praetorian

DATA SHEET

Application Penetration Testing

KEY BENEFITS

Assess the software technology stack, from the service mesh and managed services to proprietary application logic

Identify security risks associated with design, implementation, and configuration

Receive solutions to mitigate identified vulnerabilities

YOUR CHALLENGE

Your organization's applications rely on cloud-first technology stacks. That means the data and secrets you need to protect could be vulnerable to the full range of software- and cloud-based attacks that adversaries are continually expanding. You need assurance that your cybersecurity strategy is comprehensive, that your data and that of your clients is as secure as possible, and that your applications meet any applicable industry regulatory requirements.

OUR SOLUTION: CAPABILITIES OVERVIEW

Praetorian's Application Penetration Testing engagements provide clients with a timely, tailored, and thorough assessment of their product's cybersecurity from an adversarial perspective. Our assessments include a comprehensive analysis of the building blocks that make up modern applications, including the service mesh, managed services, and application-layer logic. We conduct assessments in one of the following two ways, depending on the client's needs:

- **Framework-based**

  What it does: benchmarks your application against industry standards such as OWASP ASVS or MASVS.

- **Goal-based**

  What it does: pursues attack paths that target specific critical assets based on a collaboratively-constructed custom threat model.

The application's deployment characteristics (and threat model, if applicable) determine whether we focus on externally facing attack surfaces or the security of private APIs, container breakout scenarios, and other secondary attack surfaces.

Using a combination of manual and automated techniques, we can identify vulnerabilities ranging from classical web application vulnerabilities on the OWASP Top 10 to complex attack paths that chain together multiple weaknesses. Manual techniques, such as code review, log analysis, and analyzing memory in a debugger provide depth of coverage. They also give us the right opportunities to emulate attackers in order to find subtle vulnerabilities. Automated techniques, such as fuzzers and custom enumeration scripts, provide breadth of coverage and ensure we are finding as much as possible.

Once we have identified the material risks in the application, Praetorian collaborates with your team to develop a pragmatic, actionable remediation plan. This is always a union of technical and business considerations that will meet the client's security needs without derailing the product roadmap.

SERVICES COMPARISON

	Foundational Application Penetration Test	Risk-Informed Security Assessment
TESTING REQUIREMENTS		
Authentication Credentials	✓	✓
Source Code Access	optional	✓
Design Documentation Access	optional	✓
Security & Engineering Interviews		✓
FEATURE COMPARISON		
DAST & Vulnerability Scanning	✓	✓
OWASP Top 10 Coverage	✓	✓
Business Logic testing	✓	✓
Code Assisted Testing	optional	✓
SAST & Manual Code Review		✓
Threat Modeling		✓
DELIVERABLES		
PDF Report	✓	✓
CSV/Excel Vulnerability Export	✓	✓
Engagement Summary Letter	✓	✓
Security Benchmark Comparison	✓	✓
Threat Model Diagram(s)		✓
Abuse and Test Case Matrices		✓
Strategic Recommendations		✓

WHY PRAETORIAN

Praetorian's clients gain maximum benefit from our decade of experience and deep technical expertise in application penetration testing. Our team is equally adept with cloud-first applications and on-premises deployments, and can assess server-side, desktop, and mobile applications. Praetorian's engineers bring a creative, adversarial mindset to every engagement.

We pair that expertise with a focus on the client experience, tailoring each engagement to the client's business needs in order to provide actionable findings. You can rely on us to ask deep questions, work closely with your teams, and provide direct, clear feedback on what we find. Our team keeps your bigger picture in mind so we can help your company understand both the ground truth about your security program and its implications for your company's future.

WHO NEEDS THIS SERVICE

- **Organizations** wanting to analyze risk to make security a central part of their business proposition. These engagements are highly productive, as Praetorian can help identify the best-in-class security controls needed to reach specific goals, then retest to verify those controls are implemented properly.
- **Security teams** requiring independent, trusted security reviews of their products to meet customer- or regulatory-driven requirements.

DELIVERABLES

Executive Summary

Concise explanation of engagement goals, significant findings, business impacts, and strategic recommendations

→ Upon request, a letter of attestation

Engagement Outbrief Presentation

Similar to the executive summary, presented to the audience of your choosing

Technical Findings Report

Detailed description of issues and the methodology used to identify them, as well as an impact assessment for each

Praetorian Security, Inc.
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive security engineering company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today's leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios.