

Breaking Down ZERO TRUST

June 2023



WHO AM I?

Ryan Zacha is a Principal Solutions Architect spearheading Zero Trust Architecture for Booz Allen's Federal civilian and DoD clients supporting Zero Trust assessment, developing solutions to complex technical problems, and scaling capabilities in boundary protection, threat modeling, and network defense. Ryan currently leads a team of engineers and architects supporting DISA's Thunderdome project and is the technical lead on a DoD Zero Trust Architecture prototype.



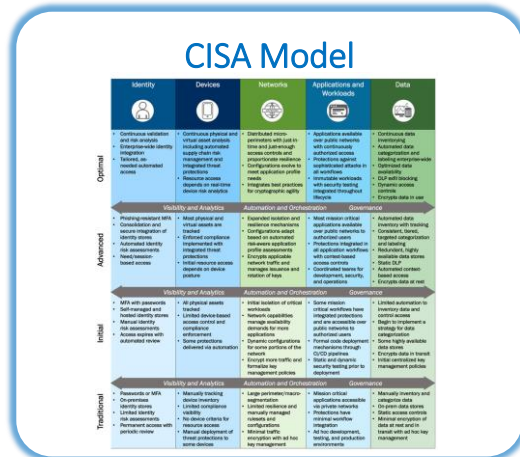
AGENDA

- Aligning to a Maturity Model
- Common Understanding Through Capability Mapping
- CISA & DoD Capability Maturity Models
- Maturity Assessment Methodology
- Where to Start
- Conditional-Based Access Example
- High-Level ZT Architecture
- Remote Access Architectures
- ICS/SCADA Reference Architecture

ALINGING TO A MATURITY MODEL

CISA Maturity Model

Align to CISA's Maturity Model



DoD ZT Reference Architecture

Align to DoD CIO's Reference Architecture v2.0

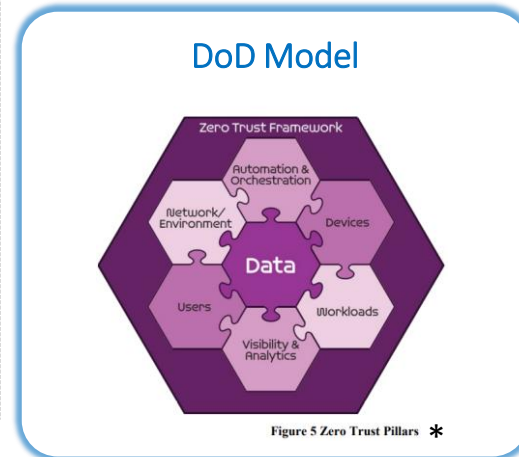
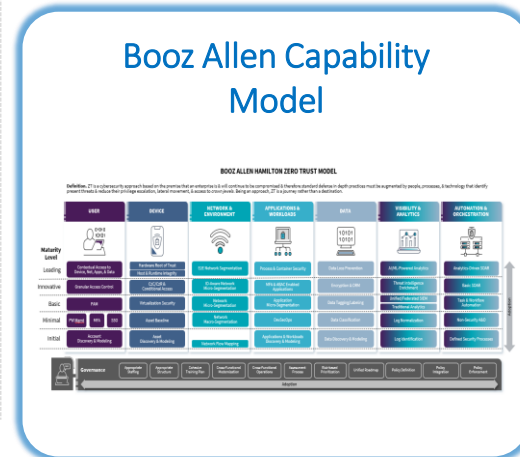


Figure 5 Zero Trust Pillars *

Tailored Model

Tailor a model unique to your needs



Supporting Documents and Frameworks

- NIST 800-207: Zero Trust Architecture
- OMB M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- Vendor Specific Approaches (Microsoft, Google BeyondTrust, Netflix LISA)
- DoD Zero Trust Strategy (Nov 7th, 2022)

COMMON UNDERSTANDING THROUGH CAPABILITY MAPPING

- Prior to November 2022 (DoD ZT Strategy release), the existing maturity models and reference architectures lacked capability mappings to each pillar to help organizations assess their current state and create roadmaps to track execution against.
- Through internal effort at Booz Allen and validated against DoD ZT Strategy we mapped security capabilities (e.g., Data Tagging, Asset Inventory, Micro-Segmentation) to each of the 5 or 7 pillars (depending on CISA vs. DoD Model) to allow a common maturity level understanding.
- Once the capabilities are mapped it opens the door for maturity assessment through current state assessment, target state creation, and capability road mapping.

