RSAConference™2024
San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: IDY-TD09

# Lesson Learned - General Motors Road to Modern Consumer Identity

#RSAC

**Andrew Cameron**

IT Fellow, Identity and Access Management
General Motors
https://www.linkedin.com/in/kandrewcameron

**Razi Rais**

Senior Product Manager
Microsoft
https://www.linkedin.com/in/razirais

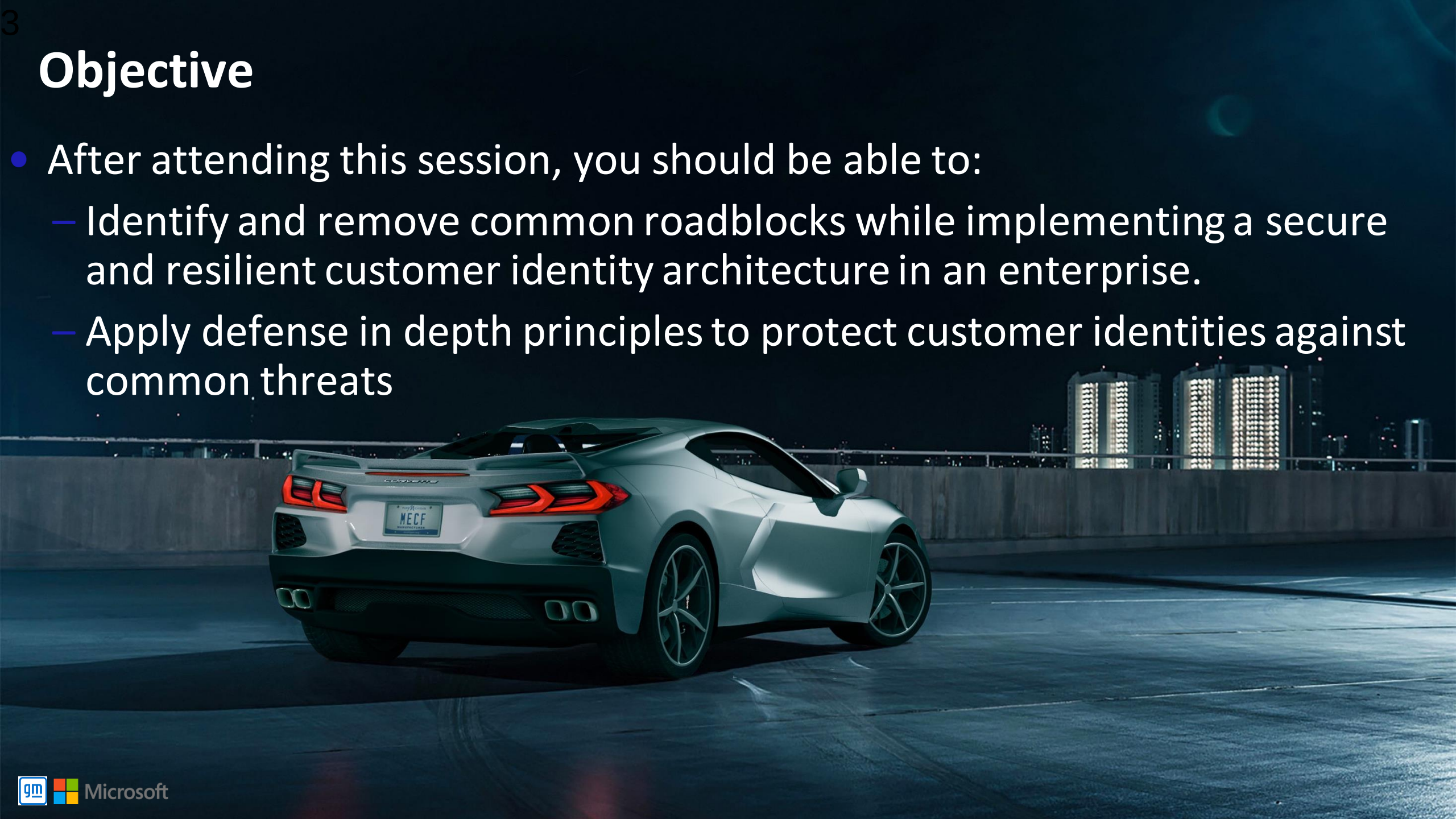
# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

# Objective

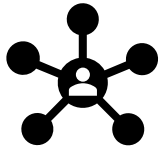
- After attending this session, you should be able to:
  - Identify and remove common roadblocks while implementing a secure and resilient customer identity architecture in an enterprise.
  - Apply defense in depth principles to protect customer identities against common threats



# Lesson: Customer identities are significantly distinct from workforce identities.

# Customer identities vs Workforce identities

## Identity creation



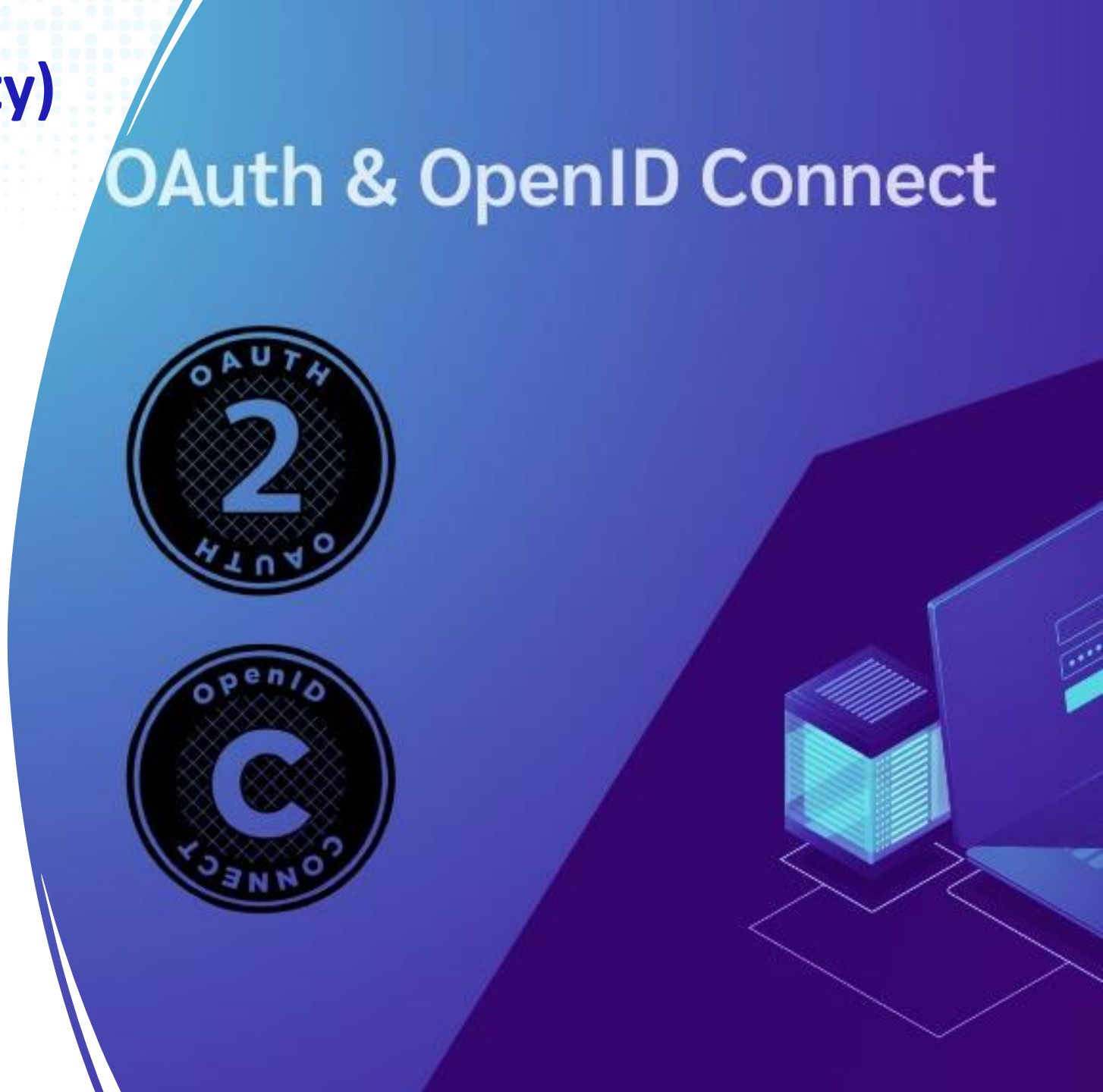
## Identity proofing

## Business focus

## Branding needs

# Protecting The client (identity)

- Use Modern Auth Protocols
  - Open ID Connect Auth Code Flow w PKCE
  - OAuth 2.1
- FIDO and WebAuthN are proven now, we CAN use them!
  - Move to ‘Identifier first’ login
- Use Risk Based MFA
- Support federated logins but consider the experience!
- Behavior and Usage Analytics are your friend, use them wisely!



