



# Zero Trust Security for B2C Architectures

Andrew Cameron, Technical Fellow – IAM

General Motors

#identiverse



# **Andrew Cameron**

Technical Fellow - IAM

**General Motors**

# Defining the Vehicle, with Software

TRANSPO / GM / TECH

**GM's new software platform will enable over-the-air updates, in-car subscriptions, and maybe facial recognition**



Photo by Sean O'Kane / The Verge

/ Ultifi will start rollir vehicles in 2023

By [Andrew J. Hawkins](#), transportation editor with 10+ years covers EVs, public transportation, and aviation. His work has York Daily News and City & State.  
Sep 29, 2021, 3:00 PM EDT | [0 Comments](#) / [0 New](#)



TRANSPO / GM / ELECTRIC CARS

**GM created its own open-source software protocol and wants its competitors to use it**



/ The automaker is joining the Eclipse Foundation to underscore its commitment for more open communication standards



[COMPANY](#) ▶

[COMMITMENTS](#) ▶

[STORIES](#)

[BRANDS](#)

[Customers](#)

[Careers](#)

[Investors](#)

[Newsroom](#)

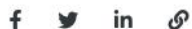


Illus

Newsroom:

## GM's Safe Deployment of Hands-Free Technology Shapes Ultra Cruise

Ultra Cruise will debut a unique sensor suite, providing the system with a 360-degree view of the vehicle's surroundings



- Ultra Cruise-equipped vehicles will have more than 20 sensors
- The driver attention system will continue to play a key role in ensuring driver attention

