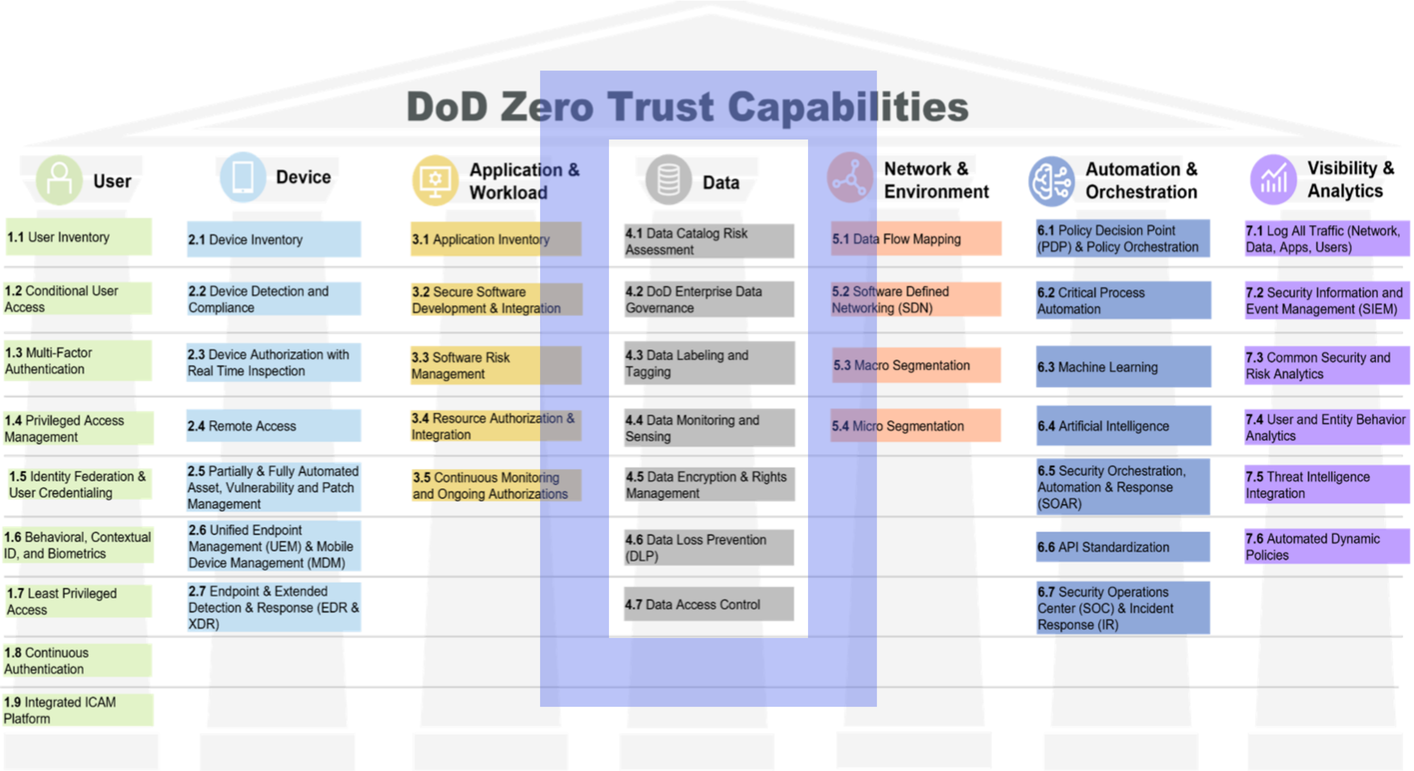
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Zero Trust Strategy

DoD CIO ZERO TRUST
DATA
SERVICES
APPLICATIONS
ZT
numquam confidunt semper verificate
ASSETS
PORTFOLIO MANAGEMENT OFFICE

- Integrates VPN and File Encryption Functionality
- Supports Decentralized Key Control
- Tracks Movement Of Data And Access To It