CISA CAPABILITY MAPPING

LEGEND

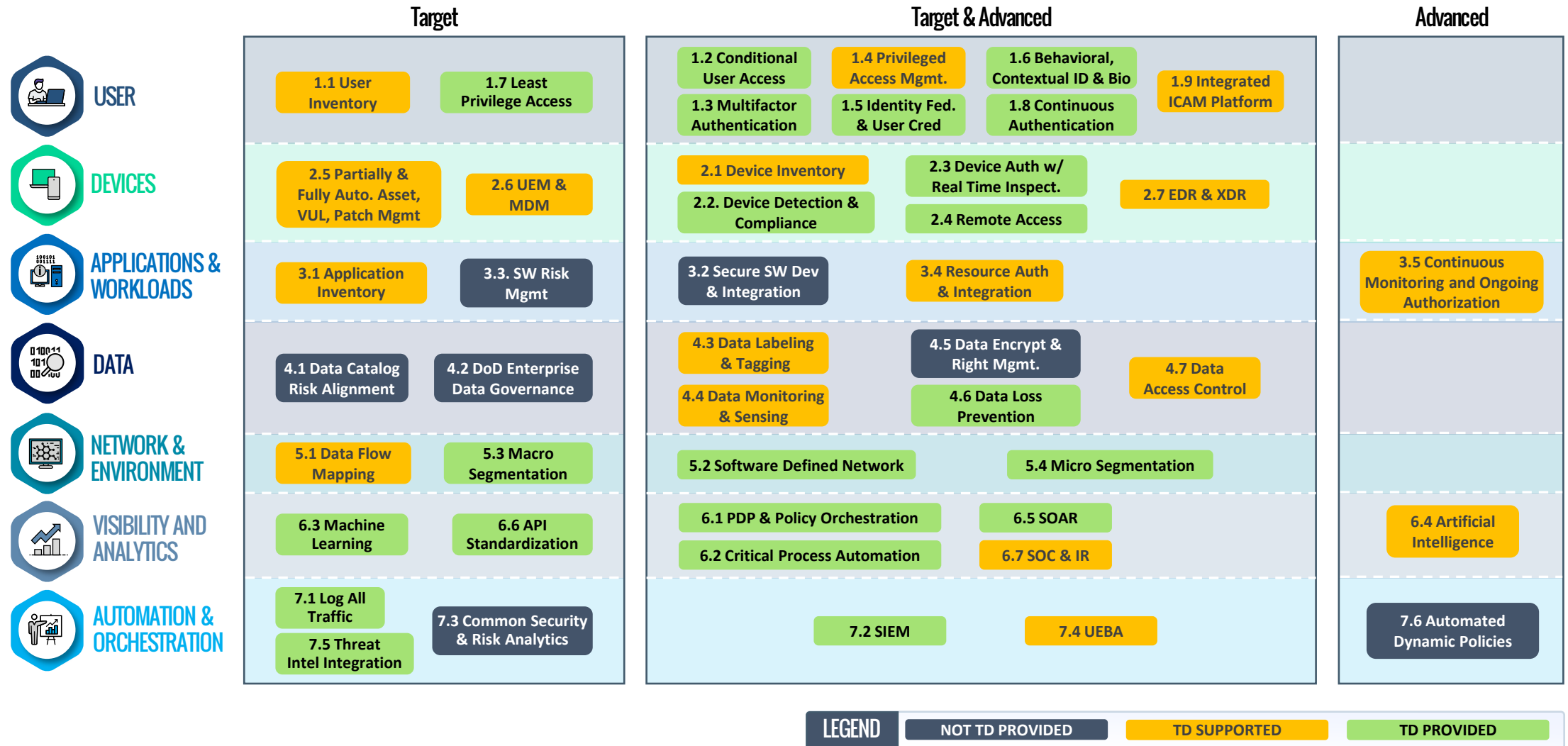
UNKNOWN

IN-PROGRESS

COMPLETE

	Traditional		Initial		Advanced		Optimal	
IDENTITY	Password or MFA Auth	Permanent access w/ period review	MFA w/ passwords	Self-Managed/ hosted ID store	Phishing-Resistant MFA	Need/Session-based access	Continuous validation and risk analysis	Enterprise-wide ID integration
	Limited risk assessment		Manual risk assessment	Access expires w/ automated review	Automated risk assessment	Consolidation and security integration of ID Stores		Tailored, as-needed automated access
DEVICES	Limited compliance visibility	Manually tracking device inventory	All physical assets tracked	Limited device-based access control and compliance	Most physical and virtual assets tracked	Enforced compliance w/ integrated threat protection	Continuous asset analysis including automated SCRM and threat protection	Resource access depends on real-time device risk
	No device criteria for resource access	Manual deploy of threat protection	Some protections delivered via auto		Initial resource access depends on device posture			
APPLICATIONS & WORKLOADS	Mission critical apps accessible via private network	Ad hoc dev, testing, and production environments	Some mission critical workflows have integrated protections and are accessible over public network	Formal code dev mechanisms / CI-CD pipelines	Most mission critical apps available over public network	Protections integrated in all application workflows w/ context-based access control	Applications available over public networks w/ continuously authorized access	Protections against sophisticated attacks in all workflows