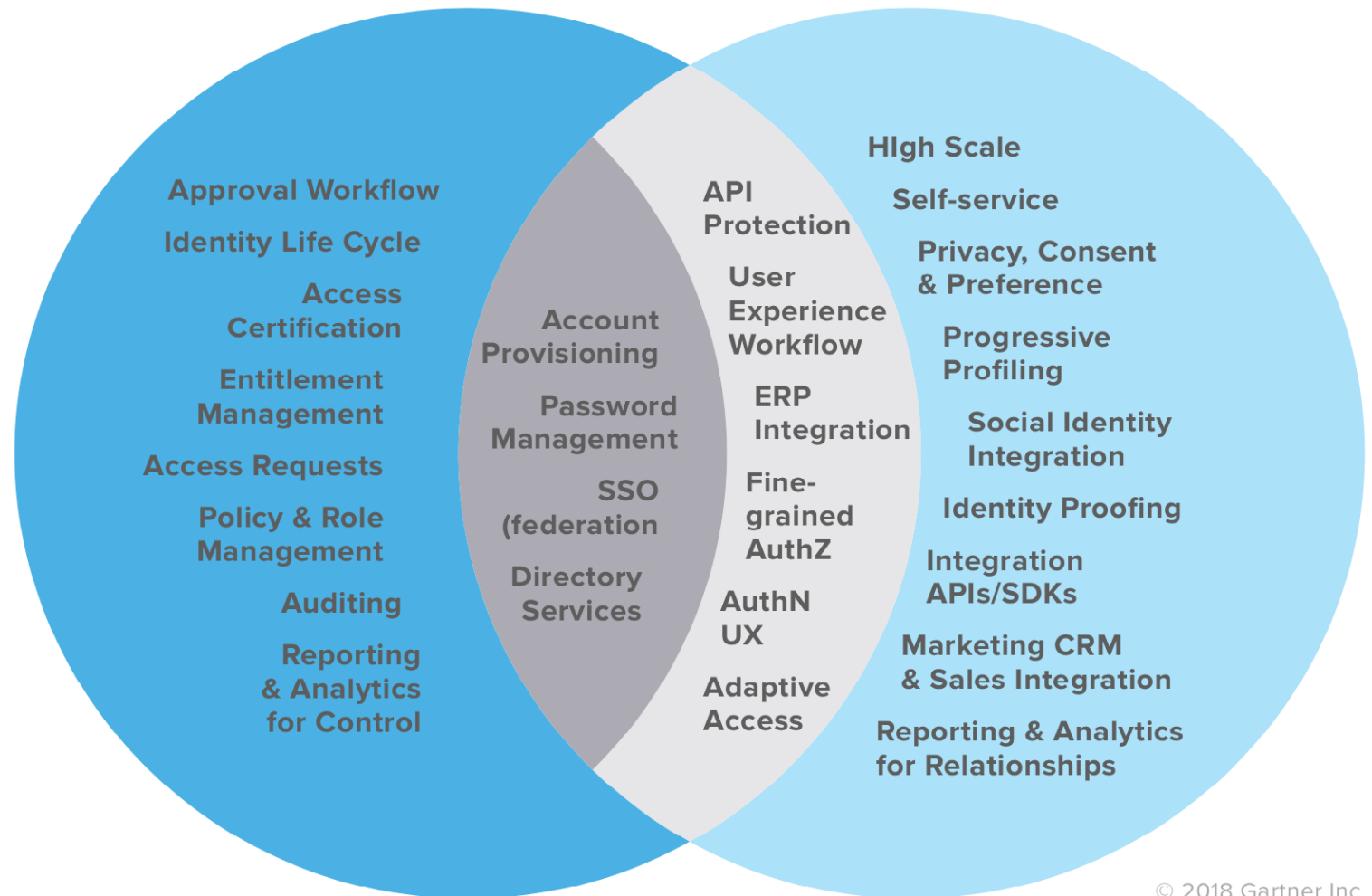
# Defining The Architecture

# B2C (CIAM) vs B2E (Workforce) Identity

CIAM and IAM  
Feature Overlap  
is Increasing

- **Workforce IAM**
- **Consumer IAM**

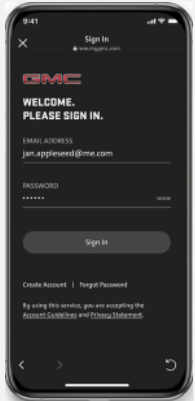
Gartner Figure 3, CIAM  
and Workforce IAM Feature  
Overlap Is Increasing,  
*Top 5 Trends in CIAM  
Solution Design*,  
5 March 2018



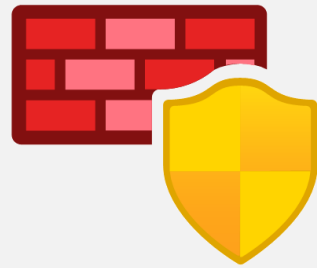
Source: Gartner (March 2018)

© 2018 Gartner Inc.