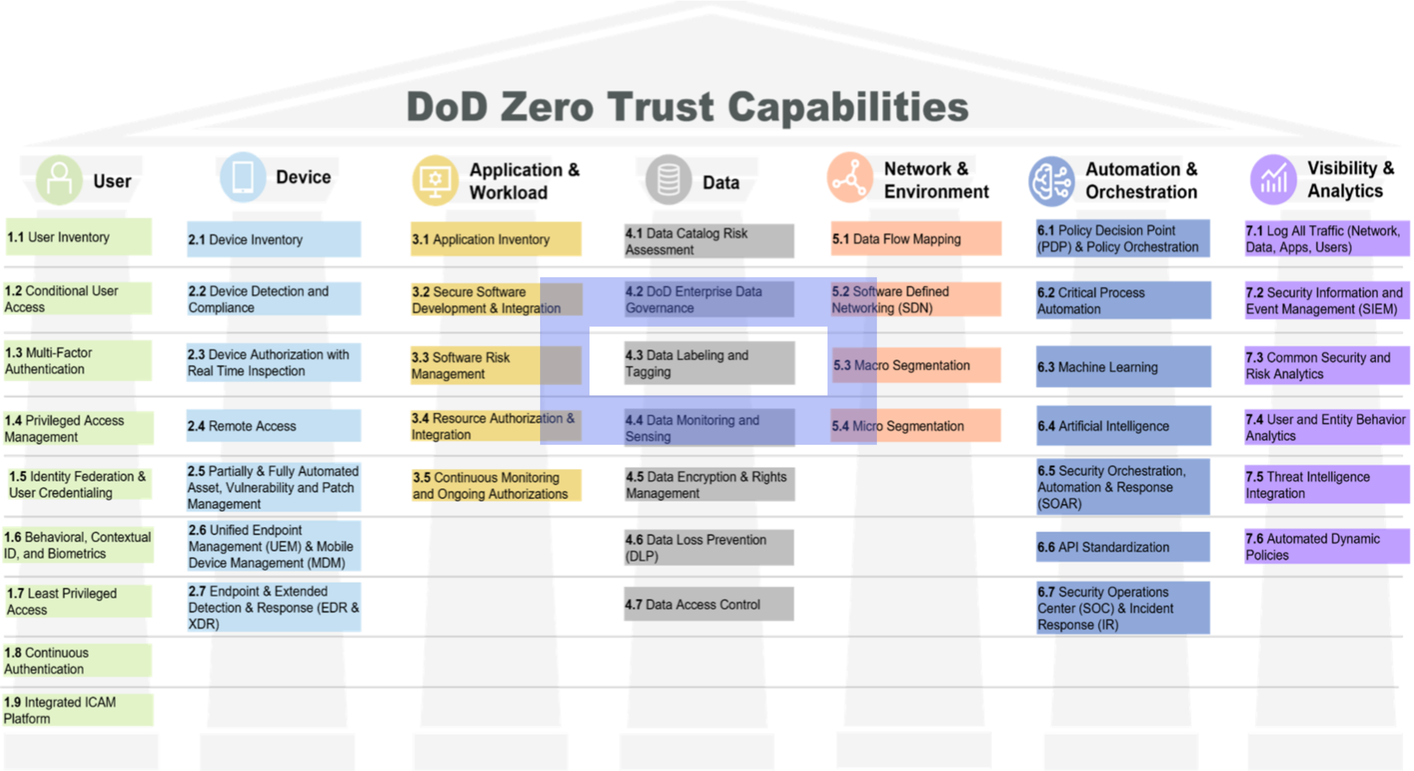
Enabling Technology:



DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	6.1 Policy Decision Point (PDP) & Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection and Compliance	3.2 Secure Software Development & Integration	4.2 DoD Enterprise Data Governance	5.2 Software Defined Networking (SDN)	6.2 Critical Process Automation	7.2 Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	2.3 Device Authorization with Real Time Inspection	3.3 Software Risk Management	4.3 Data Labeling and Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security and Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	4.4 Data Monitoring and Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	3.5 Continuous Monitoring and Ongoing Authorizations	4.5 Data Encryption & Rights Management		6.5 Security Orchestration, Automation & Response (SOAR)	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Detection & Response (EDR & XDR)		4.7 Data Access Control		6.7 Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