	Protections have minimal workflow integration			Static & dynamic security testing	Coordinated teams for dev, security, & operations		Immutable workflows w/ integrated security testing	
DATA	Manual inventory and data categorization	Static access controls	Limited automation to inventory data and control access	Some high available data stores	Auto Data inventory	Static DLP	Continuous data inv	Optimized data availability
	On-prem data stores	Minimal encryption of DAR, DIT w/ ad hoc key mgmt	Begin to implement a data category strategy	Encrypted DIT	Consistent, tiered, targeted data categorization and labeling	Auto context-based access	Enterprise auto data categorization and labeling	DLP exfil blocking
				Initial centralized key mgmt policies		Encrypted DAR	Encrypt data in use	Dynamic access control
NETWORKS	Large perimeter/ macro-segmentation	Minimal traffic encryption w/ ad hoc key mgmt	Initial isolation of critical workloads	Network capabilities manage availability demand for more apps	Expanded isolation and resilience mechanisms	Configs adapt based on auto risk-aware apps profile	Distributed micro-perimeters w/ JIT and JEA controls and resilience	Configs evolve to meet application profile needs
	Limited resilience and manual ruleset and config mgmt		Dynamic config for some portions of network	Encrypt more traffic and formalize key mgmt	Encrypts applicable network traffic and manages issuance and key rotation		Integrates best practices for crypto agility	
VISIBILITY AND ANALYTICS								
AUTOMATION & ORCHESTRATION								
GOVERNANCE								

