ATARC Zero Trust Vendor Presentation Outline

Outline

- Architecture Review Diagram
    - Display/Describe for following Use Cases as well in regards to architecture:
        - **Use Case 1 – Central HQ Operations**
          This use case involves a large, CONUS headquarters location. The following assumptions should be applied to this use case:
            - Robust, reliable connectivity is available from multiple sources.
            - Users operate using government furnished equipment on a network with a clearly definable perimeter.
            - Users access data and applications located both on-premise and in the cloud.

        - **Use Case 2 – Satellite office with highly reliable, robust connectivity**
          The following assumptions should be applied to this use case:
            - Satellite office location may be CONUS or OCONUS.
            - Staff size ranges from a dozen to several hundred.
            - Robust, reliable connectivity is available from multiple sources.
            - Users operate using government furnished equipment on a network with a clearly definable perimeter.
            - Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.

        - **Use Case 3 - Bandwidth challenged satellite office and little to no local IT support staff**
          The following assumptions should be applied to this use case:
            - Satellite office location may be CONUS or OCONUS.
            - Staff size ranges from 10 to several dozen.
            - Connectivity options are limited and sometimes/often prove unreliable.
            - Users operate using government furnished equipment on a network with a clearly definable perimeter.
            - Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.

        - **Use Case 4 - A remote user accessing corporate applications and data using a government-issued device**
          The following assumptions should be applied to this use case:
            - The user may be operating out of a CONUS or OCONUS location.

- Device could be a PC/Mac, tablet, or smart phone.
- In the case of a smart phone, the device is managed using an agency controlled and issued mobile device management solution.
- Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.

- **Use Case 5 - A remote user accessing corporate applications and data using a personal device**
  The following assumptions should be applied to this use case:
  - The user may be operating out of a CONUS or OCONUS location.
  - Device could be a PC/Mac, tablet, or smart phone.
  - The device is privately, personally owned and not controlled or managed by the government agency.
  - Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.
  - In the case of cloud access, the access is direct between the device and the cloud. The traffic does not traverse a government owned/managed network. (Non-VPN)

- What specific tools or suite of tools are being use in the POC?
  - NOTE: Vendors must be specific in identification. Many have an umbrella suite of tools or tools with various modules. Vendors need to be explicit in what tools in the suite or modules are being used as applicable.
- Solution Prerequisites:
  - Virtual/Physical and Appliance
    - Compute
    - Storage
    - OS/Software
    - Necessary integration?
    - Etc…
- Functional Areas solution covers in the ZT Architecture
  - Data
    - Data Loss Prevention
    - Data Classification
    - Metadata Management
    - Data Encryption
      - At Rest
      - On the Wire
    - Data Segmentation
    - Dynamic Data Masking (DDM)
    - Data Tagging
      - Manual
      - Fully-automated via ML/AI
    - Data Rights Management (DRM)

- Device & Endpoint
  - Device Authorization
  - HW & SW Inventory
  - Cloud-based Baseline Enforcement
  - Compliance Enforcement
  - Device Authentication
  - Could-based Software Deployment & Management
  - Intelligence for Endpoint Response
- Network and Environment
  - API Integration
  - Fully Encrypted Traffic
  - Common Service Access
  - Network Segmentation
  - Cloud Access Security Broker (CASB)
  - Software Defined Networking (SDN)
  - Software Defined Perimeter (Access to Apps and Data)
  - Application Proxy
- Application and Workload
  - DevSecOps
  - Application Delivery
  - Micro Segmentation
  - Application Segmentation
  - Software Chain Supply
  - Software Defined Compute
  - Application Approved/Prohibited List
  - Applications Visibility and Access (Anytime, Anywhere)
- User
  - User Authentication
    - Continuous Authentication
  - User Authorization
    - Continuous Authorization
  - Cybersecurity Access Policy
  - Privilege Access Management
  - Single Identity Platform
  - MFA
  - In-session Monitoring
  - ABAC
  - Key Management
  - Transparent Authentication
- Visibility and Analytics
  - Discovery and Baselining
  - Machine Learning
  - Advanced Threat Protection
  - Monitoring and Auditing
  - Risk Evaluation and Dynamic Risk Scoring
  - Security and Information Event Management (SIEM)

