



CHARIOT



www.praetorian.com
@praetorianlabs
info@praetorian.com

Praetorian's Chariot Attack Surface Management Platform and Managed Security Service

The total attack lifecycle solution

Advances in SaaS and DevOps that transform your business also expand the attack surface—all the ways adversaries can exploit your connections to the internet or cloud. Knowing the unknowns is the first step, but the attack surface keeps changing and your risks are multiplied by ransomware and talent shortages. It's time security goes on offense. Cut through noise, extend your team, and reduce false positives to zero with Praetorian's all-in-one offensive security service.

Beyond an ASM Product, Chariot® Managed Service is a Partnership

Chariot Identify provides comprehensive attack surface discovery by combining outside-in adversarial expertise with inside-out integrations for cloud systems, container registries, source code managers, and CI/CD pipelines.

Chariot Attack prioritizes risk with zero false positives. Our offensive operators exploit dangerous exposures to confirm risk and demonstrate impact using constant, automated mapping of the evolving attack surface.

Chariot Detect retraces compromise paths to ensure you can detect and respond to real attacks. Using automation and MITRE ATT&CK expertise, we quickly identify gaps and benchmark your detection abilities.

Chariot Prevent enables you to flag security policy violations and enforce compliance by allowing you to define policy as code.

Use Cases and Risks

- Attack Surface Management
- Shadow IT Identification
- M&A Due Dilligence and Post Integration
- Subsidiary Risk Management
- Cyber Insurance Premium Reduction
- Defensive Investment Validation

Key Benefits

Comprehensive Attack Surface Mapping

Using AI-driven outside-in and inside-out mapping techniques, Chariot continuously and comprehensively catalogs your organization's external attack surface.

Modern and Advanced Threat Simulation

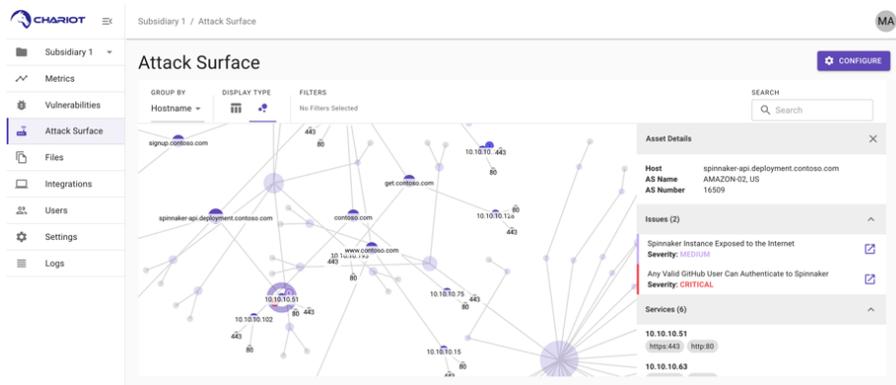
Praetorian's offensive security engineers rapidly adopt and codify new attacker tactics and techniques to pressure test each customer's cybersecurity posture against the latest threats.

Zero False Positives

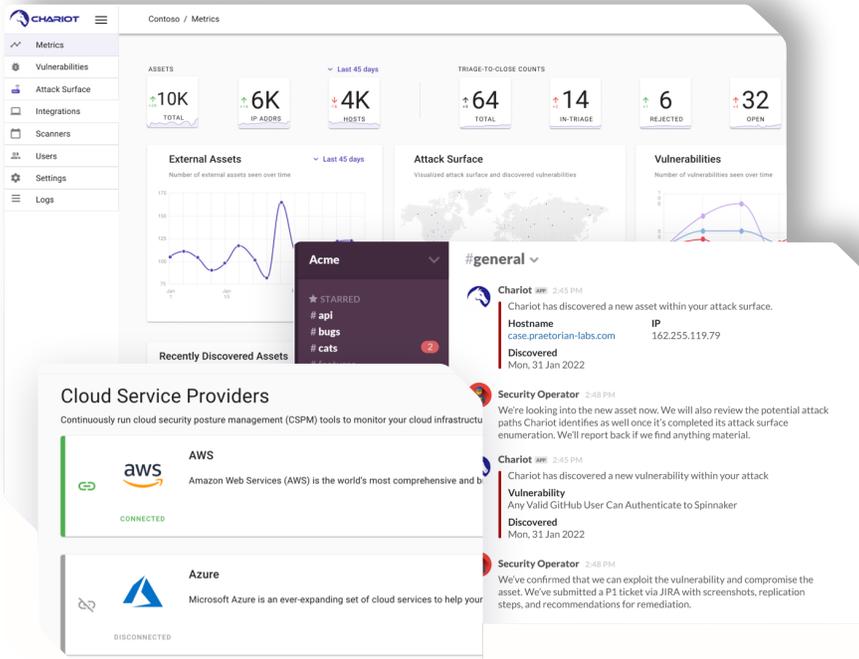
Our security experts validate vulnerabilities to remove false positives, confirm the criticality of potential security exposures, and demonstrate impact through compromise.

Personalized Concierge Service

Security experts operate as an extension of your security team, working within your collaboration channels to alert you on critical risks, align on mitigation strategies, validate remediation, and improve detection and prevention controls.



Chariot's All-in-One Managed Service Enables a Trusted Partnership that Helps Your Team Address Complex Risks



- 1 | Enumerate your organization's attack surface
- 2 | Find weaknesses the same way an attacker does
- 3 | Demonstrate significance through compromise
- 4 | Verify remediation has mitigated the risk
- 5 | Improve detection and prevention controls

Free Trial

Register on www.praetorian.com to learn more about offensive security managed services.

“The Chariot platform pressure tests our cybersecurity program's effectiveness every single day.”

— Melody Hildebrandt, CISO, FOX

About Praetorian

Praetorian delivers the only end-to-end security platform and managed service that acts like attackers to protect customers. As an extension of your security team, Praetorian helps enterprises achieve business resilience by continuously discovering assets, contextualizing their relationship and import, pinpointing vectors of compromise, and personalizing protection to remediate future risk. Engage with Praetorian offensive security engineers and experts to locate your critical exposures and continuously validate your cybersecurity program. Follow at www.praetorian.com or [Twitter](#) and [LinkedIn](#).