# B2C Architecture – Key Components



**Client**



**Edge Protection**



**IAM Platform**



**Backend Resources**

# Client Protection

# Protecting The client

---

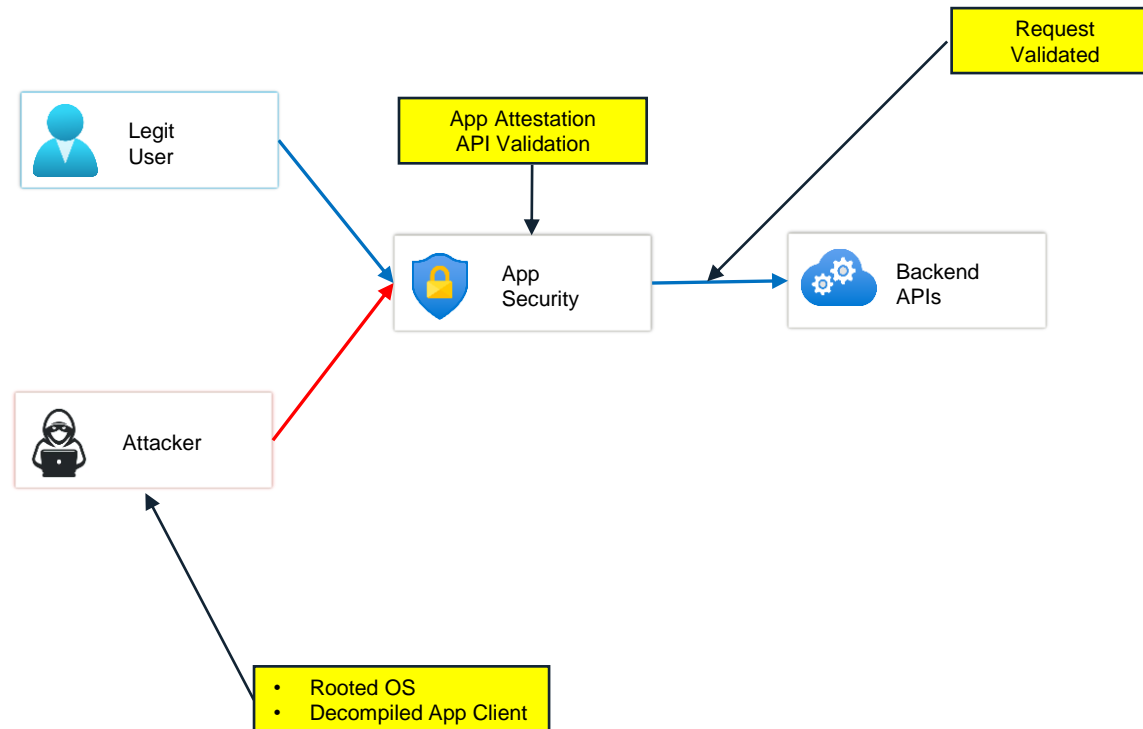
- Protect the Identity with Modern Auth Protocols
  - Use OIDC Auth Code Flow w PKCE
  - Use Integrated Risk Based MFA
- Identity Federation
  - Use for identity validation only
- Protect the Application with Mobile App Security
- WebAuthN is the way forward
  - Passkeys!