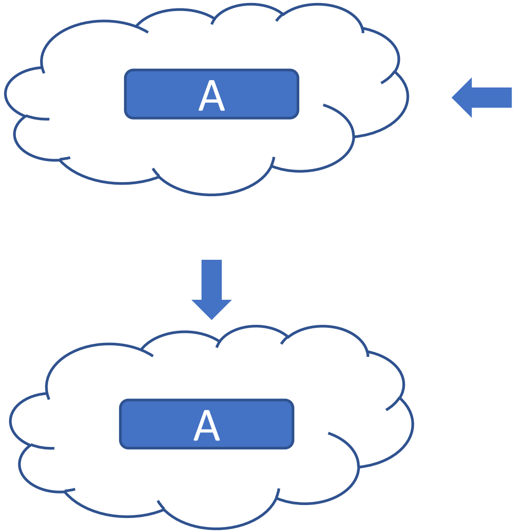
Enabling Technology: Dynamic Labeling



DoD Zero Trust Capabilities

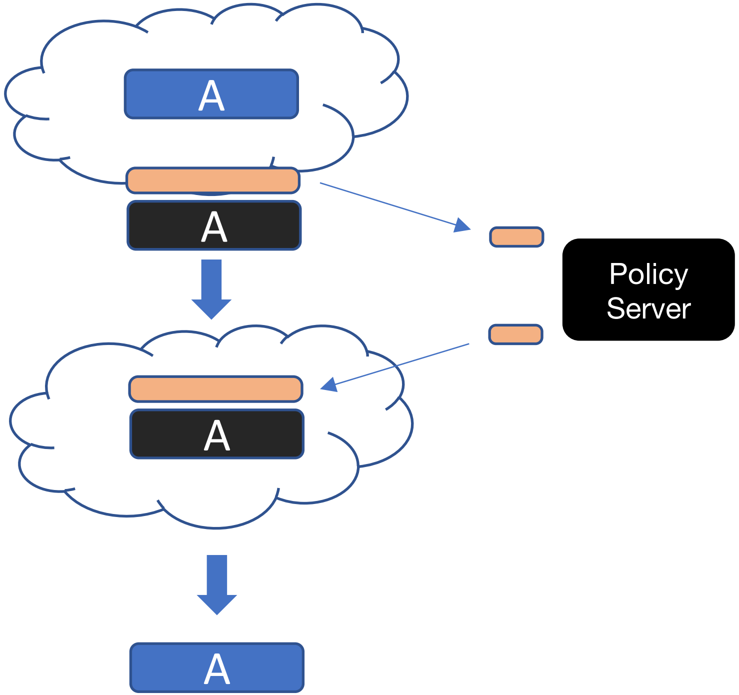
User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Short History Of Dynamic Labeling

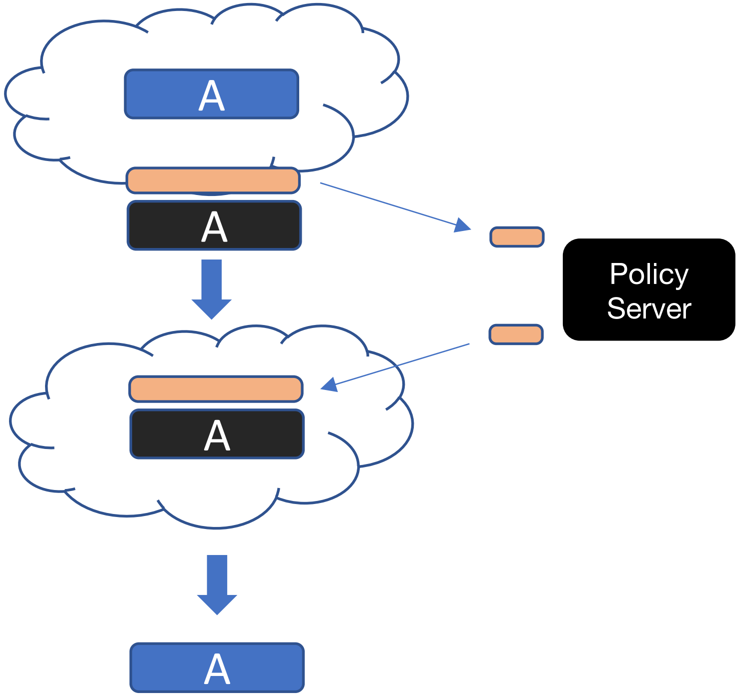


How do you securely access a piece of Mobile Data or Mobile Device or Warfighter?