DOD CAPABILITY MAPPING



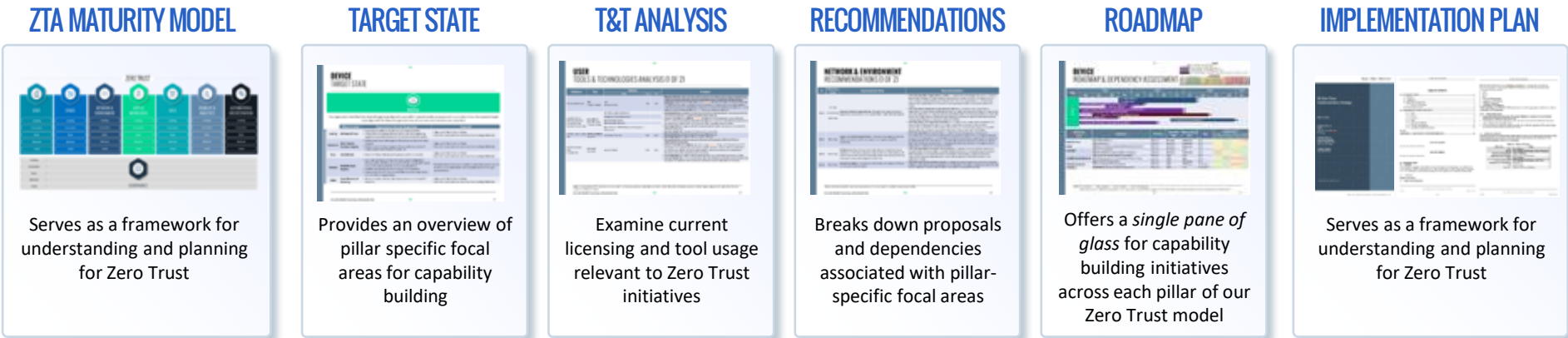
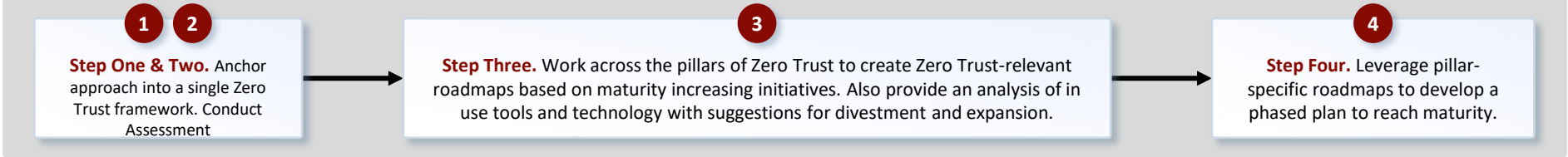
MATURITY ASSESSMENT METHODOLOGY



ZERO TRUST TARGET STATES AND ROADMAPS ARE INFORMED BY THREE DISTINCT INPUTS; COLLECTIVELY, THESE INPUTS PROVIDE THE BASE OF INSIGHT REQUIRED TO DEFINE A PATH FORWARD FOR ZERO TRUST



APPROACH TO DEFINING AN INTEGRATED ZERO TRUST ARCHITECTURE ROADMAP



WHERE TO START

Validate an Existing or Build a Target State Architecture for each of the 5 pillars

- Include supporting Automation & Orchestration and Visibility & Analytics features, platforms, and systems
- Zero Trust Architecture's core is Data Security but there is a heavy interaction between the Data, User, and Device pillars to ensure enforcement.








Assess your highest value data, applications, and attack surface to prioritize implementation

Build Roadmaps for each Pillar to track capability maturity inclusive of dependency mapping with a 3-to-5-year horizon to guide the organization

Use a simplified ZT assessment process (can look different for each organization) to remain aligned to strategy and highlight areas of concern and risk to completion