    - Automation and Orchestration
        - API Standards
        - Incident Response
        - Artificial Intelligence
        - Security Orchestration, Automation and Response (SOAR)
    - Governance and Scoring
        - Threat Scoring
        - Risk Scoring
        - Target Valuation
        - Triage Prioritization
        - Compliance Scoring
            - Dynamic
            - Snapshot
            - Trending
        - User Interface
            - Reporting
            - Dashboarding
- Functional Areas that allow for direct integration within the ZT Architecture with vendor solution
    - Data
        - Data Loss Prevention
        - Data Classification
        - Metadata Management
        - Data Encryption
            - At Rest
            - On the Wire
        - Data Segmentation
        - Dynamic Data Masking (DDM)
        - Data Tagging
            - Manual
            - Fully-automated via ML/AI
        - Data Rights Management (DRM)
    - Device & Endpoint
        - Device Authorization
        - HW & SW Inventory
        - Cloud-based Baseline Enforcement
        - Compliance Enforcement
        - Device Authentication
        - Could-based Software Deployment & Management
        - Intelligence for Endpoint Response
    - Network and Environment
        - API Integration
        - Fully Encrypted Traffic
        - Common Service Access
        - Network Segmentation
        - Cloud Access Security Broker (CASB)

        - Software Defined Networking (SDN)
        - Software Defined Perimeter (Access to Apps and Data)y
        - Application Proxy
    - Application and Workload
        - DevSecOps
        - Application Delivery
        - Micro Segmentation
        - Application Segmentation
        - Software Chain Supply
        - Software Defined Compute
        - Application Approved/Prohibited List
        - Applications Visibility and Access (Anytime, Anywhere)
    - User
        - User Authentication
            - Continuous Authentication
        - User Authorization
            - Continuous Authorization
        - Cybersecurity Access Policy
        - Privilege Access Management
        - Single Identity Platform
        - MFA
        - In-session Monitoring
        - ABAC
        - Key Management
        - Transparent Authentication
    - Visibility and Analytics
        - Discovery and Baselining
        - Machine Learning
        - Advanced Threat Protection
        - Monitoring and Auditing
        - Risk Evaluation and Dynamic Risk Scoring
        - Security and Information Event Management (SIEM)
    - Automation and Orchestration
        - API Standards
        - Incident Response
        - Artificial Intelligence
        - Security Orchestration, Automation and Response (SOAR)
    - Governance and Scoring
        - Threat Scoring
        - Risk Scoring
        - Target Valuation
        - Triage Prioritization
        - Compliance Scoring
            - Dynamic
            - Snapshot
            - Trending

        - User Interface
            - Reporting
            - Dashboarding
- Scope Solution Covers
    - On-Prem
    - Cloud
        - SaaS
        - IaaS
        - PaaS
    - Hybrid
- NIST 800-53 Control Mapping
    - Detail, describe or show some of the mapping of solution presented to 800-53 controls where possible
- Differencing Feature(s) (i.e. What distinguishes you from other, anticipated solutions?)
- Licensing
    - Licensing Model (i.e. User, subscription, device, transaction, hybrid, etc…)
    - Budgetary Costs (Optional)
- Current Customers
    - Government
    - Non-Government
- Demo
    - Use Cases Scenarios (Note: It should be assumed that all customer environments will have on-prem, SaaS, IaaS and PaaS infrastructure to account for)
    - Demo should point out types of attacks solution is mitigating as a result of solution set
    - Each scenario should take into account a number of risk factors and how the scenario would address. The following are only examples and an non-exhaustive list of such factors:
- **User:**

Cleared Gov't Employee	**Low**
Cleared Contract Employee	**Low**
Uncleared Contract Employee	**Med**
External Gov't User	**Med**
External Non-Gov't User	**High**
Public User	**High**
Privileged User/Service Account	**High**