# Lesson: Security is a balancing act for customer identities

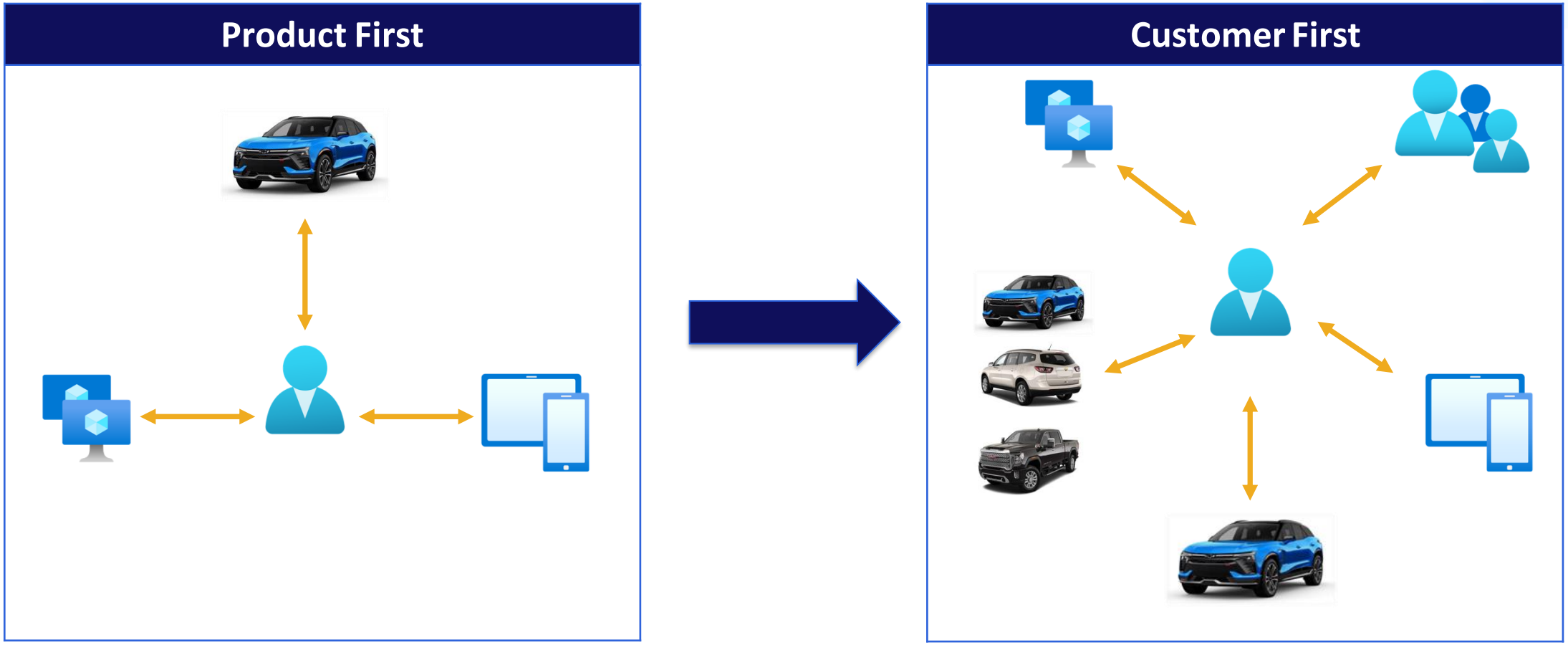
Microsoft

# Security Balancing Act for Customer Identities Services


| Security | Usability |
| --- | --- |
| Compliance | Increase site traffic |
| Prevent Fraud and Misuse | Improve conversion rates |
| Secure Customer Information | Create/Retain Customers |
| Protect Digital Assets | Integrate services |

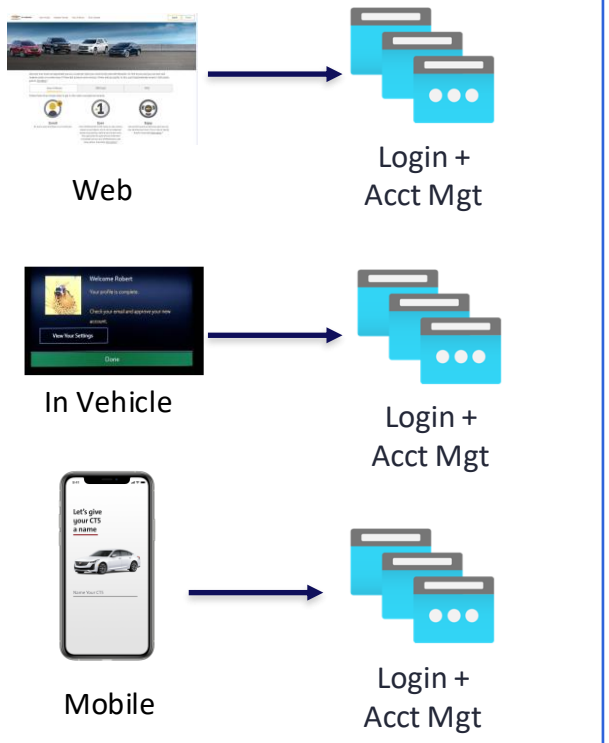
# Customer IAM requires a fundamental shift…

We've changed from a vehicle-first to a customer-centric model for experiences and infrastructure

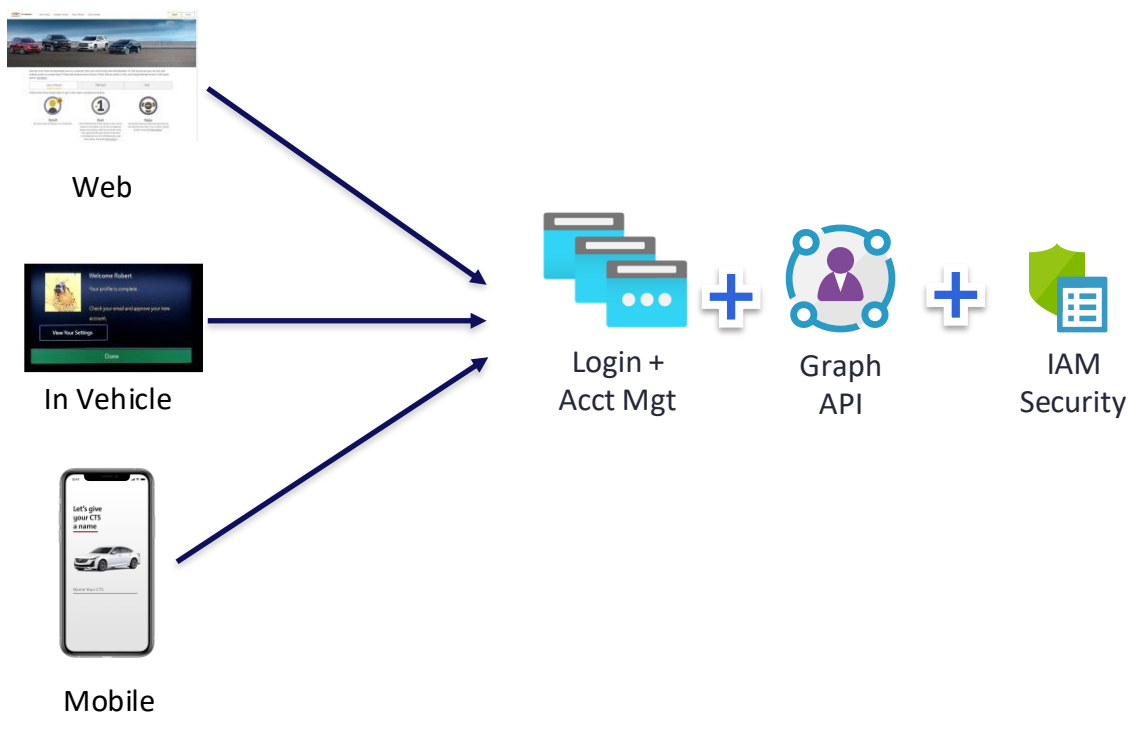


# Legacy vs Modern CIAM Architecture

## IAM Apps Per Channel (Legacy Model)




## Common Services (Cloud Native Model)



# CIAM Service - Core Requirements and Features

**Feature: Account Management**

**Feature: Delegated Admin**

**Feature: Preference Management**

## Single Identity & Account

Customers have a single identity and account across all products and experiences, ensuring a cohesive journey.

