NetSPI™

Cloud Penetration Testing

Secure Your Cloud. Secure Your Business.

82% of data breaches included cloud-based data – National University

Modern enterprises are accelerating their migration to cloud platforms, but with increased velocity comes amplified risk. Whether deployed on **AWS, Azure,** or **Google Cloud Platform**, cloud environments demand security strategies that extend far beyond baseline configurations. Misconfigurations, excessive permissions, exposed secrets, and inadequate segmentation create attack vectors that leave organizations vulnerable to devastating breaches.

The Challenge

Cloud infrastructure presents a dynamic and increasingly complex attack surface that organizations struggle to secure effectively.

Many organizations face challenges with overly permissive IAM roles, publicly accessible cloud services exposing sensitive data, and cleartext secrets embedded in configuration files. Weak segmentation, misconfigured security groups, and rapid cloud expansion create additional attack vectors that enable lateral movement and persistent access. Even security-mature organizations find it challenging to assess and harden their evolving cloud environments. Traditional vulnerability scanners identify surface-level misconfigurations but fail to uncover the sophisticated attack chains that real-world adversaries exploit.

The Solution

NetSPI delivers comprehensive **cloud penetration testing** aligned with industry-leading frameworks including **NIST 800-53, MITRE ATT&CK,** and **CIS benchmarks**. Using a combination of human-led and automated techniques, NetSPI transcends checkbox compliance. We identify exploitable weaknesses and demonstrate tangible business impact through real-world penetration testing. Our deep technical expertise spans **AWS, Azure,** and **Google Cloud Platform**, with over 300 in-house security experts, enabling us to identify platform-specific attack vectors and validate security controls through chained attack scenarios. We deliver the detailed context you and your team need through validated and prioritized findings, detailed attack narratives, step-by-step evidence verification for streamlined remediations, and more, all within The NetSPI Platform.

- **Multi-perspective testing** from both anonymous, external attacker and authenticated, internal user viewpoints
- **Real-world attacks and configuration review** including lateral movement and privilege escalation that demonstrate actual business impact and risk exposure
- **Platform-specific expertise** and insights across AWS, Azure, and Google Cloud environments

AWS Penetration Testing

NetSPI conducts comprehensive security assessments of AWS environments, targeting the most common yet critical vulnerabilities that expose organizations to significant risk. Our testing methodology combines automated scanning with expert-led manual exploitation techniques to uncover attack paths that lead to account compromise. We leverage real-world attack scenarios that demonstrate how misconfigurations can escalate into full infrastructure takeover.

- **S3 bucket misconfigurations** exposing sensitive credentials and proprietary data
- **IAM role privilege escalation** through excessive permissions
- **EC2 metadata exploitation** enabling lateral movement and administrative access

Azure Penetration Testing

Our Azure penetration testing focuses on the unique security challenges within Microsoft's cloud ecosystem, including identity management and tenant-level access controls. NetSPI's experts systematically evaluate Entra ID configurations, Azure resource permissions, and more to identify exploitable weaknesses. We demonstrate how seemingly minor misconfigurations can lead to tenant-wide compromise and persistent administrative access.

- **Account Blob Storage exposure** revealing database credentials and application secrets
- **Entra ID privilege escalation** through over-permissioned applications and service principals
- **Azure privilege escalation** through excessive RBAC permissions and managed identities

Google Cloud Platform Penetration Testing

NetSPI provides specialized Google Cloud Platform security assessments that address the platform's unique architecture and service-specific vulnerabilities. Our testing methodology evaluates Cloud Storage permissions, IAM role configurations, and serverless security to identify attack vectors specific to Google's cloud environment. We focus on the interconnected nature of Google Cloud Platform services and how misconfigurations can create unexpected attack paths.

- **Cloud Storage exposure** allowing unauthorized data access
- **Service account compromise** through insecure key management and excessive privileges
- **Serverless vulnerabilities** in Cloud Functions and Cloud Run deployments

You Deserve The NetSPI Advantage

- **300+ In-House Security Experts**
- **Intelligent Processes**
- **Advanced Technology**

Your Proactive Security Partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), and Breach and Attack Simulation (BAS) as a Service.

© 2025 NetSPI LLC | All Rights Reserved | 06.30.25