## OAuth & OpenID Connect



# Protecting The client – Mobile App Security

- Protect the Application with Mobile App Security
- Enables attestation from mobile app platform providers
- Ensures API requests are from valid clients



# Edge Protection

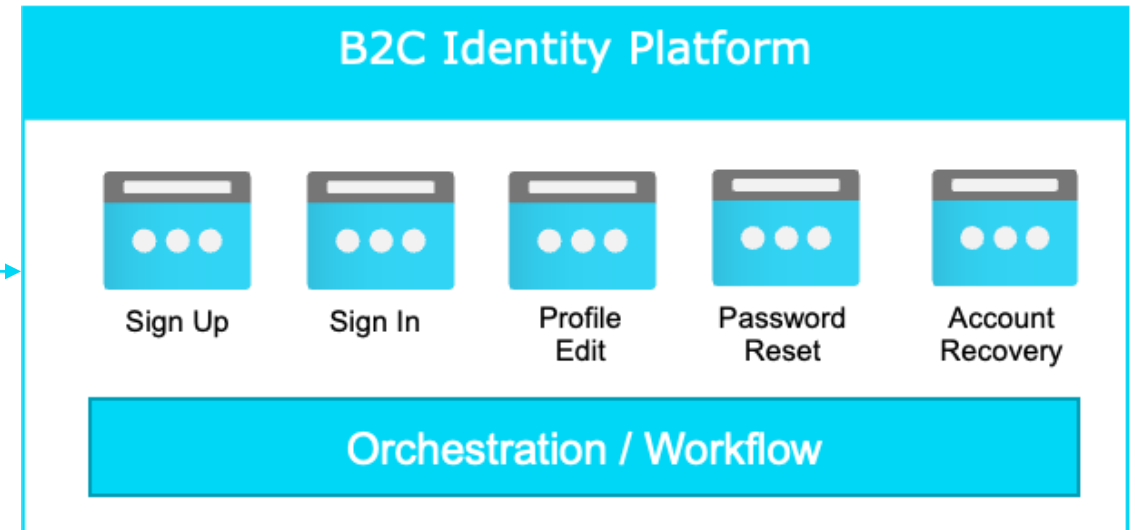
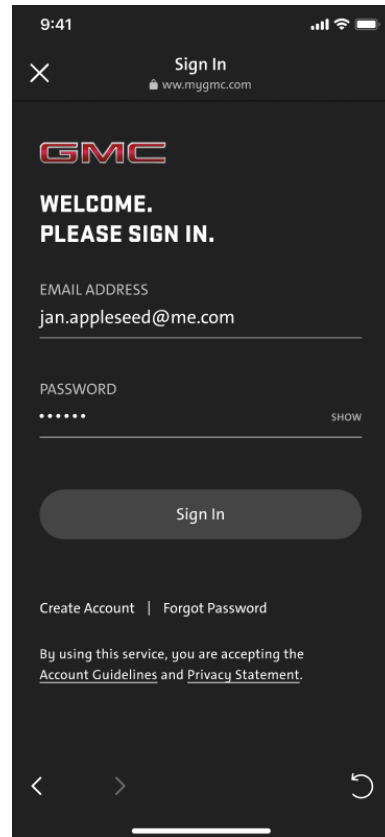
# Edge Protection Components