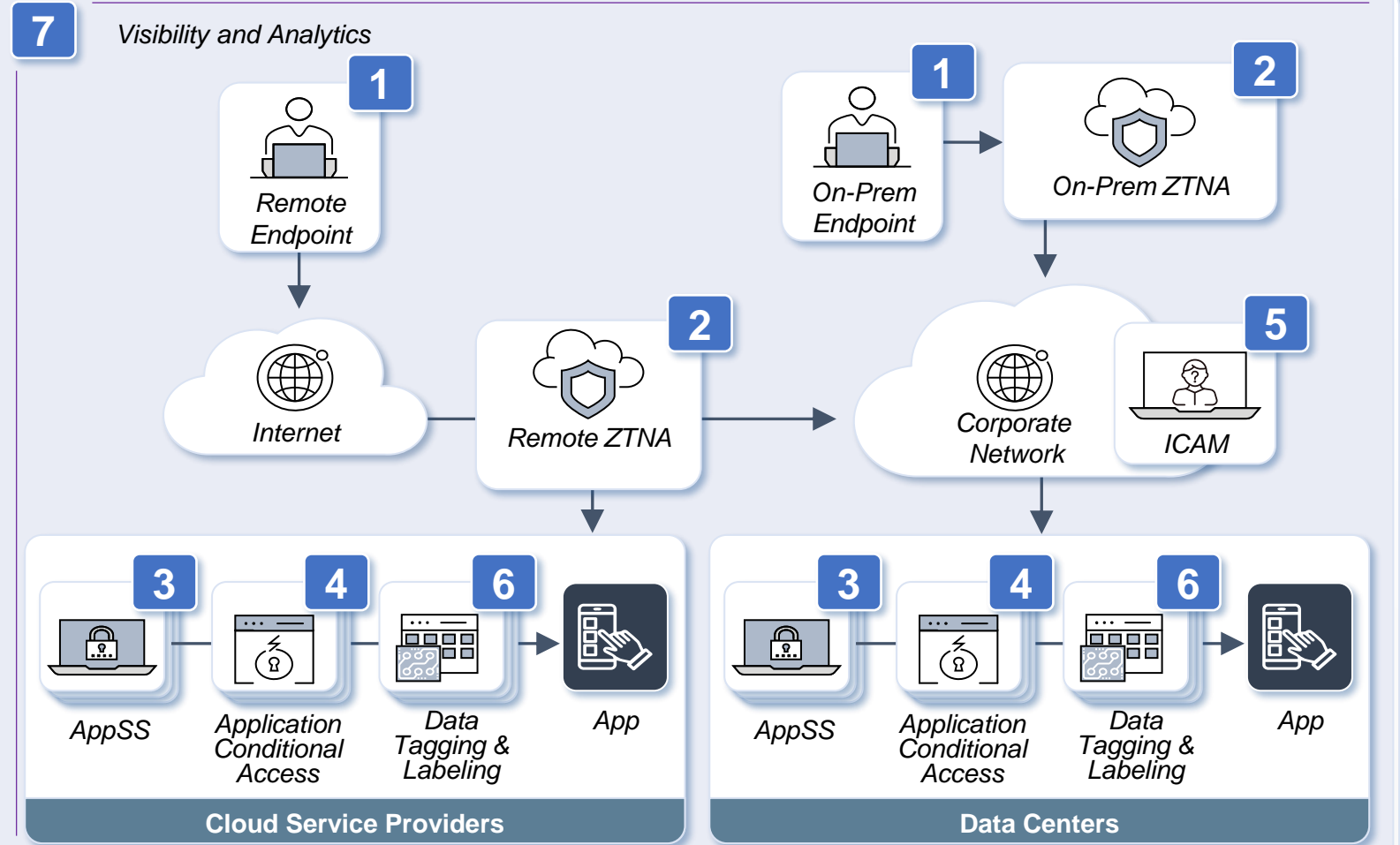
CONDITIONAL ACCESS EXAMPLE

ZTNA platform evaluates a user's group and the user's device hardening status before granting access to a resource

 USER	 USER GROUP	 DEVICE-HARDENING STATUS	 ACCESS LEVEL GRANTED	 APP 1 LOW VALUE	 APP 2 MODERATE VALUE	 APP 3 HIGH VALUE
A	Authorized to High Value	<ul style="list-style-type: none"> ✓ Latest OS patch ✓ Antivirus running ✓ Disk encryption enabled 	Full Access	ALLOW	ALLOW	ALLOW
A	Authorized to High Value	<ul style="list-style-type: none"> ✗ Latest OS patch ✓ Antivirus running ✓ Disk encryption enabled 	Limited Access (High→Mod)	ALLOW	ALLOW	DENY
B	Authorized to Mod Value	<ul style="list-style-type: none"> ✓ Latest OS patch ✓ Antivirus running ✓ Disk encryption enabled 	Full Access (for this user profile)	ALLOW	ALLOW	DENY
B	Authorized to Mod Value	<ul style="list-style-type: none"> ✗ Latest OS patch ✗ Antivirus running ✓ Disk encryption enabled 	No Access	DENY	DENY	DENY