Short History Of Dynamic Labeling



Short History Of Dynamic Labeling



Netcentric Warfare DoD

Connecting Mobile Devices

2002-2004

C2S Access Control IC

Encrypting Mobile Data

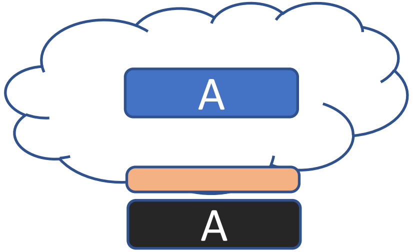
2012-2016

Zero Trust Data DoD

Moving Data Between Systems

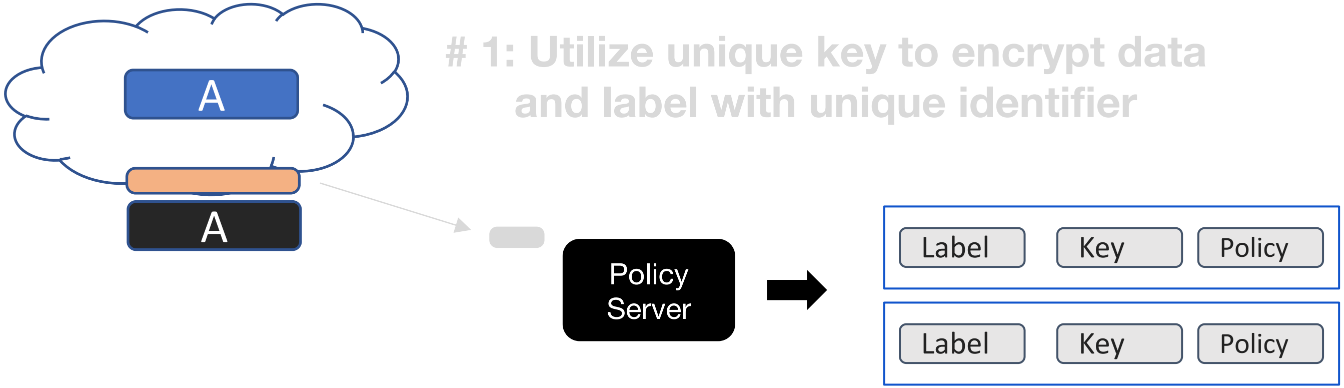
2020- 2022

Zero Trust Data Workflow



# 1: Utilize unique key to encrypt data and label with unique identifier

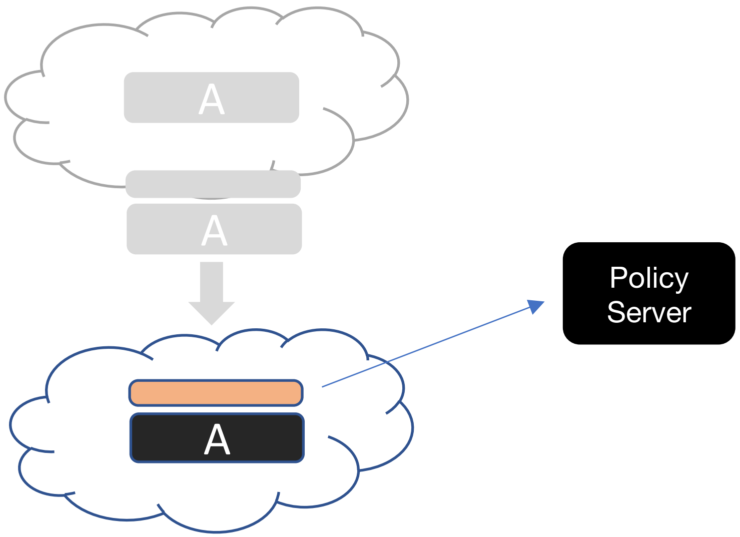
Zero Trust Data Workflow



# 1: Utilize unique key to encrypt data and label with unique identifier

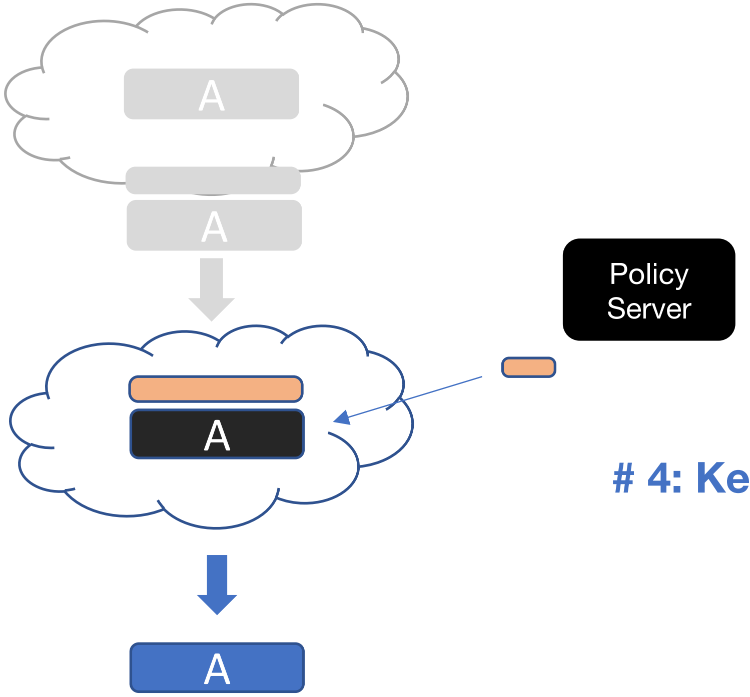
# 2: Post Label + Key To Policy Server with Access Conditions