Component	What it Does	How it Protects
Web Application Firewall	<ul style="list-style-type: none"><li>• First line of protection on open internet</li><li>• Rule based enforcement (i.e., based on OWASP Top 10)</li></ul>	<ul style="list-style-type: none"><li>• Uses threat intelligence to detect malicious traffic and provide enforcement</li><li>• Stops malicious traffic from entering corporate boundary</li></ul>
Content Delivery Network	<ul style="list-style-type: none"><li>• Cloud component that delivers content to endpoint devices</li></ul>	<ul style="list-style-type: none"><li>• Enables custom (hosted) domains to be protected</li><li>• Streamlines cert management of custom domains</li></ul>


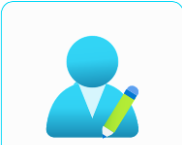

# Identity Platform Protection

# B2C Identity Platform

- B2C Identity Platform implements core user scenarios (User Journeys)
- Journeys are customizable, built upon a common workflow / orchestration layer
- Abstracted from application functionality

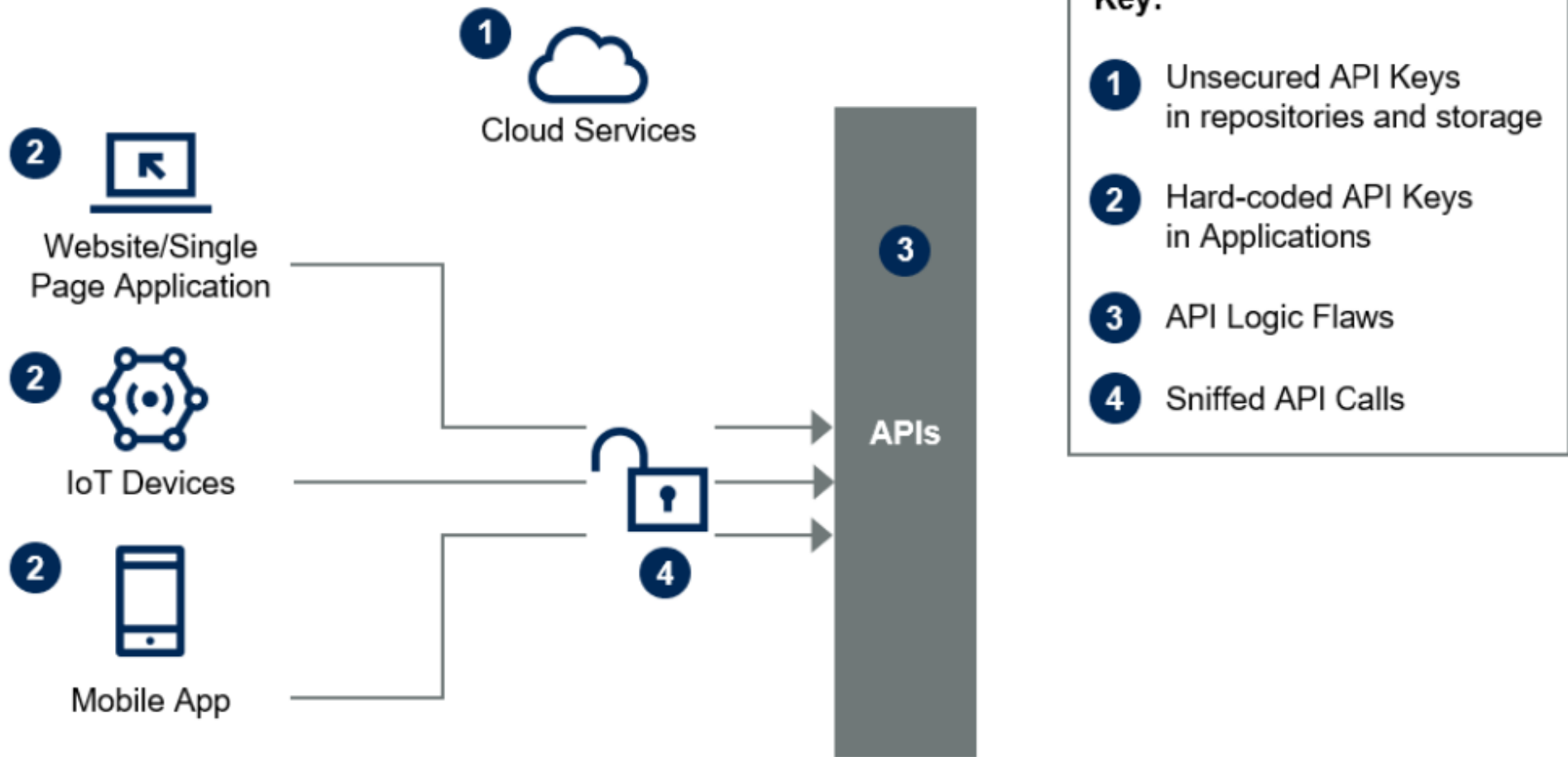


# Protect the Identity Platform

Component	How Its Vulnerable	How to Protect It
 IDP Endpoints	<ul style="list-style-type: none"><li>• Denial of Service Attacks</li><li>• Bot based attacks</li><li>• Cloud Resource Exhaustion</li></ul>	<ul style="list-style-type: none"><li>• WAF Policies (Bot detection, OWASP Top 10 Rule protection)</li><li>• Secure custom domains, certificate management / rotation</li></ul>
 Sign Up Flow	<ul style="list-style-type: none"><li>• Fraudulent accounts</li></ul>	<ul style="list-style-type: none"><li>• Enable Fraud Protection services</li><li>• Block fake email services</li><li>• Enable Identity proofing for email and phone number validation</li></ul>
 Sign In Flow	<ul style="list-style-type: none"><li>• Brute force logins</li><li>• Password Spray attacks</li><li>• Leaked credentials</li></ul>	<ul style="list-style-type: none"><li>• Detect Risky logins with Identity Protection polices</li><li>• Detect Risky users with Threat intelligence validation</li></ul>