## Frictionless and Secure

We ask customers to provide personal information only once and with a clear value exchange. Account creation, authentication and dashboard navigation are frictionless, secure experiences.

## Scales easily as the business transforms

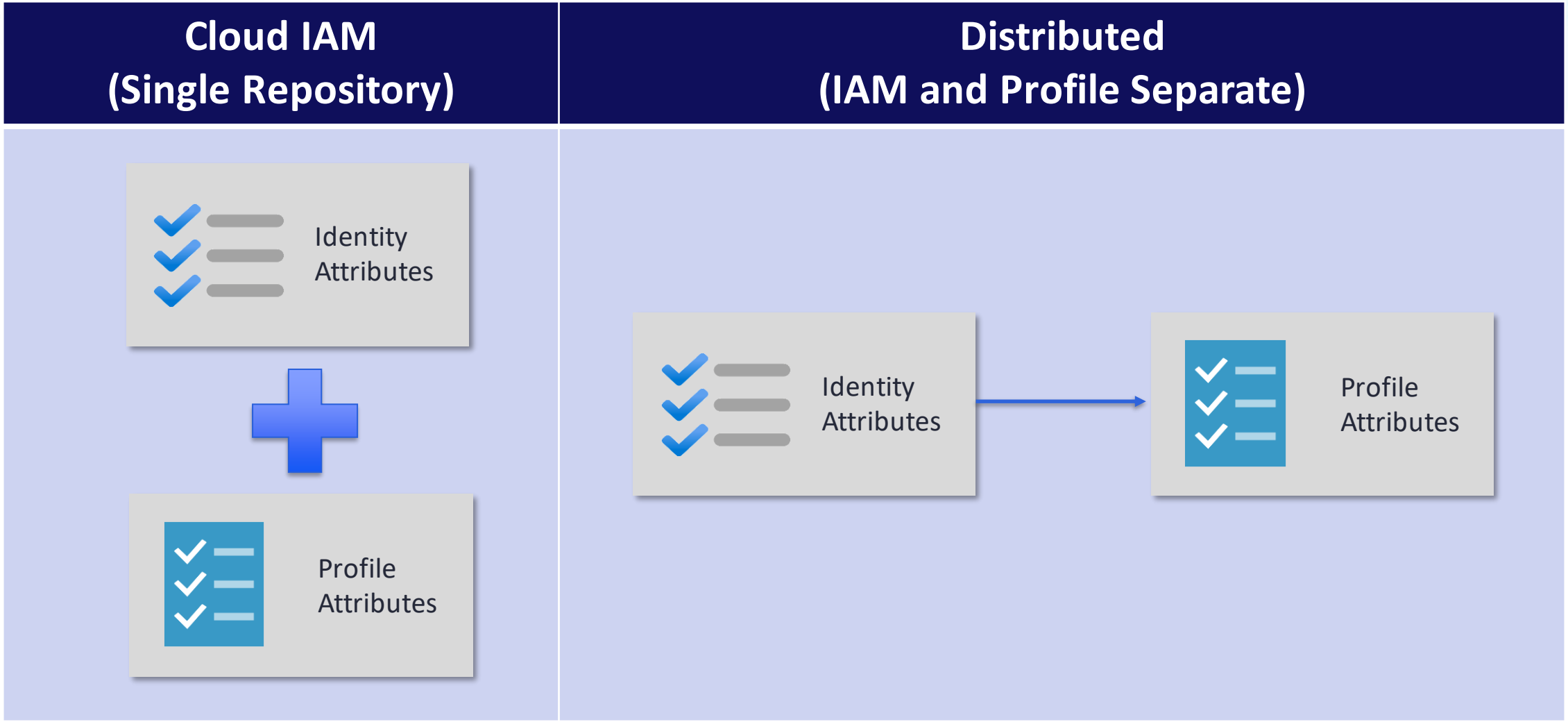
Customers can see and manage new types of products and services that GM is bringing to market.

## Personalization

Personalized experiences follow customers through the journey and across products. (omni-channel)

*Customers can **see** and **manage** their relationship through a single and cohesive experience.*

# Profile Management Options



# Building blocks for defense in depth for customer identities

# Building blocks

## Establish Intent

- What? What this request is trying to do (assume malicious indent unless proven otherwise)
- Why? Why should this be allowed/denied?

## Establish Proof

- Who? Who are you and what can you assert about yourself?

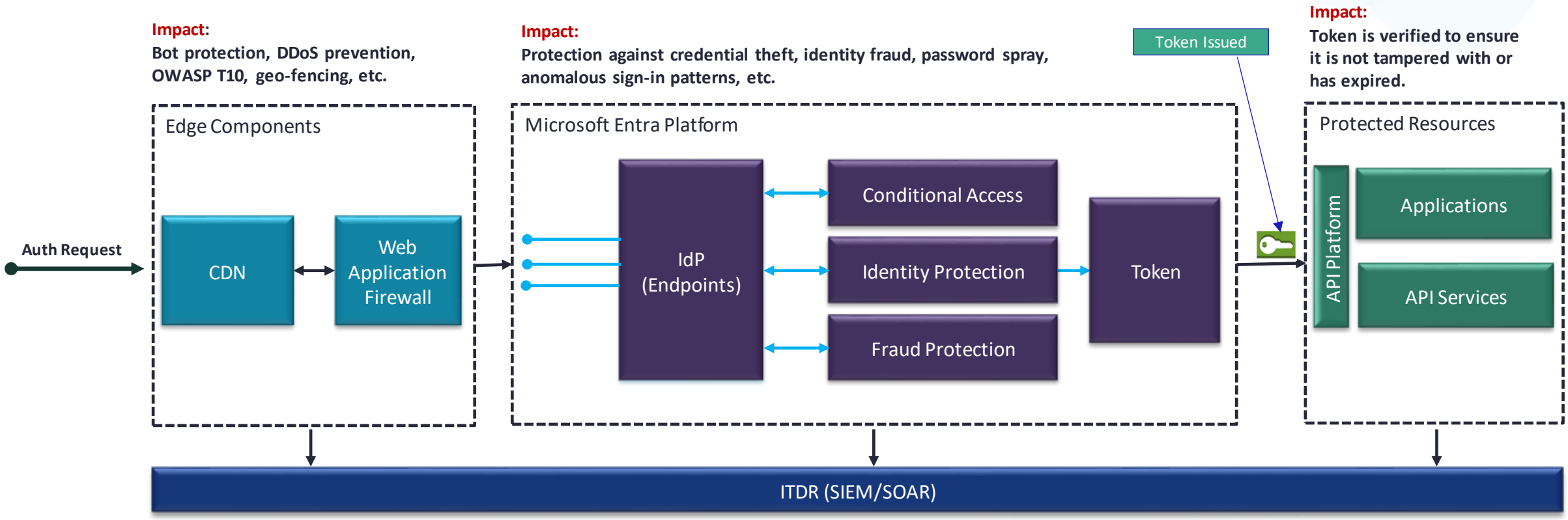
## Observe

- Continuous awareness via monitoring
- See something say something - early warning signals