Zero Trust Data Workflow



# 3: Label utilized to identify policy server holding key

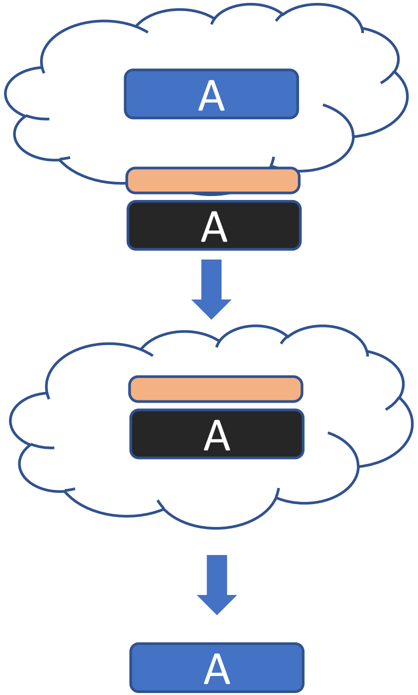
Zero Trust Data Workflow

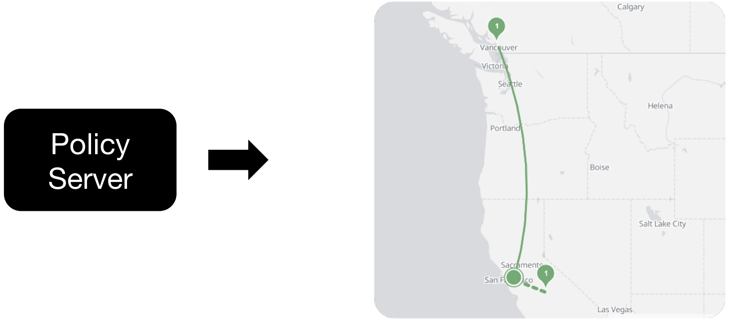


# 3: Label utilized to identify policy server holding key

# 4: Key transmitted to requestor if policy challenge met

Zero Trust Data Workflow



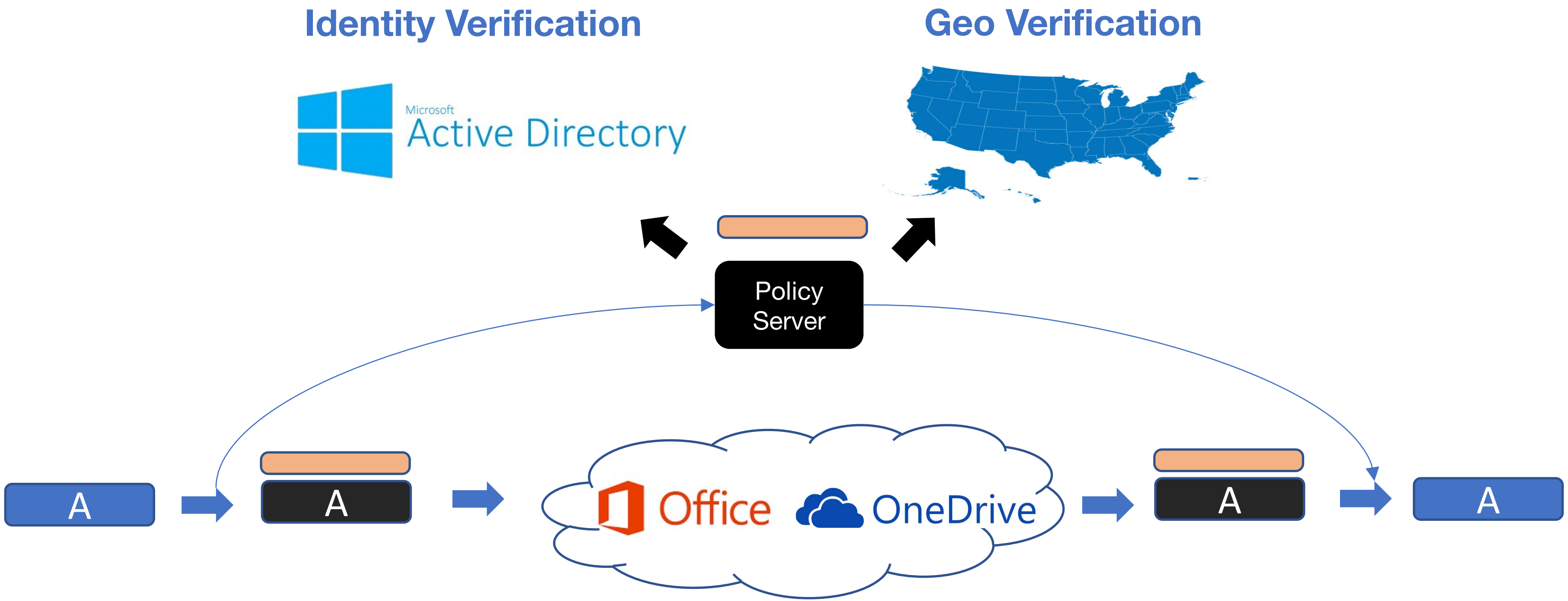


# 5: Movement of Data and Access to it logged by Policy Server

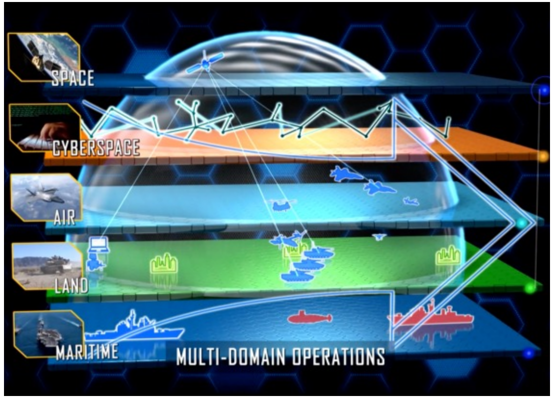
Zero Trust Data Use Case: CMMC Level 2

- **CMMC LEVEL 2 Challenge:**
  - 84/110 Controls Require Strict Access and Geo-Tracking Of Data NIST 800-171
  - Verification of all controls NIST 800 1717A
- **Zero Trust Data For CMMC Level 2:**
  - Utilize Zero Trust Data To Ensure Data Can Only Be Accessed By Authorized Users Within The US
  - Logging Of All Events Simplifies Verification Requirements