HIGH-LEVEL ZERO TRUST ARCHITECTURE

- 1 Endpoint**
Monitors and manages devices; provides device attributes for ZTNA enforcement
- 2 Zero Trust Network Access (ZTNA)**
Implements conditional access to the network based on endpoint device posture and user identity provided by ICAM
- 3 Application Security Stack (AppSS)**
Scalable security stack providing micro segmentation, intrusion, and lateral movement protections against network and application-layer based attacks
- 4 Application Conditional Access**
Provides application-specific conditional access checks
- 5 ICAM**
Leveraged by ZTNA & Application Conditional Access components to provide user identity information
- 6 Data Tagging and Labeling**
Apply metadata to files/data for policy enforcement
- 7 Visibility and Analytics**
Monitors all components, providing analytics and incident response



REMOTE ACCESS ARCHITECTURES

• Remote Access Architectures:

1. Centralized Security Stacks

- Increases delay due to 'hairpinning' at locations not close to the source or destination

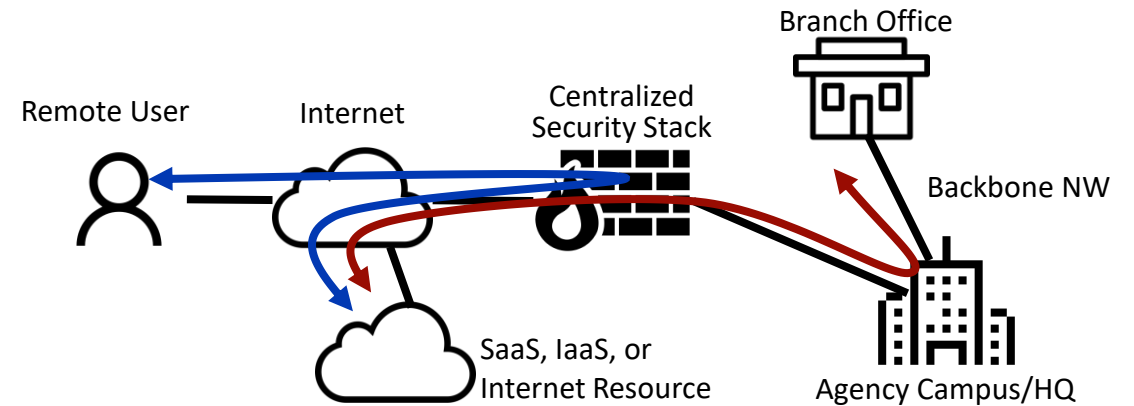
2. Direct to Internet/Cloud

- Easy to connect remote users to one SaaS/IaaS application
- Difficult to scale; each vendor provides their own security solution impacting operations and visibility
- Reliance on SaaS provider security

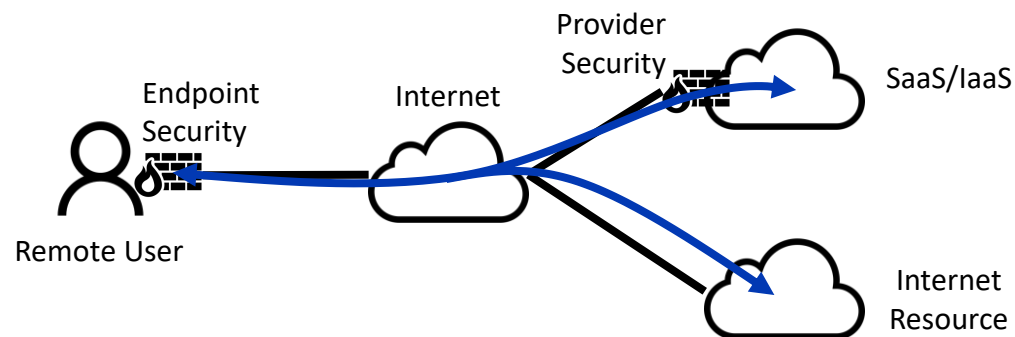
3. Secure Access Service Edge (SASE)/Security as a Service (SECaaS)