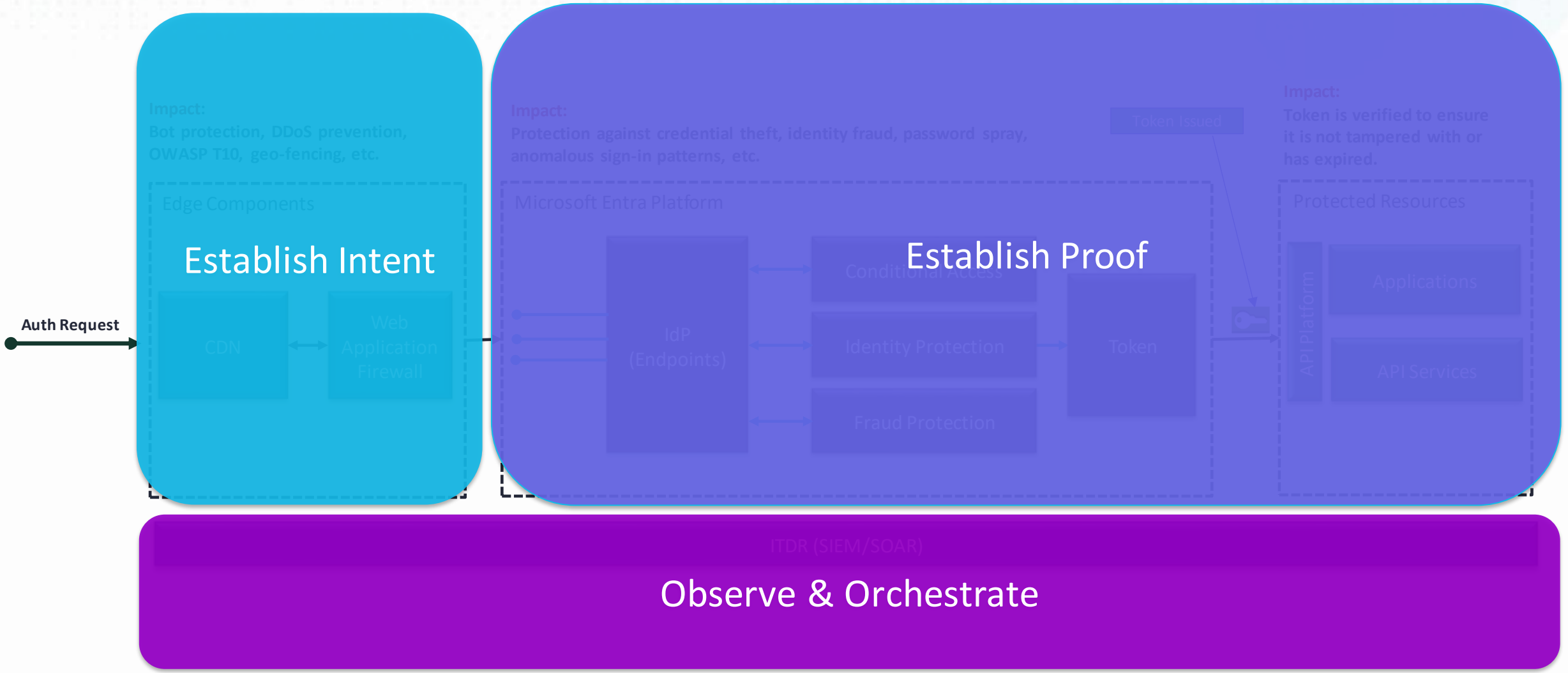
## Orchestrate

- Detect
- React

# CIAM Architecture



# CIAM Architecture

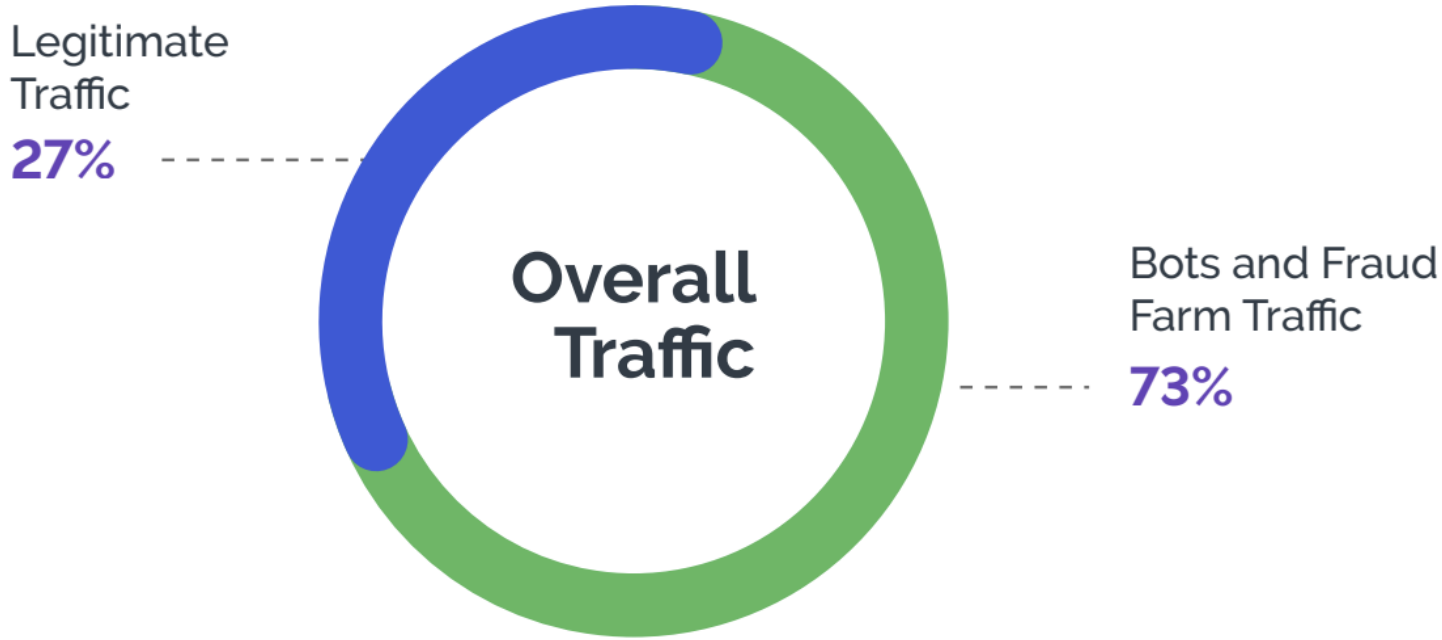



# Lesson: Malicious bots are root of all evil

Microsoft

# Malicious bots are root of all evil

- Bots are used heavily to attack customer identities at scale:
  - > DDoS
  - > Fake account creation
  - > Inflated MAU
  - > Subscription abuse




Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks: Arkose Q4 2023

# Malicious bots - mitigation

# Lesson: Protect sign-ups with identity fraud protection

# Identity Fraud

- **Fake accounts**: Fake account creation is the process of creating accounts using bogus or stolen identity information.
- Impact: Free trial abuse, subscription abuse, fake reviews, brand damage, etc.

- **IRSF: International Revenue Share Fraud** attack which target businesses by artificially inflates traffic by generating calls/SMS to premium number ranges without paying for the calls.
- Impact: High cost to service provider, revenue loss due to high user on-boarding cost, etc.

# Identity Fraud Protection

- Most fraud abuse is driven by bots so use **WAF as first layer of defense**.
- **Fraud protection** and identity proofing to protect against creation of fake accounts during sign-ups
- **PSTN phone calls/SMS** based MFA are are root cause of IRSF. Avoid using them when you can (use TOTP etc.).
- Security Controls: **WAF + Identity proofing + MFA (non-PSTN based)**

# DEMO> WAF [GEO-FENCING/RATE-LIMITING]

# DEMO> WAF [GEO-FENCING/RATE-LIMITING]

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. Learn more about custom rules

Custom rule name * BlockRequestFromOutsideUS

Status Enabled Disabled

Rule type Match Rate limit

Priority * 1

Block/rate limit request based on region/country


Example: Block request

# DEMO> WAF [GEO-FENCING/RATE-LIMITING] Cont.

```json
"customRules": {
    "rules": [
        {
            "name": "BlockRequestFromOutsideUS",
            "enabledState": "Enabled",
            "priority": 1,
            "ruleType": "MatchRule",
            "rateLimitDurationInMinutes": 1,
            "rateLimitThreshold": 100,
            "matchConditions": [
                {
                    "matchVariable": "SocketAddr",
                    "operator": "GeoMatch",
                    "negateCondition": true,
                    "matchValue": [
                        "US"
                    ],
                    "transforms": []
                }
            ],
            "action": "Block"
        }
```