Zero Trust Data Use Case: CMMC Level 2



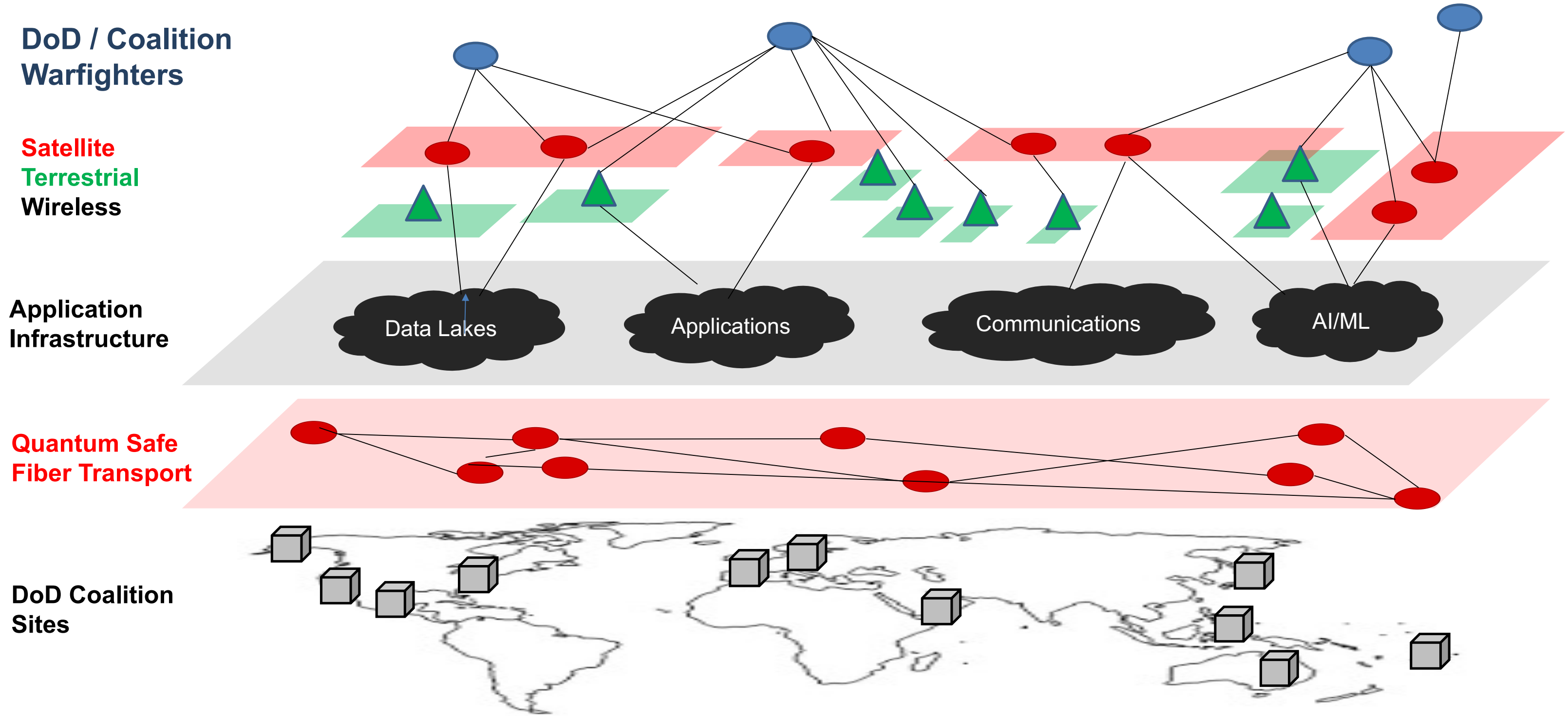
Zero Trust Data Use Case: JADC2



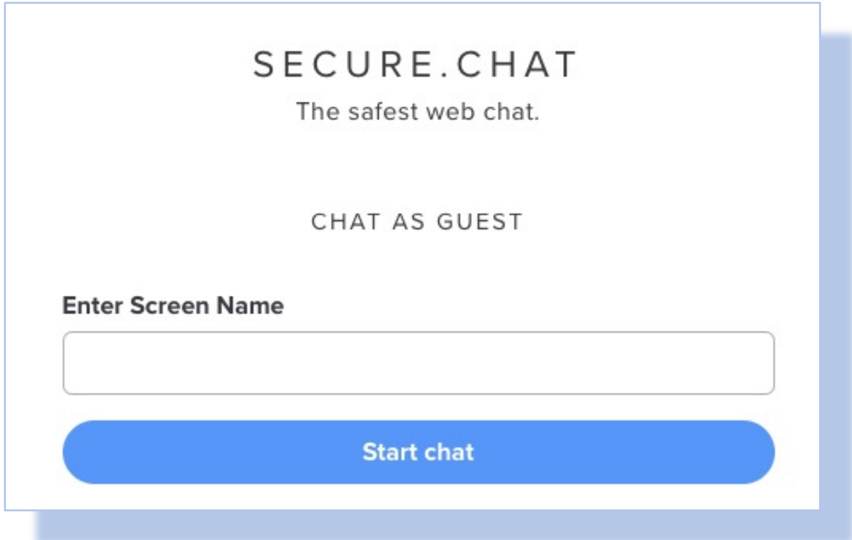
- **JADC2 Challenge:**
  - Data must be protected while being dynamically shared across different application and network infrastructure
  - Global footprint requires new level of scale and redundancy

- **Zero Trust Data For JADC2:**
  - Zero Trust Policy Server can issue/revoke access to software processes, networks and warfighters
  - Multiple Policy Servers can operate in parallel to ensure non-stop operations

Zero Trust Data Use Case: JADC2



Zero Trust Data Online Demos



SECURE.CHAT

The safest web chat.

CHAT AS GUEST

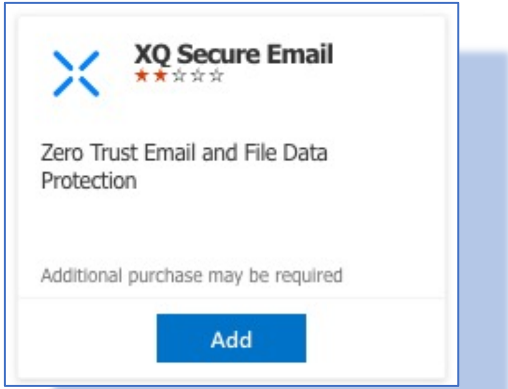