# **Backend Resource Protection** **(aka API Security)**

# Typical Vulnerability Paths - APIs



# OWASP API Security Top 10 (2023 RC)

OWASP API Security Top 10 2019

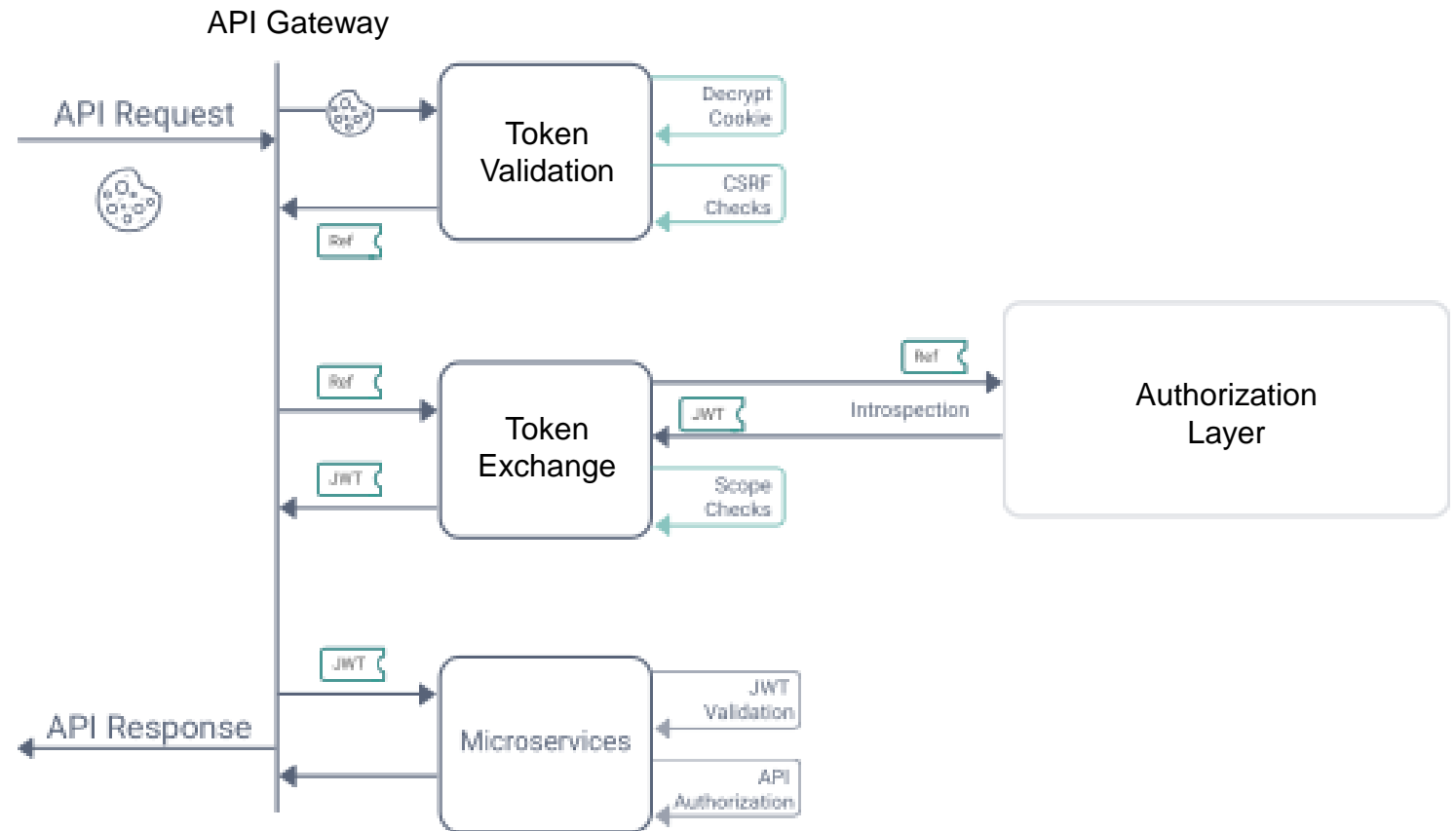


OWASP API Security Top 10 2023 RC

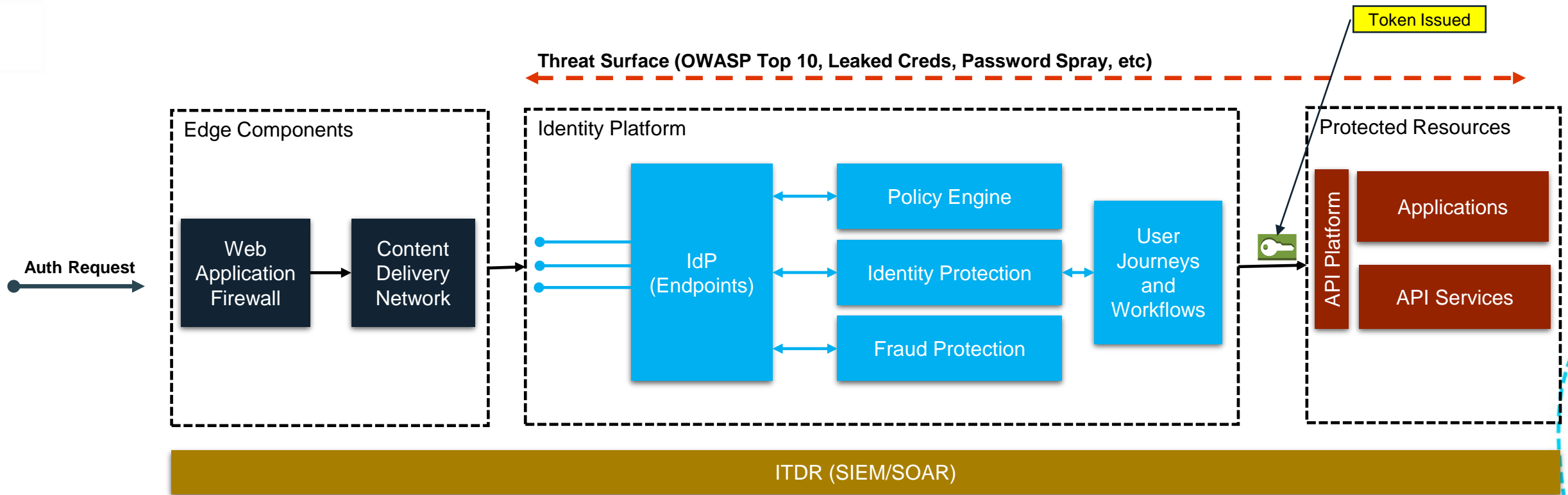


# Protect the backend - Recommendations

- Use an API Gateway
- Use Token Based Authentication
- Claims based authorization
- Understand token management patterns
  - Phantom Token Pattern
  - Token Handler Pattern