- **Network:**

On Premises Managed	**Low**
VPN	**Low/Medium**
Raw Internet/Unmanaged	**High**
Guest Network	**High**

- **Device:**

Managed Desktop	**Low**
Managed Laptop	**Low**
Managed Mobile	**Medium**
BYOD	**High**
Virtual Image (Zero/Thin Client)	**Medium**
External Contractor Device	**High**
Proxy Based Access	**Medium**
IOT	**High**

- **Authentication:**

PIV/CAC Card	**Low**
Username and Password	**High**
MFA Call Back	**Medium**
MFA Ubi Key	**Low**
MFA Biometric	**Low**
MFA PIN	**Medium**
Time Bound	**Low**

- **Conditional Access Controls (Immediate Action)(Examples):**

Impossible Travel	**Quarantine or Severe**
Geo-location	**Block areas don't want to have access/permit those that can (country-based potentially)**
Risky/Dirty IP	**Quarantine or Severe**

- **Scenario 1**
- An agency employee is working remotely, using personally owned devices, must regularly access a public cloud based, agency application. The employee routinely accesses the system as a standard user but occasionally switches to administrator mode to perform systems maintenance. The user's physical location changes frequently with personal travel.
- **Scenario 2**
- An agency employee, working on from an agency satellite office and using government furnished equipment, is accessing Internet sites. The sites vary between sites supporting job related research and his/her personal bank. Limited personal use is acceptable per agency policy.
- **Scenario 3**
- A contracted employee provides ongoing improvements to an agency system as part of a development team and provides administrator and routine maintenance to the operational system. Development is performed from the contracted employee's corporate offices using devices provides by his/her company.

Development is performed on a separate network, isolated from the production network. Both operate within a data center located at the agency's facilities. When appropriate, the contracted employee moves systems from the development environment into production.

- **Scenario 4**
- Use the conditions described in Scenario 3 but both the development and production systems are cloud-based.
- **Scenario 5**
- An agency system interfaces with another agency's system, accessing fingerprint information as part of a background investigation process. Both systems are public cloud-based.
- **Scenario 6**
- Use Scenario 5 but both systems are located on-premise in the agencies' data centers.
- **Scenario 7**
- Use Scenario 5 but the primary system is located on-premise in the agencies' data centers and the secondary, accessed system is in a public cloud.
- **Scenario 8**
- Use Scenario 5 but the primary system is housed in a public cloud and the secondary, accessed system is located on-premise in the agency's data center.
- **Scenario 9**
- Use Scenarios 5 through 8 above but address from the perspective the primary agency system is being accessed to gain fingerprint data by another agency's system.
- **Scenario 10**
- The remote users (e.g. telework, off-site) of an agency's cloud-based HVA system are having connectivity issues that are inconsistently kicking them off their session. Outline any tools you provide for administrators' troubleshooting.
- **Scenario 11**
- The ICAM administrator has reported a user's credentials were compromised. Describe any tools/methods you provide to validate unauthorized access to systems under the ZTA umbrella has not occurred, either on-premise or cloud-based.
- **Scenario 12**
- An agency has decided to perform penetration exercises against their HVA systems operating under the ZTA umbrella, both on-premise and cloud-based. Describe the tools/methods you provide or support to accommodate these penetration exercises.
- **Additional Scenarios Considerations:**
    - Workload to Workload - within On-Premises Data Center
    - Workload to Workload – On-premises Data Center to/from Public Cloud

        - Monitoring Capabilities – On-Premises, Cloud and Hybrid, Continuous Monitoring and Evaluation
        - Privilege Access to Critical Infrastructure
        - IoT
        - Migration from On-Premises to Cloud
        - Cloud to Cloud Integration
        - Public/Non-employee or Customer Facing Services
        - Threats
            - Insider
            - Ransomware Prevention, Detection and Response
            - Phishing
            - Etc…
- POCs for customers to follow-up