

# Vulnerability Management as a Service (VMaaS)

Whether it be new technology, systems, people or processes, your business is continually growing. Growth is positive. But as your organisation expands, so does its exposure to cybersecurity risks.

Many businesses struggle with Patch Management. Internal Vulnerability Management programs often lack structure, require significant financial resources, and fail to offer a clear and accurate view of security gaps and compliance status.

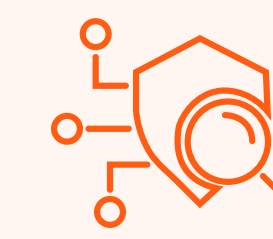
**Cyberintelsys** simplifies this challenge by handling the scanning and maintenance burden—delivering accurate, automated, and ongoing vulnerability assessments.

## Smart Scanning with Risk Prioritisation

**VMaaS 24/7** is delivered by our certified security analysts and leverages powerful technology, including Qualys, Tenable, and our in-house platform, **Cyberintelsys** Response, which provides advanced incident management and analytics capabilities.

**Cyberintelsys** Vulnerability Management as a Service (VMaaS) goes several steps ahead of standard Vulnerability Management programs, by ensuring that organisations accurately detect, classify, and contextualise vulnerabilities, with designed & prioritised remediation programs, for full-proof Vulnerability, Compliance, and Patch Management.

## What We Offer?



Continuous Vulnerability Scanning



Manual Penetration Testing



Automated Patch Management



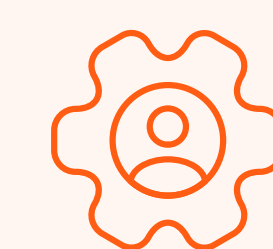
Asset Discovery



Threat Intelligence Correlation



Remediation Support & Validation



Role-Based Reporting



Audit-Ready Documentation

## Our Key Achievements



**10,000 +**  
Managed Endpoints



**20 +**  
Vulnerability Assessments  
Per Month



**3,000 +**  
Security Devices Managed



**100 +**  
Global Customers



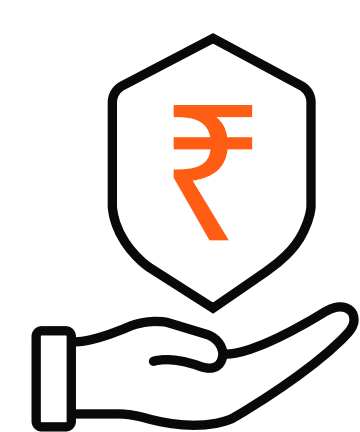
**50 +**  
Experienced & Certified  
Resources



**06 +**  
Year of Experience



## Who **Needs** This Service?



### Financial Services and Banking Institutions

Protecting financial services and banking institutions with advanced cybersecurity solutions.



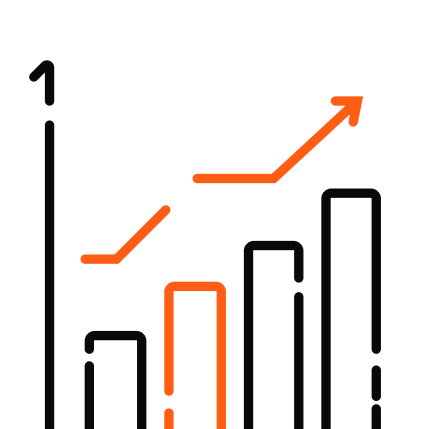
### Healthcare and Life Sciences

Securing healthcare and life sciences with tailored, compliance-driven cybersecurity protection.



### Retail and E-commerce Platforms

Protecting retail and e-commerce platforms with end-to-end security for transactions and customer data.



### Startups and Growing Enterprises

Empowering startups and growing enterprises with scalable, cost-effective cybersecurity solutions.



### Government and Public Sector Agencies

Safeguarding government and public sector agencies with robust, mission-critical cybersecurity.



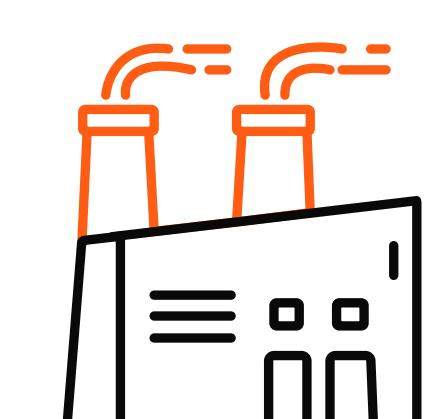
### Cloud, SaaS, and Software Development Firms

Securing cloud, SaaS, and software development firms with scalable, code-to-cloud cybersecurity solutions.



### Educational Institutions and EdTech Providers

Securing educational institutions and EdTech providers with reliable, student-first cybersecurity solutions.



### Industrial, Manufacturing, and Critical Infrastructure

Defending industrial, manufacturing, and critical infrastructure with resilient, real-time cybersecurity.

## Our **Approach**

We don't just defend — we empower your organization to operate fearlessly in the face of cyber threats.



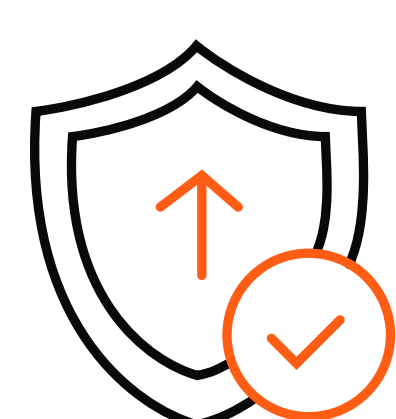
### Assess & Identify

Analyze systems, detect risks, and strengthen your security foundation.



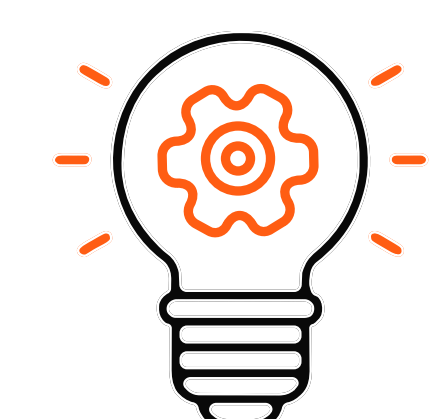
### Monitor & Respond

Enable 24/7 monitoring and instant response to stop threats before they escalate.



### Protect & Prevent

Deploy continuous scanning, risk-based assessments, and timely patching to block threats and prevent breaches.



### Evolve & Optimize

Continuously update systems and adapt with smart automation to stay ahead of threats.





## Why Choose **Cyberintelsys**?

- Continuous scanning and automated patching coverage
- Manual testing by experienced cybersecurity professionals
- Full patch lifecycle management
- Reduced false positives through expert validation
- Audit-ready documentation and compliance alignment
- Trusted by organizations in India, the Middle East, and globally

## Manual **Testing** Includes

- SQL Injection, XSS, and Input Validation Flaws
- Broken Authentication and Session Handling
- Insecure Access Control and Authorization Bypass
- File Handling Vulnerabilities (Upload/Download)
- Privilege Escalation and Lateral Movement
- Business Logic Exploitation, Multi-step Exploit Chaining

## Got questions? Our team is ready to respond



### India

First Floor, 686, 16th Main, 4th T Block East,  
Jayanagar, Bangalore – 560041, India



### Email

info@cyberintelsys.com



### Website

www.cyberintelsys.com



### Singapore

143, Cecil Street, #03-01, GB Building  
Singapore – 069542

## Take control of your security posture.

Cyberintelsys scans, tests, patches, and protects—keeping you ahead of cyber threats.