Enter Screen Name

Start chat

XQ Secure Gmail

xqmsg.com

Featured



XQ Secure Email

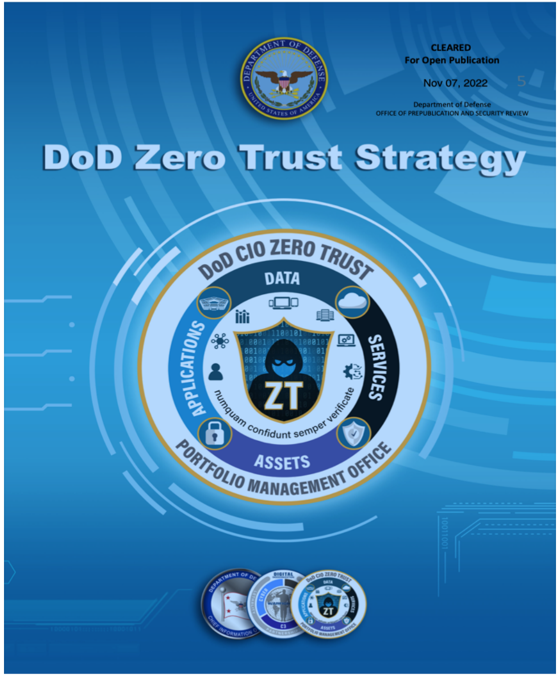
★★☆☆☆

Zero Trust Email and File Data Protection

Additional purchase may be required

Add

Zero Trust Data Redefines Cybersecurity



CLEARED
For Open Publication

Nov 07, 2022

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Zero Trust Strategy

DoD CIO ZERO TRUST
DATA
APPLICATIONS
SERVICES
ZT
numquam confidunt semper verificate
ASSETS
PORTFOLIO MANAGEMENT OFFICE

- Integrated Countermeasures
  - Defeats Data Exfiltration and Inside Attacks
- Simplifies Compliance
  - Low Cost CMMC Level 2 Solution
- Foundation For The Future
  - Enables Coalition JADC2 Operations