- Easy to scale
- Security data visibility through one centralized platform
- Infrastructure and software maintenance is SASE/SECaaS provider responsibility

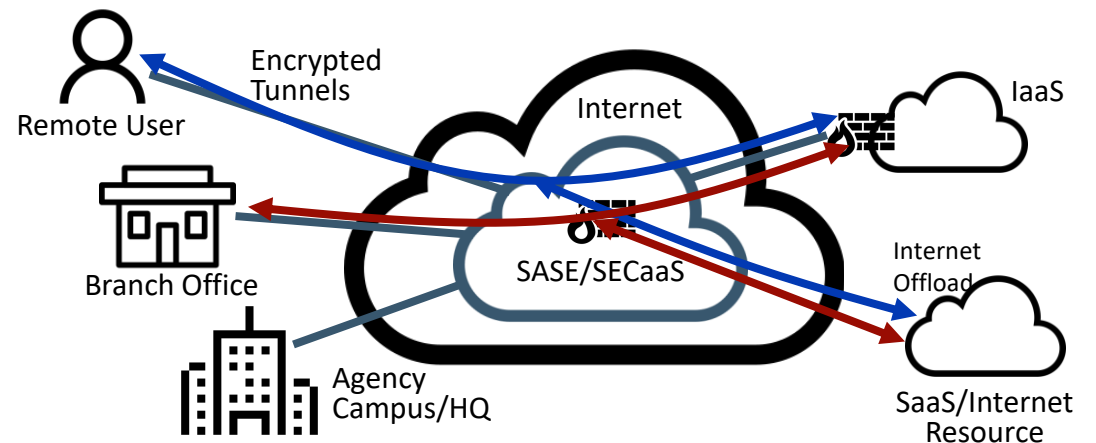
Traditional Centralized Security Access Points