Infrastructure as Code [JSON]

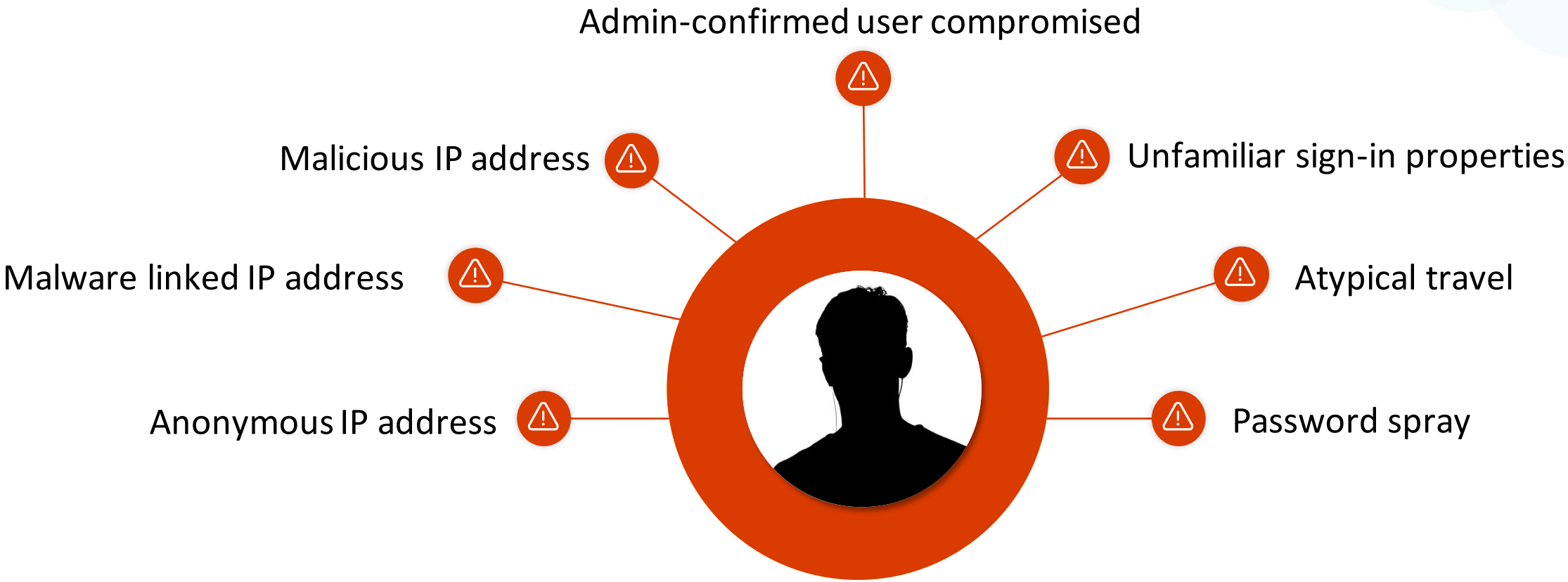
```powershell
New-AzFrontDoorWafPolicy -Name $policyName -ResourceGroupName $resourceGroupName
```

```
PS /home/razi> $policy.CustomRules

RuleType                  : MatchRule
Action                    : Block
MatchConditions           : {Microsoft.Azure.Commands.FrontDoor.Models.PSMatchCondition}
Priority                  : 1
RateLimitDurationInMinutes : 1
RateLimitThreshold        : 100
Name                      : BlockRequestFromOutsideUS
EnabledState              : Enabled
```

Script [PS]

# User Identity Protection – ML Based Risk Detections



# DEMO> RISK BASED ADAPTIVE AUTHN POLICY

# DEMO> RISK BASED ADAPTIVE AUTHN POLICY

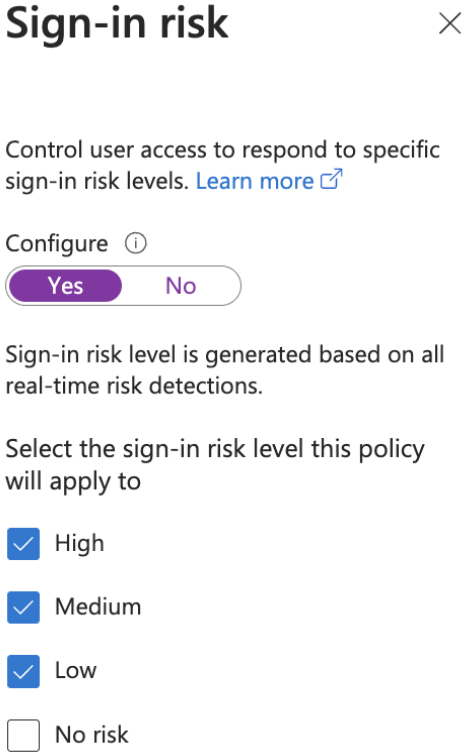
**CONDITIONAL ACCESS POLICY [LOGIC]**

**IF**

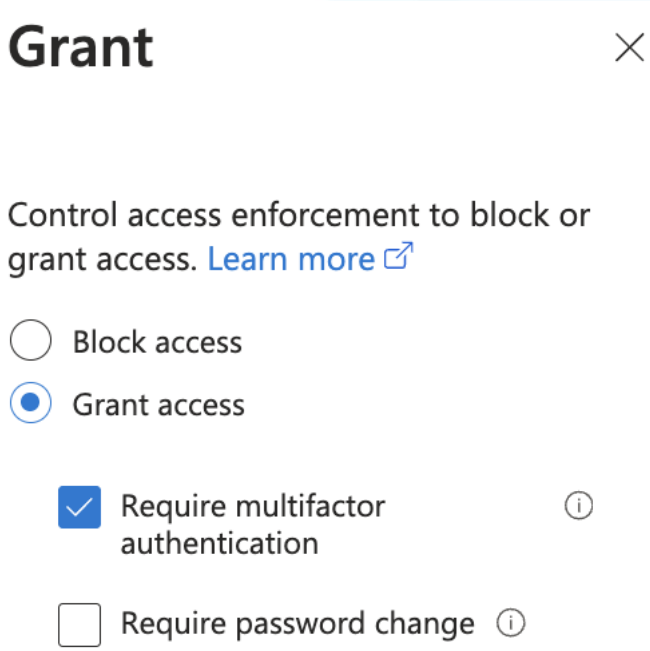
[CONDITIONS 1..n]

**THEN**

[APPLY CONTROL(s)]




Example - CONDITION: Trigger when risk is detected during sign-in.




CONTROL: Grant access only after successful MFA.

# DEMO> MFA METHODS

## Multi-Factor Authentication

Multi-Factor Authentication (MFA) can be used to help protect your account from unauthorized access by requiring you to enter a security code when you sign in.

Available authentication methods (select 1):

**Text (SMS) Authentication**

Use your phone number as your MFA method. When you sign in, you'll be required to enter a verification code sent via text (SMS) message.

**Email Authentication**

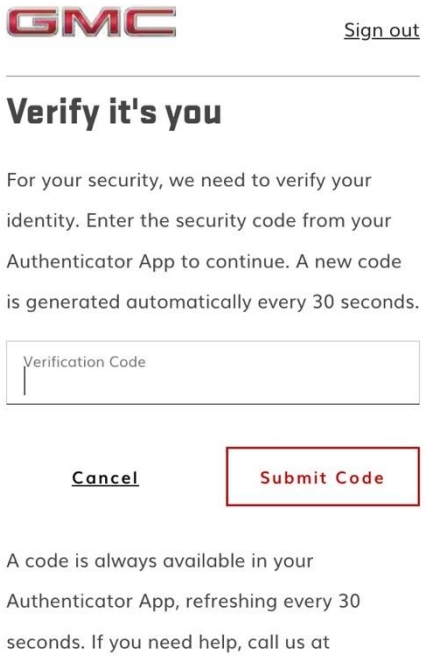
Use your email address as your MFA method. When you sign in, you'll be required to enter a verification code sent to your email address.

