Service Definition – Kaseya Vonahi vPenTest Automated Network Penetration Testing

This document describes how the service works and is intended for publication on the Digital Marketplace service page. It does not include pricing.

Document version: 1.0

Last updated: 30 January 2026

Supplier: Kent MSP Ltd

Service name: Kaseya Vonahi vPenTest (managed)

1. What the service is

- vPenTest is an automated internal and external network penetration testing platform that simulates real-world attack paths, exploits vulnerabilities, and provides rapid reporting to help organisations identify and remediate security risks.

1.1 Core capabilities

- Automated exploitation, privilege escalation, credential attacks, and lateral movement.
- Internal and external penetration testing on demand.
- Real-time activity logging for SIEM correlation.
- Compliance-ready assessments (CREST, PCI, HIPAA, SOC 2).

2. Service interface

- Accessed through a secure cloud-based portal with user accounts and RBAC.
- Supports scheduling, configuration, real-time monitoring, and report downloads.

3. Assessment management

- Internal/external test scheduling with custom scope and frequency.
- Activity logs and assessment status tracking.

4. Onboarding

- Tenant setup and user assignment.

- Deployment of internal agent VM.
- Assessment configuration and first-run validation.
- Documentation and guidance provided; on-site assistance optional.

5. Offboarding and end-of-contract

- Users download all final reports and logs before closure.
- Tenant access disabled and data removed upon request.

6. Service constraints

- Agent VM requires 8GB RAM, 80GB disk, bridged NIC.
- Testing may trigger security alerts due to real-world exploit behaviour.
- Platform updates delivered centrally as SaaS.

7. Service levels

- Platform delivered as multi-tenant SaaS with vendor availability SLAs.
- Support response targets follow managed service agreement.

8. After-sales support

- Incident handling, ticketing, and guidance.
- Assistance with assessment tuning and report interpretation.

9. Technical requirements

- Internal agent VM with required resources.
- Outbound connectivity for portal communication.

10. Outage and maintenance management

- Vendor publishes maintenance and release information.
- We notify customers of impactful maintenance.

11. Hosting options and locations

- Delivered from Vonahi cloud infrastructure; region based on provisioning.

12. Access to data

- Users export reports and logs via portal.
- Data no longer accessible after tenant deletion.

13. Security

- RBAC, MFA options, and tenant isolation.
- Encrypted communications and audit logging.
- Risk-based vulnerability and incident processes.

14. Accessibility

- Accessible document format; alternate formats available on request.