NEXT

Terms and Conditions

Vulnerability Scanning - Schedule PROF-2

Effective Date: March 25, 2026 | Supersedes prior versions.

Service Summary

Service Provider shall provide Vulnerability Scanning services ("Vulnerability Scanning") to identify known security vulnerabilities in systems and applications by running automated scans against designated assets. Vulnerability Scanning is designed to improve visibility into security weaknesses but does not guarantee detection of all vulnerabilities or prevent exploitation. Vulnerability Scanning is a point-in-time assessment and does not constitute continuous monitoring or a comprehensive security program.

Scope of Services

- Deployment and management of vulnerability scanning tools on Covered Systems or networks
- Scheduled scans (internal and/or external) in accordance with Service Provider's standard scanning policy
- Vulnerability scans are performed on a periodic basis as determined by Service Provider (typically monthly or quarterly) and are not continuous or real-time unless otherwise agreed in writing
- Reporting of identified vulnerabilities, including severity ratings and general remediation recommendations
- Integration of results into Service Provider's ticketing system or dashboard where applicable
- Advisory support for prioritizing remediation efforts

Exclusions

- Remediation of vulnerabilities identified through scans is not included in this service and will be separately scoped, quoted, and billed
- Guarantee of detection of all vulnerabilities, especially zero-day or previously unknown threats
- Continuous monitoring between scheduled scans
- Coverage of unsupported systems or environments that cannot run scanning agents or accept probes
- Scanning of assets not designated and approved by Client

Client Responsibilities

- Provide accurate scoping of assets and systems to be scanned
- Obtain any required permissions from hosting providers, cloud platforms, or third parties as required
- Review vulnerability scan reports and act upon recommended remediation steps
- Maintain system configurations that support scanning activities
- Retain ultimate responsibility for system security and remediation of vulnerabilities

General Terms

- Vulnerability Scanning is a visibility and risk-identification service. It provides information to aid remediation but does not itself reduce vulnerabilities unless action is taken by Client.
- Client acknowledges that Vulnerability Scanning is one element of a layered security strategy. While scanning improves visibility into risks, no single control or combination of controls can guarantee complete protection.
- Service Provider strongly recommends complementary safeguards such as endpoint protection (EDR/XDR), multi-factor authentication, conditional access controls, email filtering, and ongoing patch management to achieve a more comprehensive security posture.
- Vulnerability Scanning does not constitute or guarantee compliance with any regulatory or certification framework, including but not limited to CMMC, NIST 800-171, or similar standards.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included unless otherwise specified. Additional costs (e.g., custom scans, advanced reporting, or third-party integrations) may apply and will be billed separately.