**Third-Party Authenticator App**

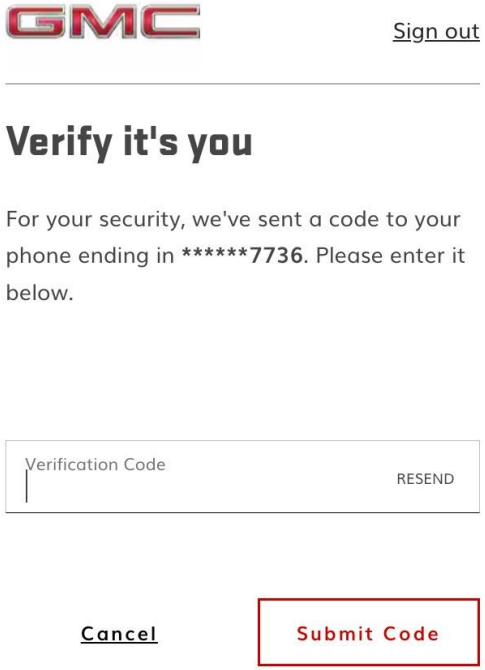
Use an Authenticator App as your MFA method. When you sign in you'll be required to use the security code provided by your Authenticator App.

Multiple MFA options are available [flexibility is key, but phishing resistance method authenticator is recommended]

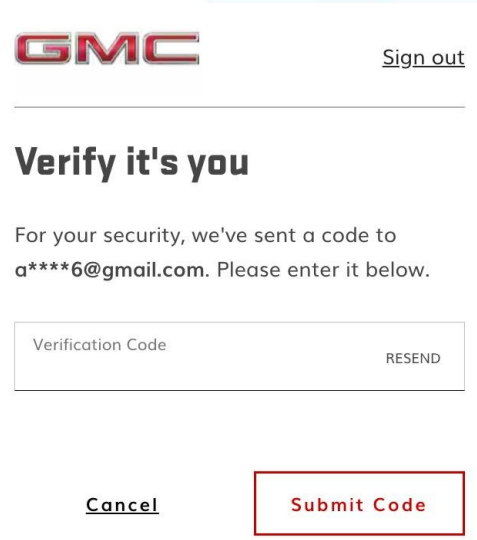
# DEMO> MFA METHODS (Cont.)