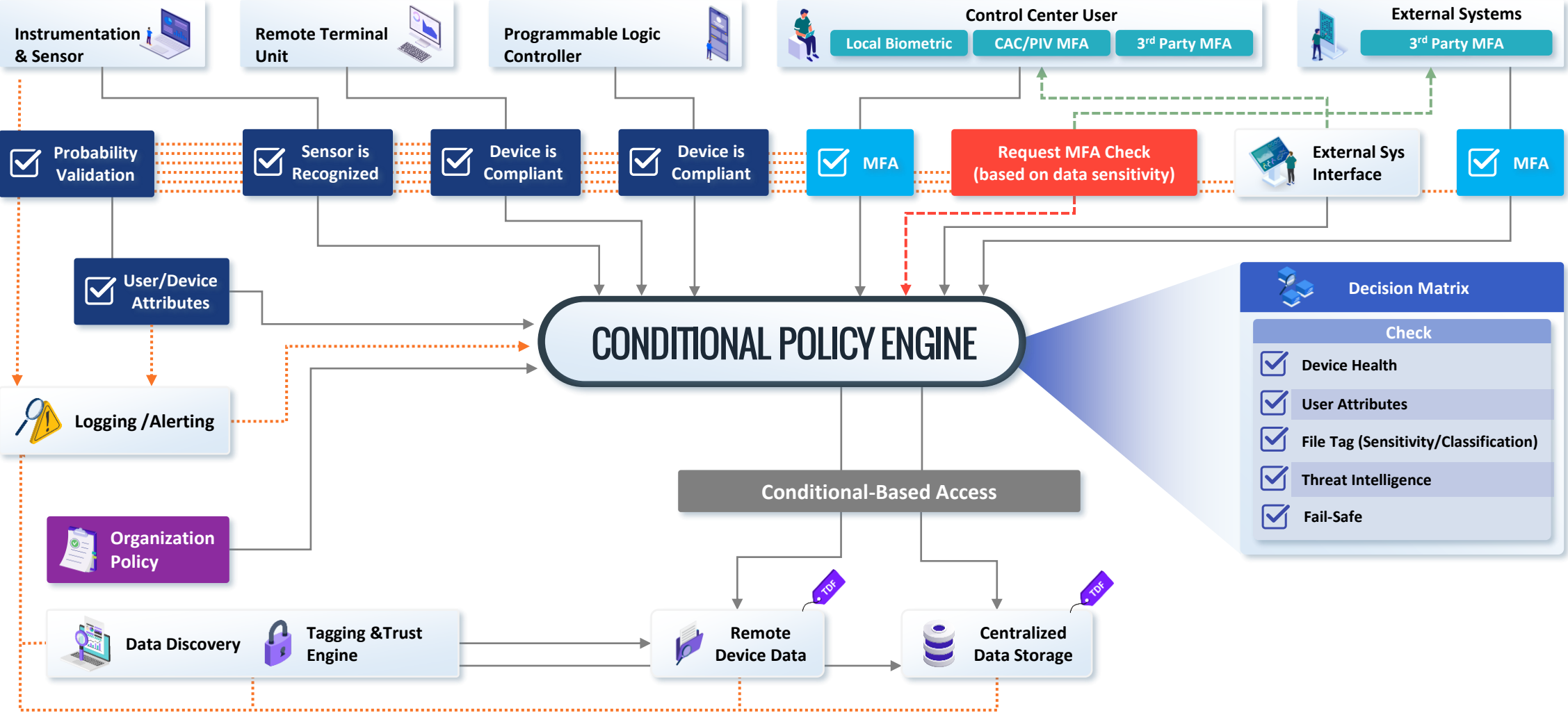
Direct to Internet/Cloud

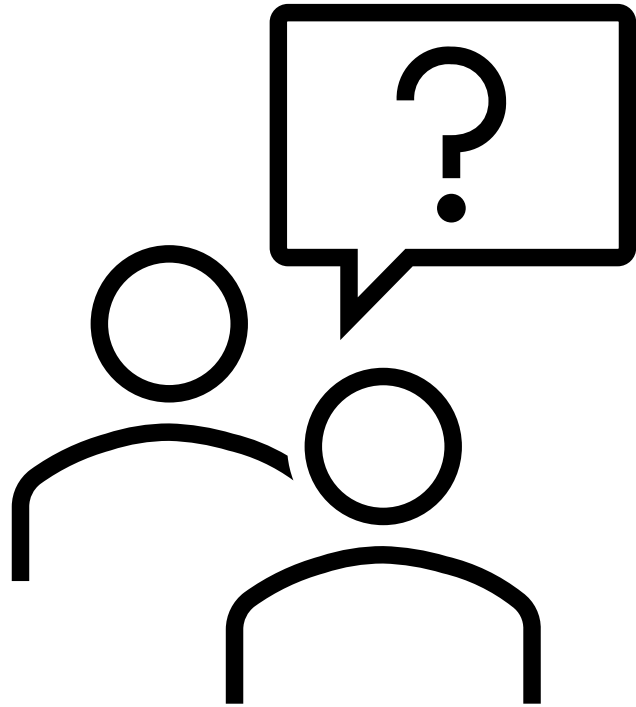


SASE/SECaaS



ICS/SCADA SECURITY - REFERENCE ARCHITECTURE





Questions?

Contact Us:

Ryan Zacha – zacha_ryan@bah.com

Imran Umar – Umar_Imran@bah.com

[Zero Trust \(boozallen.com\)](https://www.boozallen.com)