



## DRAFT ATARC ZT Lab 3 - Mobility Track Use Cases

### Use Case 1: Mobile Workforce with Continuous Monitoring and Logging

#### Scenario 1: Teleworkers with Mobile Devices

Teleworkers are equipped with mobile devices (smartphones and tablets) that are used to access mission-critical applications and data from various locations (both CONUS and OCONUS).

- Utilizing continuous monitoring and logging, detect and respond to any anomalous behavior or unauthorized access attempts in real-time.
- All access requests must be logged, analyzed, and stored securely, providing a comprehensive audit trail to ensure compliance and forensics in case of a security breach.

Threats Addressed: Unauthorized access, data breaches, compromised devices, man-in-the-middle attacks, and insider threats.

#### Scenario 2: Mobile Command Center

A mobile command center operates in remote locations with varying levels of connectivity.

- Continuously monitor command center's network infrastructure and log of all devices and users accessing the network, ensuring that any suspicious activity is immediately flagged for review.
- The solution should include automated alerts and dynamic network segmentation capabilities to isolate potential threats without disrupting overall operations.

Threats Addressed: Network intrusions, data breaches, unauthorized access, compromised devices, and lateral movement within the network.

#### Scenario 3: Emergency Response Team Operations

Emergency response teams require rapid, secure access to sensitive data and applications while in transit or deployed in field conditions.

- Demonstrate continuous authorization measures when using a mobile device to access data, such as behavior-based analytics and multi-factor authentication (MFA), to ensure that only authorized personnel can access specific resources.
- Test the ability of the solution to maintain security and performance standards even under intermittent connectivity or high-stress conditions.

Threats Addressed: Data leaks, unauthorized access, compromised communications, and device integrity threats.



## **Use Case 2: Mobile Device as Primary Authenticator**

### **Scenario 1: Biometric-Based Authentication for Secure Facilities**

Users access secure facilities using mobile devices as the primary authentication method, leveraging biometric features such as facial recognition or fingerprint scanning

- Integrate mobile-based authentication methods into existing physical security controls and IT infrastructure.
- Demonstrate seamless user experience while maintaining high security standards through Zero Trust principles.

Threats Addressed: Credential theft, spoofing, unauthorized facility access, and tampered devices.

### **Scenario 2: Cross-Platform Authentication in Collaborative Environments**

Mobile devices are used as authenticators in a cross-platform environment, where users need to access both government and third-party applications.

- Support integration across different devices and operating systems, ensuring that Zero Trust principles are maintained irrespective of the platform.

Threats Addressed: Cross-platform data breaches, unauthorized access, compromised devices, and network intrusions.

### **Scenario 3: Emergency Access Protocols Using Mobile Devices**

The focus is on demonstrating how Zero Trust can be implemented in scenarios where speed and security are equally critical.

- Rapid access is required (e.g., during emergencies or critical incidents), users are authenticated using mobile devices configured for rapid authentication (e.g., via passkeys or proximity-based access controls).

Threats Addressed: Unauthorized access during emergencies, device compromise, and insider threats.



## **Use Case 3: Continuous Authorization and Access Management**

### **Scenario 1: Adaptive Security for High-Risk Users**

High-risk users, such as those handling sensitive or classified information, are subject to continuous authorization checks based on their location, device health, and behavior.

- Dynamically adjust access permissions in real-time, ensuring that security policies adapt to the changing risk landscape.
- Evaluate the system's ability to enforce fine-grained access control while minimizing user friction.

Threats Addressed: Insider threats, compromised credentials, unauthorized access, and device health risks.

### **Scenario 2: Secure Remote Collaboration**

Teams collaborating across multiple geographies require secure access to shared resources and data.

- Continuous authorization demonstrating users' access is constantly validated based on context, such as time of access, location, and device status.
- Allow for maintaining productivity without compromising security, even in a highly distributed workforce.

Threats Addressed: Data breaches, unauthorized access, compromised devices, and insecure communications.

### **Scenario 3: Insider Threat Detection and Response**

Identifying and responding to potential insider threats through continuous authorization and behavioral analytics.

- Simulate an insider attempting to exfiltrate data using a compromised or unauthorized device, testing the system's ability to detect and mitigate such threats.

Threats Addressed: Insider threats, unauthorized data access, compromised devices, and data exfiltration.



## **Use Case 4: Passkeys and Passwordless Authentication**

### **Scenario 1: Transition to Passwordless Authentication**

A large organization transitions from traditional password-based authentication to passkeys for accessing internal applications and systems.

- Test the implementation of passkeys as a secure alternative to passwords, focusing on ease of use, user adoption, and security improvements.
- Ensure seamless integration with existing identity management systems and adherence to Zero Trust principles.

Threats Addressed: Credential theft, phishing attacks, unauthorized access, and device compromise.

### **Scenario 2: Multi-Factor Authentication with Passkeys**

Passkeys are implemented as part of a multi-factor authentication (MFA) solution, where users must authenticate using a combination of passkeys and other factors (e.g., biometrics or security tokens).

- Examine the usability and security implications of using passkeys in conjunction with other authentication methods.
- Demonstrate enhanced security without negatively impacting the user experience.

Threats Addressed: Unauthorized access, compromised credentials, phishing attacks, and device compromise.

### **Scenario 3: Secure Access to Cloud Resources**

Users accessing cloud resources (e.g., SaaS applications) must authenticate using passkeys as part of a broader Zero Trust strategy.

- Evaluate the effectiveness of passkeys in securing access to cloud environments and protecting against common attack vectors such as phishing.
- Demonstrate robust security while maintaining user convenience and minimizing friction.

Threats Addressed: Cloud data breaches, unauthorized access, compromised devices, and phishing attacks.