Authenticator/TOTP 💯




SMS OTP

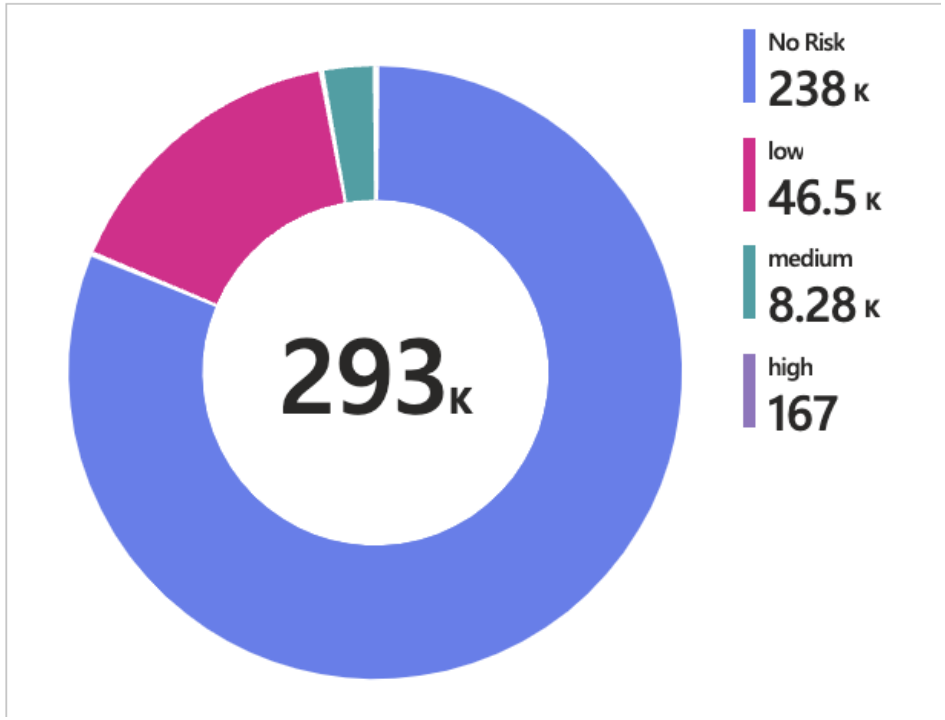



Email OTP

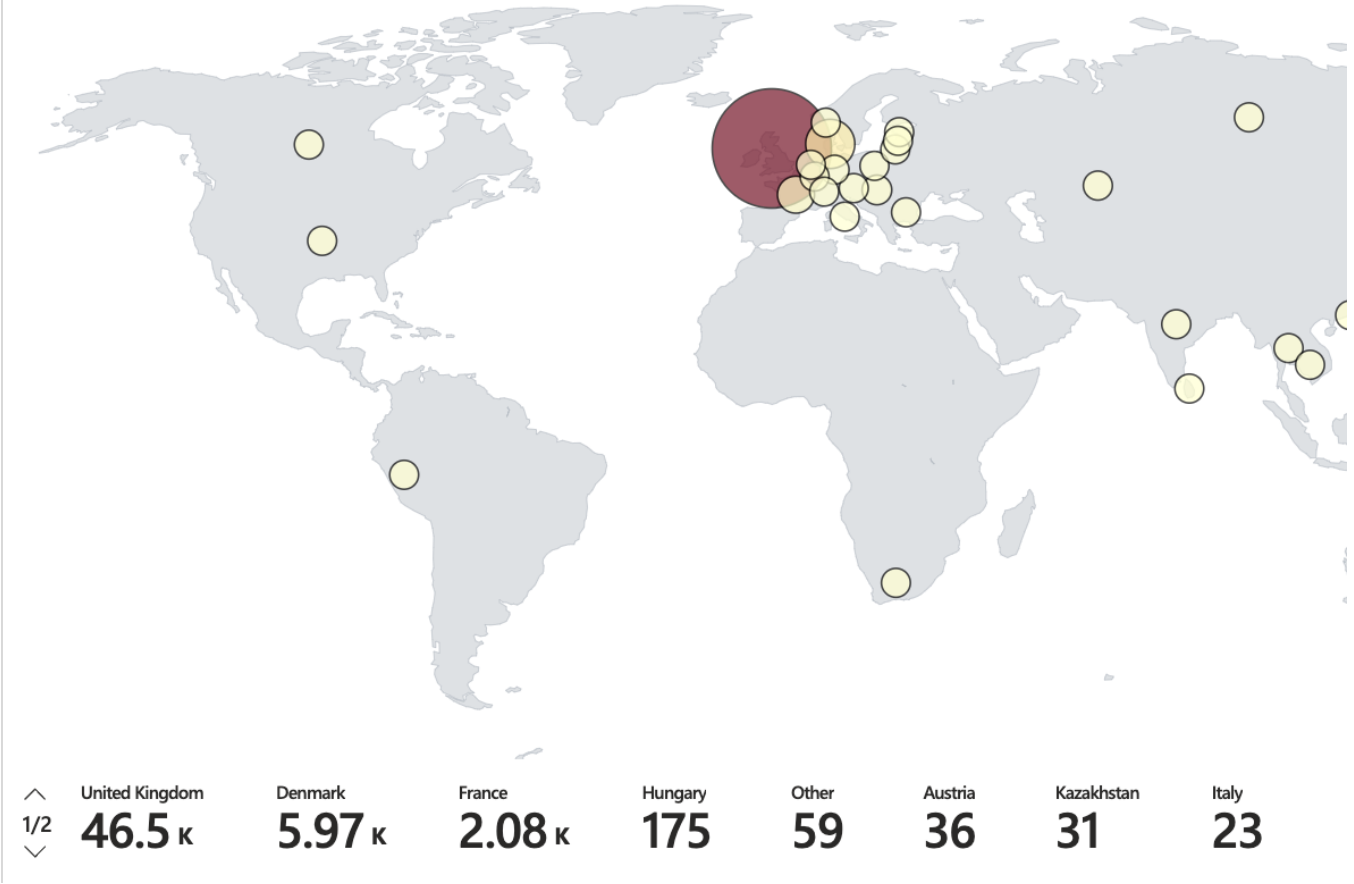
Example of different MFA modalities

# DEMO> RISK DETECTIONS [REGIONAL VIEW]

Sign-in risk levels




Total sign-in risk events by country



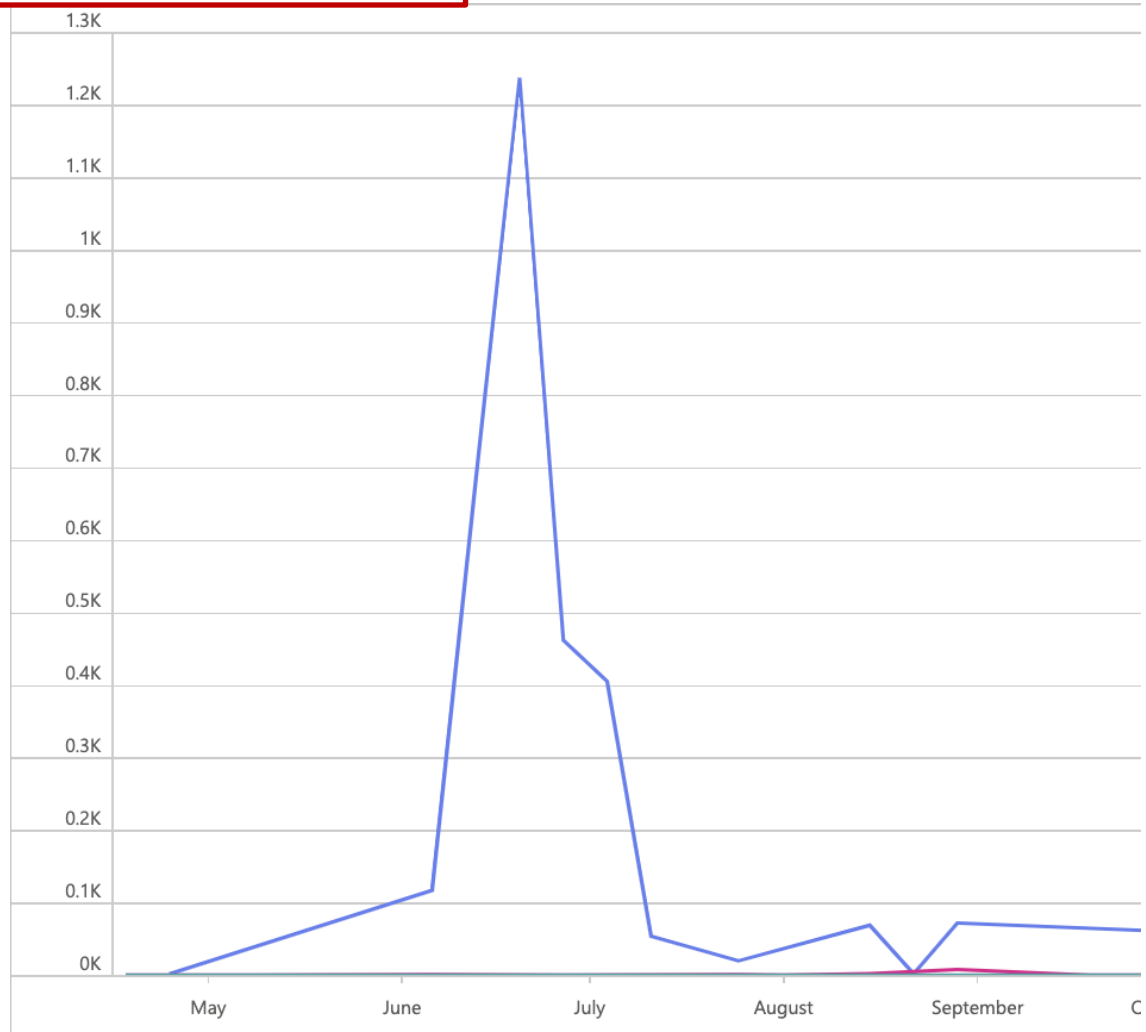
# DEMO> RISK DETECTIONS

**Total - Risky sign-ins by risk type and risk level**

Search

| Detection type | high | low | Mediu... |
|---|---|---|---|
| ["anonymizedIPAddress"] | 9 | 2708 | 416 |
| ["unfamiliarFeatures"] | 2 | 21 | 2 |
| ["unfamiliarFeatures","unlikelyTravel"] | 0 | 4 | 1 |
| ["anonymizedIPAddress","passwordSpray"] | 0 | 0 | 3 |

**Risky sign-ins by risk type over time**



# DEMO> RISKY SIGN-INS DETAILS

Details - Risky sign-ins by risk type and risk level

Search

| SignIn Risk | Risk Type | UserId | Identity | IPAddress | Location |
|---|---|---|---|---|---|
| low | ["unfamiliarFeatures","unlikelyTravel"] | | | 5.185 | |
| low | ["unfamiliarFeatures","unlikelyTravel"] | | | 5.185 | |
| low | ["unfamiliarFeatures","unlikelyTravel"] | | | 7.105 | |
| low | ["unfamiliarFeatures","unlikelyTravel"] | | | 2.28 | |
| medium | ["unfamiliarFeatures","unlikelyTravel"] | | | 5.133 | |

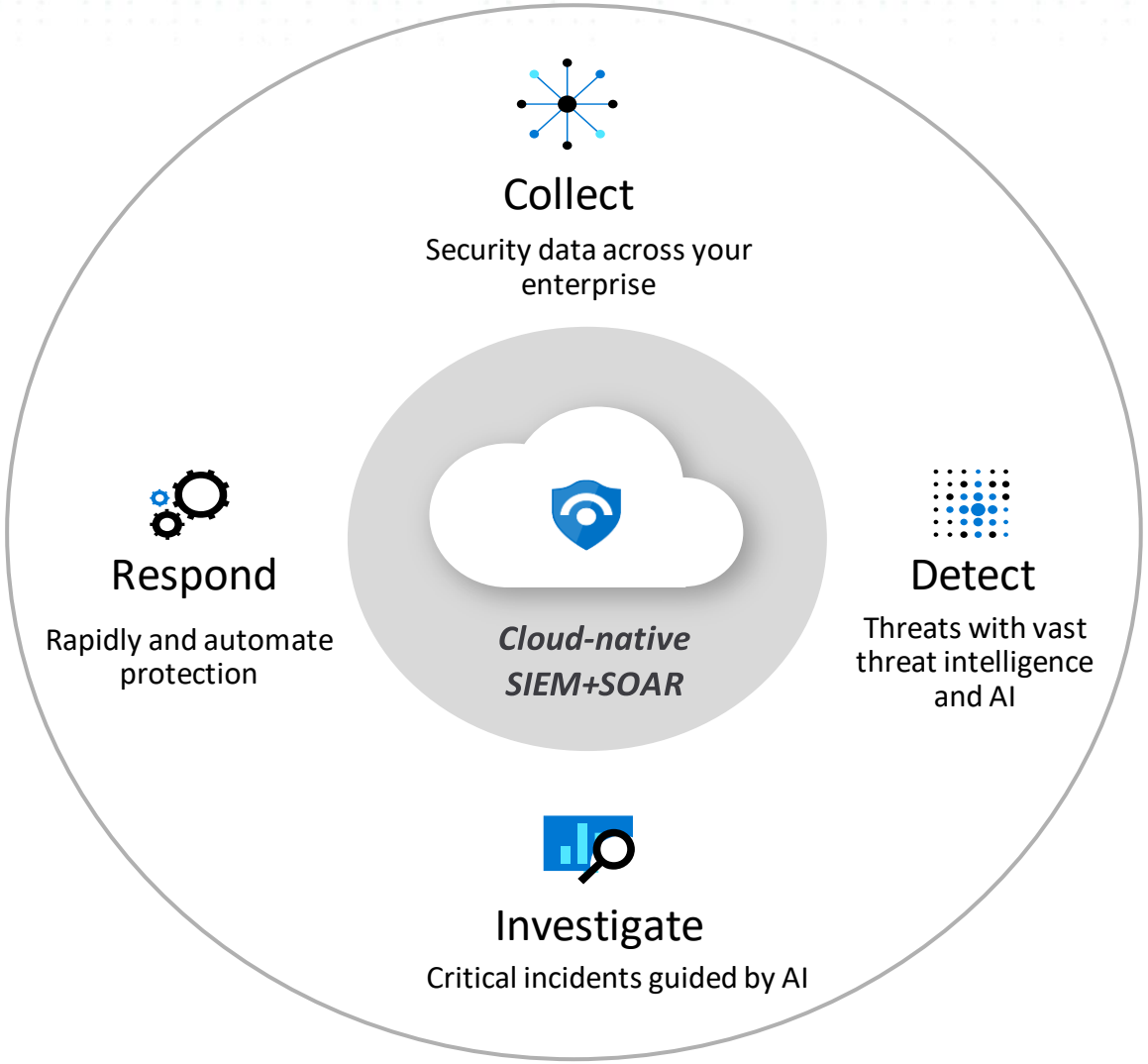
Risk detection details

Search

| TimeGenerated | Identity | OperationName | Details | Result |
|---|---|---|---|---|
| | | Issue an id_token to the application | No additional details | success |
| | | Evaluate conditional access policies | CA-SignIn | success |
| | | Validate local account credentials | No additional details | success |

