Case Study

LoginRadius Strengthens CIAM Platform Security Through AppSecure's Offensive Penetration Testing

Company Size	Asset type	Key Result
51-200	CIAM Web App & APIs, Cloud Platform	100% Critical Risks Resolved

Client overview: LoginRadius

LoginRadius is a global Customer Identity and Access Management (CIAM) platform trusted by enterprises to secure millions of digital identities worldwide. The platform enables secure authentication, identity lifecycle management, and privacy protection across web and mobile environments while supporting large-scale cloud deployments.

Challenge

Ensuring secure tenant isolation and identity enforcement at scale

Operating a CIAM platform requires consistent enforcement of authentication, authorization, and tenant isolation controls across shared infrastructure.

While LoginRadius maintained a strong security baseline, independent adversarial validation was essential to:

- Validate tenant isolation across shared cloud infrastructure
- Stress-test authorization and privilege enforcement logic
- Analyze authentication and identity workflow behavior
- Establish independent technical assurance for enterprise trust

Security controls needed to remain consistent across complex identity interactions and real-world attack scenarios.

Our unique approach

Black-box adversarial testing driven by real exploitability

AppSecure executed a comprehensive black-box penetration test simulating an external attacker with no credentials or insider access.

Company
LoginRadius

Headquarters
Canada

Industry
Customer Identity &
Access Management
(CIAM)

Department
Product & Engineering

Service Used
Offensive Penetration
Testing

Through structured reconnaissance and adversarial testing, AppSecure:

- Identified exposed authentication and identity components
- Enumerated APIs and external interaction points
- Analyzed session lifecycle and identity state behavior
- Evaluated tenant boundary enforcement
- Tested privilege and authorization validation logic
- Assessed authentication and session handling consistency
- Analyzed identity workflows for logic-driven attack paths

Each identified weakness was validated for practical exploitability and real-world impact. The assessment aligned with OWASP Top 10 and OWASP ASVS while prioritizing exploitability over compliance-only validation.

Hear it from our client, LoginRaius

> "What stood out was the focus on real-world exploitability rather than compliance checklists. AppSecure helped us validate how the platform would hold up against realistic attack scenarios."
>
> **Kundan Singh**
> VP, Product & Engineering, LoginRadius

Building a Resilient Security Foundation

AppSecure's customized approach drove measurable security improvements for LoginRadius

- 100% of critical findings resolved and validated within 2 weeks
- High-severity findings remediated within defined timelines
- Strengthened multi-tenant isolation controls
- Improved authorization and access control validation
- Enhanced API and session validation mechanisms
- Strengthened authentication and identity workflow protections
- Reduced risk of logic-based exploitation
- Security improvements integrated into the engineering roadmap

Each finding was prioritized based on real-world impact, enabling faster remediation, structured validation, and measurable security improvement without disrupting product velocity.

Hear it from our client, Healthkart

> "The engagement felt highly collaborative, with AppSecure working closely alongside our security and engineering teams at every stage."
>
> **Kundan Singh**
> VP, Product & Engineering, LoginRadius

A Trusted Offensive Security Partner

LoginRadius's engagement with AppSecure demonstrates how focused adversarial testing strengthens complex identity platforms. By identifying and resolving real security risks across authentication, authorization, and tenant isolation layers, LoginRadius enhanced platform resilience and reinforced enterprise trust.

The assessment delivered independent validation aligned with OWASP ASVS and Top 10, supporting enterprise vendor risk reviews, SOC 2 and ISO 27001 assurance initiatives, and customer procurement evaluations.

Through this engagement, LoginRadius strengthened long-term platform resilience, reduced practical exploit risk, and reinforced its commitment to protecting millions of digital identities worldwide.