GUIDEPOINT
SECURITY

Bringing The Hypothetical To Reality

We Bring Both Worlds Together to Give You Real, Tangible Information

Our Cloud Penetration Test focuses on current and emerging cloud-specific threats to help take you from the hypothetical to the actual with exploitation and evidence.

Leveraging the expertise of both our Cloud Security and Threat & Attack Simulation teams, we have created a tailored service for cloud penetration testing to solve two emerging challenges:

1. **Traditional penetration testing methodologies are NOT cloud-native** - Penetration testers have defined robust processes and skillsets to test on-premise environments. Still, the responsibilities, technologies, threats, and their related vulnerabilities are different in a shared security model.

2. **Current cloud security assessments don't verify their findings** - You tend to deal with hypothetical scenarios of if-then; for example, if you use these configurations, an attacker might do this to gain access. Using information from these assessments to advocate change can be challenging because it can be prone to push-back from various stakeholders.

Cloud Security Practice

GuidePoint's Cloud Security Practice offers expertise in agile infrastructure operations, security controls, compliance, high availability, identity management, and architecture. Our clients look to GuidePoint for guidance in specific security areas such as encryption, identity management, entitlements, compliant architecture, and secure networking (VPN, MPLS), etc.

Threat & Attack Simulation Practice

GuidePoint's Threat & Attack Simulation (TAS) practice focuses exclusively on attack-oriented and related professional services, such as Red/Purple Teaming, Penetration Testing, and Social Engineering. TAS engagements are flexible, and we can tailor them to ensure they fully satisfy our clients' objectives and requirements. Our mission is to provide high-quality, actionable results that include realistic recommendations to bolster our clients' security postures.

Put an ELITE Team of Cybersecurity Practitioners on Your Side
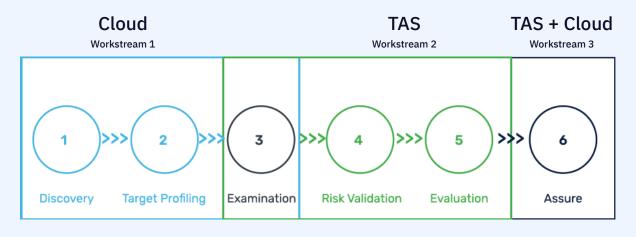
Our team will perform a Cloud Penetration Test that evaluates your current cloud-based environment from a security perspective, leveraging our best practices and cloud security standards.

Goals and Objectives

- Identify risks, vulnerabilities, and gaps
- Impact of exploitable vulnerabilities
- Determine how to leverage any access obtained via exploitation
- Deliver clear and actionable remediation information
- Provide best practices in maintaining visibility

Recommended Scope:

- Cloud perimeter
- "Internal" cloud environments
- On-prem cloud management, administrator, and/or development infrastructure

Workstream One - Evaluation: GuidePoint's Cloud Security team establishes a five-step process to understand your cloud security needs and provide appropriate remediation. GuidePoint designed this process to look into the technical risk and vulnerability exposure present in your environment while also allowing research and assessment of findings.

Workstream Two - Exploitation: Guidepoint's Threat & Attack Simulation team will combine information provided by the Workstream One – Evaluation process with any relevant penetration testing methodologies focusing on exploitable vulnerabilities. This focus will assess your cloud environment's resiliency to attack, the coverage of your security monitoring, and your detection capabilities' efficacy. GuidePoint builds from industry best practice methodologies to maximize your value when performing penetration testing activities.

Workstream Three - Remediation: GuidePoint Security performs a follow-up remediation validation assessment to ensure that the exploitation phase's remediation and mitigation steps have been accurately implemented. GuidePoint can attest that the client's overall security posture is aligned with industry best practices by performing this stage.

GUIDEPOINT SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132