





Rising cyber-attacks and newly emerging security vulnerabilities bring unknown challenges to businesses of all shapes and sizes. Exposure to cyber risks can culminate into incidents such as cyber-attacks, malware infections, ransomware, web page compromises and data breaches. We have developed comprehensive Threat and Vulnerability Management (TVM) Services that ensure holistic view of security vulnerabilities across the organization's digital landscape.

Jio TVM services offer foundational layer security that help organizations identify vulnerabilities with security patching and hardening/ secure configuration of servers, containers, networking devices, virtualization layer, and Cloud infrastructure.


## What You Get




**Vulnerability Management**  
Get up-to-date view of security status and help prevent specific types of vulnerabilities




**Configuration Review**  
Securely review configuration and hardening of operating system parameters




**Container Security Assessment**  
Assess containers for vulnerability, secure configuration and malware




**Security Penetration Testing**  
Explore mock scenarios to identify hackable infrastructure loopholes



**Threat Advisory Services**  
Get notification of latest security vulnerabilities and their severity for various technologies



**Centralized Governance & Management**  
Manage your assets vulnerabilities and reporting centrally




**Digital Self-Care**  
An intuitive Digital Self-Care to manage your services


## Variants

| Features   | Starter Pack           | Advance Service     | Expert Service        |
|--|------------------------|---------------------|-----------------------|
| Vulnerability Scanning   |                        |                     |                       |
| Type of scans (Authenticated scan: Scan performed with credentials of the system)  | Un-Authenticated scans | Authenticated scans | Authenticated scans   |
| Detection of open N/W ports  | ✓                      | ✓                   | ✓                     |
| Discovering potential attack vectors in the system   | Partial                | Full                | Full                  |
| Security Patches required for the system   | Partial                | Full                | Full                  |
| Detailed review and verification of configuration settings   | ✗                      | ✓                   | ✓                     |
| Existence of assessment for weak authentication  | ✗                      | ✗                   | ✓                     |
| Minimum number of IPs/ active instances considered for scan  | 10                     | 25                  | 50                    |
| Scan frequency (No. of scans/ month)   | 1                      | 2                   | Continuous/ on demand |
| Infrastructure and Platform Coverage   |                        |                     |                       |
| Servers (Physical/ Virtual)  | ✓                      | ✓                   | ✓                     |
| Infrastructure systems and network devices   | ✓                      | ✓                   | ✓                     |
| Hypervisors  | ✗                      | ✓                   | ✓                     |
| Supported Cloud platform (AWS, Azure and GCP)  | ✗                      | ✓                   | ✓                     |
| Mainstream containers architecture supported   | ✗                      | ✗                   | ✓                     |
| Penetration Test   |                        |                     |                       |
| White Box penetration testing (Internal network test with prior information about the network and internal systems)                                | ✗                      | ✗                   | ✓                     |
| Black Box penetration testing (External network test, without prior knowledge of internal network and systems)                                     | ✗                      | ✓                   | ✓                     |
| Reports and Support  |                        |                     |                       |
| Reporting  | ✓                      | ✓                   | ✓                     |
| Systematic and accurate briefing of issues   | ✗                      | ✓                   | ✓                     |
| Risk view - local and remotely hackable issues   | ✗                      | ✗                   | ✓                     |
| Remediation guidance   | ✗                      | ✓                   | ✓                     |
| Post remediation rescan  | ✗                      | ✓                   | ✓                     |
| Vulnerability Program Management   |                        |                     |                       |
| Portal access  | ✗                      | ✗                   | ✓                     |
| Compliance management - PCI DSS, NIST and CIS  | ✗                      | ✓                   | ✓                     |
| Customised hardening guidelines for infrastructure components such as OS, NW, DB and MW  | ✗                      | ✗                   | ✓                     |
| End-to-end management of vulnerability during its lifecycle, from assessment to remediation support  | ✗                      | ✓                   | ✓                     |
| Automated tracking and mail notifications  | ✗                      | ✗                   | ✓                     |
| Management of reporting for security exceptions  | ✗                      | ✗                   | ✓                     |
| Zero Day Vulnerability (ZDV)- advisory and support (ZDV: An attack that has zero days between vulnerability being discovered and the first attack) | ✗                      | ✗                   | ✓                     |


## Jio Advantage




**Cost & Resource Optimization**  
Cost saving on security tool/ software licenses, optimization of resources




**Comprehensive Program**  
Complete vulnerability management program for your technology stack and infra components




**Expert led Assisted Care**  
Support all customers within defined SLA timelines



**Extensive Security Expertise**  
JioRakshaks™ - Vast pool of trained and certified security experts



**Flexible Assessments**  
Assessment reports to aligned to global industry standards and compliances



**Domain Expertise**  
Decades of experience in cyber defense and response