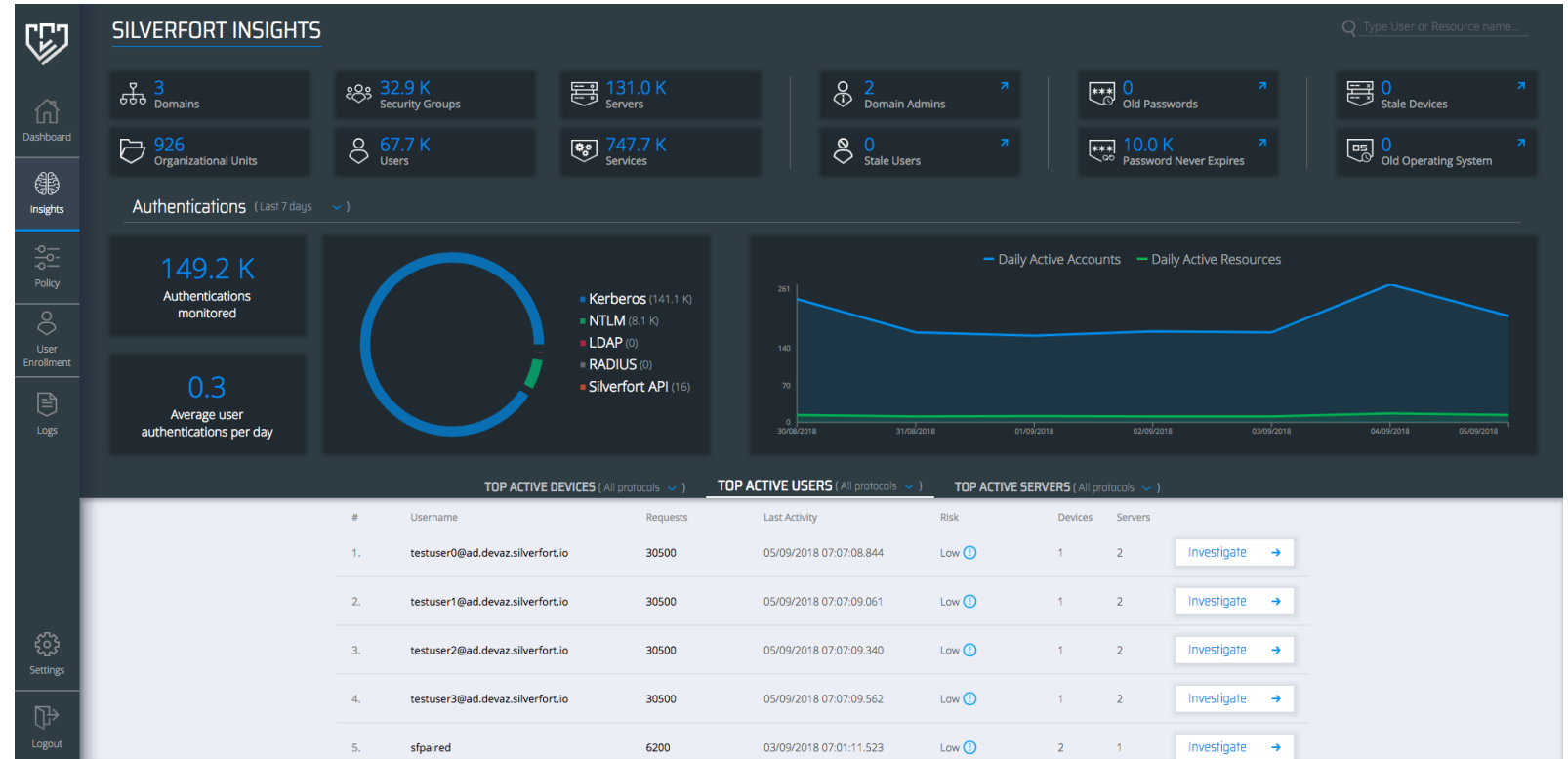


# End To End View



# The importance of Telemetry - ITDR

- Become **very familiar** with ITDR (Identity Threat Detection and Response)
- Monitor for specific attacks on the identity platform
- Correlate your logs from all sources within the architecture
- Enable Alerting for types of malicious behavior
  - Spikes in HTTP requests
  - New account creation
  - Failed login volume



# Takeaways

# Takeaways

- Consider making IAM part of the Security Organization
- API Security is the primary component of a strong identity strategy
- Comprehensive Telemetry is a **must** from end to end, continuously evaluate your risk posture and update enforcement policies
- Work with your business to balance Security and User Experience, but... **remember who you represent!**
- Avoid splintering Identity User Journeys, encourage progressive profiling of capturing user data across journeys



# THANK YOU!