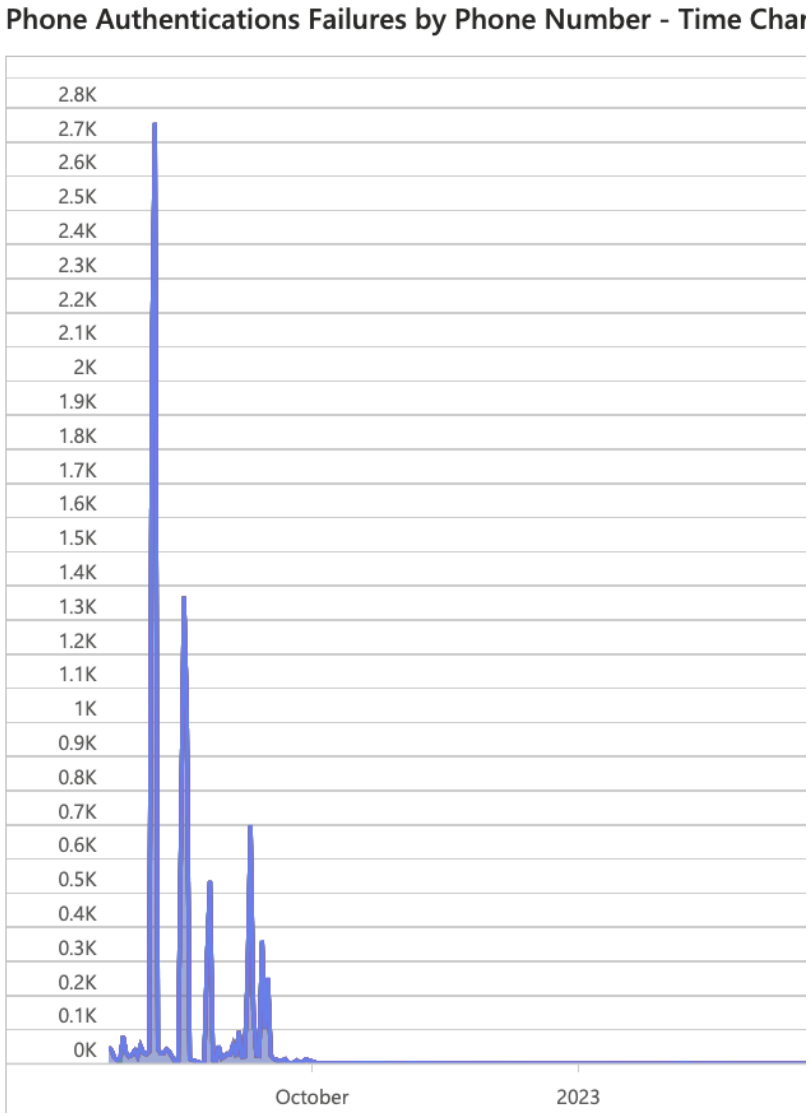
# Lesson: Observability & Orchestration

# OBSERVABILITY & ORCHESTRATION -> SIEM + SOAR



# DEMO> OBSERVABILITY & ORCHESTRATION

# DEMO> MONITORING [MFA ATTACK – IRSF]




Excessive MFA[SMS/voice] failures

# DEMO> DETECT [MFA IRSF ATTACK]


| OperationName | Success | Failure | Success_Rate | Failure_Rate |
|---|---|---|---|---|
| Send SMS to verify phone number | 328.703 K | 185.263 K | 63.95% | 36.05% |
| Verify one time password | 1.336 K | 170 | 88.71% | 11.29% |
| Verify phone number | 577 | 36 | 94.13% | 5.87% |

# DEMO> ALERT [MFA IRSF ATTACK]

## Create an alert rule ...

KQL ALERT RULE:
*MFA[SMS/voice]*
*Success rate*
*below 95%*

Scope | **Condition** | Actions | Details | Tags | Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * ⓘ — Custom log search

See all signals

Define the logic for triggering an alert. Use the chart to view trends in the data. Learn more

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

```
let start = ago(24h);
let end = now();
let threshold = 95; //% trigger.
AuditLogs
| serialize TimeGenerated, CorrelationId, Result
| make-series TotalRequests=dcount(CorrelationId) on TimeGenerated in range(start, end, 1h)
| mvexpand TimeGenerated, TotalRequests
| serialize TotalRequests, TimeGenerated, TimeGeneratedFormatted=format_datetime(todatetime(TimeGenerated), 'yyyy-M-dd
[hh:mm:ss tt]')
```

# DEMO> ALERT [MFA IRSF ATTACK]

Microsoft Azure

## Your Azure Monitor alert was triggered

We are notifying you because there are multiple counts of MFA[IRSF] Alert Firing".

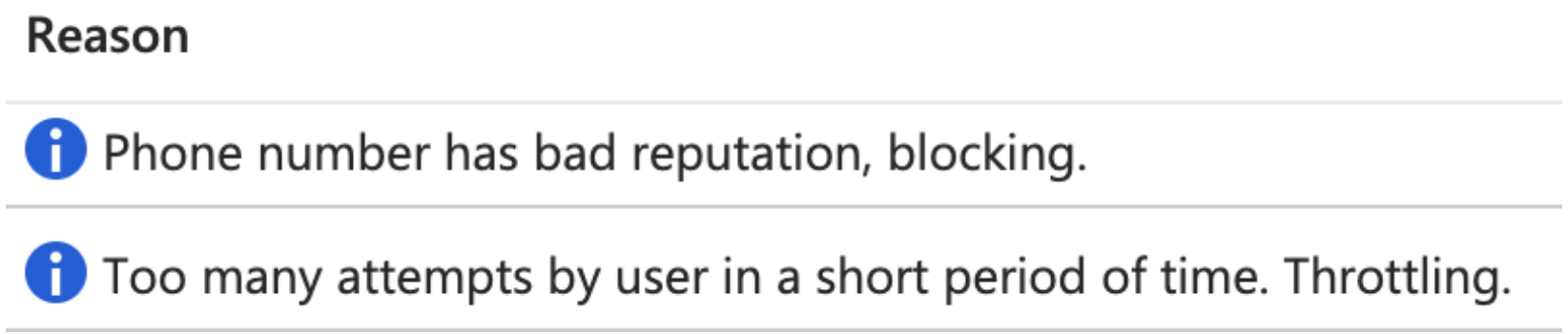
### Essentials

| | |
|---|---|
| **Name** | MFA [SME/Voice] success rate has been dropped below 95% |
| **Description** | ATTN: Potential IRSF attack. |
| **Severity** | 1 |

Alert via email.

Alternative methods [Webhook/SMS]

# DEMO> AUTOMATIC RESPONSE [MFA IRSF ATTACK]




```
Automatic response to IRSF attack [block phone numbers with bad
reputation + throttling]
```

# Apply What You Have Learned Today

# Apply What You Have Learned Today

- Next week you should
  - Identity key modalities & businesses of customer identities : mobile, web, api, IoT etc.
  - Determine key stakeholders for each modalities & business.
- In the next month following this presentation you should:
  - Design system with defense in depth principle in mind.
  - Iteratively apply four stages to design: *establish intent, establish proof, observe and orchestrate.*
- Within three months
  - Implement security controls pertaining to each stage (WAF, MFA, SIEM, SOAR, etc.)
  - Continuously improve the maturity of four stages mentioned above.


# Resources

# Questions?