AppAcuity, Inc.

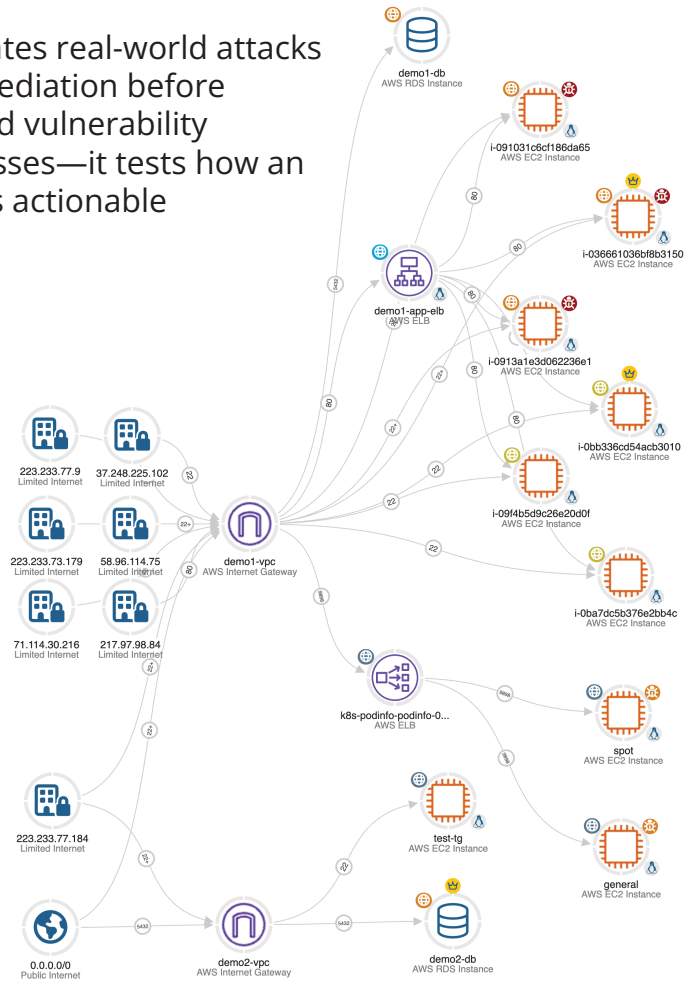
Adversarial Exposure Validation for AWS

Identify Your Exposures Before Hackers Exploit Them

Have You Tested Your Exposures Like an Attacker Would?

What is Adversarial Exposure Validation (AEV)?

(AEV) is a proactive approach to security that simulates real-world attacks to validate exposure, prioritize risks, and guide remediation before attackers strike. Unlike traditional attack surface and vulnerability management, AEV goes beyond identifying weaknesses—it tests how an adversary would exploit them, giving security teams actionable intelligence to harden defenses effectively.



AppAcuity Answers These Critical Questions

Which exposures matter most?

Pro-active validation prioritizes exploitable risks based on real attack paths, ensuring security teams focus on the most critical threats.

How would attackers get in?

By simulating real-world attacks, AppAcuity uncovers blind spots and maps potential breach paths before they're exploited.

What should be fixed first?

AEV identifies which fixes truly reduce risk, eliminating guesswork and optimizing remediation efforts.

AppAcuity's AEV platform transforms SecOps from reactive to proactive, ensuring your defenses are tested, validated, and resilient against real-world threats.

If you lack clear, validated insight into how and where your AWS assets are exposed to real-world attacks, invest just 1 hour with us – we'll show you exactly what attackers see and how to stay ahead of them.

See your cloud environment from the attacker's perspective

Real-World Exposure

Exposed Jenkins Repository

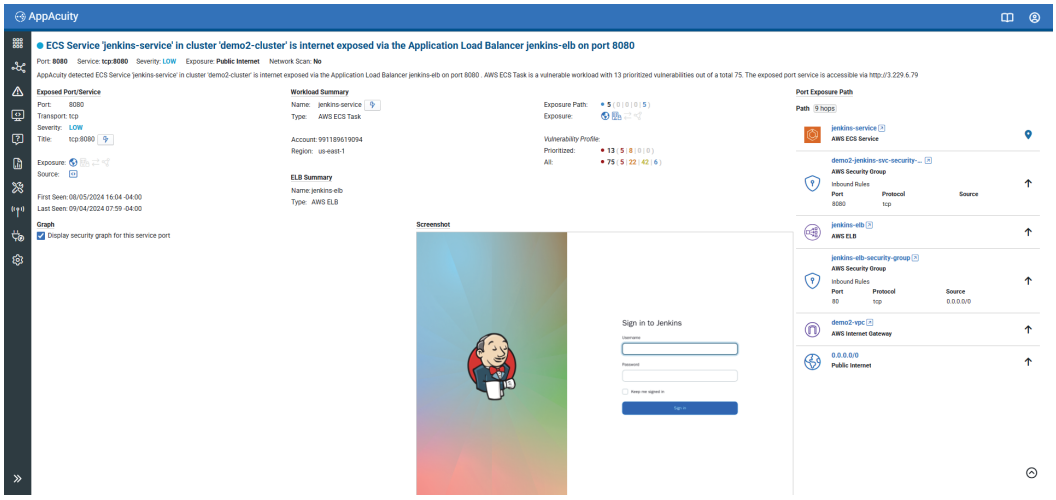
AEV detected a publicly accessible repository with sensitive code and credentials.

Validated Exploitation Risk

AEV scan confirmed attackers could access and manipulate CI/CD pipelines.

Immediate Remediation

Teams secured access, rotated credentials, and strengthened authentication.



Example report finding showing details of a validated exposure

AppAcuity's solution identifies, validates, and prioritizes real-world exposures -- like an unsecured Jenkins repository – before attackers can exploit them. By continuously testing defenses, AppAcuity helps ensure security teams stay ahead of emerging threats.

From Deployment to Insights in Minutes

Set up in under 10 minutes and gain actionable security insights immediately after your first scan.

About AppAcuity

AppAcuity, Inc. is a global provider of advanced security solutions that organizations can rely on to pro-actively enhance their security posture. Building on decades of visionary leadership creating long-lasting solutions for the Fortune 500, Department of Defense, Tier 1 telcos and Managed Service Providers around the world, our team is focused on continuous innovation to fill security and visibility gaps and help customers and partners avoid a security breach.

Contact us to learn more

1-888-238-7189 info@appacuity.com

AppAcuity, Inc. 250 Monroe Ave NW, Ste 400, Grand Rapids, MI 49503