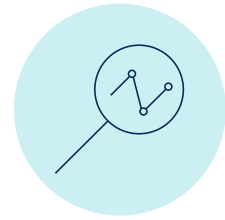


Managed Vulnerability Scanning (MVS) Service

Continuous Threat Visibility for Financial Markets

Cyber risks evolve daily, and financial institutions must detect and mitigate vulnerabilities before they become security incidents. Traditional, periodic assessments leave gaps - exposing trading platforms, infrastructure, and customer data potential breaches. Beeks managed vulnerability Scanning Service provides continuous monitoring and risk prioritisation, ensuring that vulnerabilities are identified before they can be exploited.



BENEFITS

Continuous Threat Discovery

- Regular scanning to identify risks before attackers do.

Real-World Threat Simulation

- Surfaces vulnerabilities that would be targeted by real-world attackers.

Risk-Based Prioritisation

- High/Critical vulnerabilities are triaged, ensuring the most urgent threats get addressed first.

Regulatory Compliance Support

- Helps meet security standards like ISO 27001, FCA, NIS2, DORA, GDPR, with audit-ready reporting.

KEY FEATURES

Automated Infrastructure Scanning

- Regular assessments of internal & external environments.

Light-Touch Continuous monitoring

- Scanning methods are non-intrusive, avoiding disruption to financial operations.

Cloud & On-Prem Support

- Offers both host-based scanning for flexible deployment.

Fast Detection Timeframes

- Identified vulnerabilities are made available within 4 business hours.

Comprehensive Vulnerability Testing

- Includes network surveying, port scanning, firewall testing, and exploit verification.

TECH SPECIFICATIONS

Host-Based Scanning Agents

- Lightweight agents installed directly on assets, enabling accurate scanning without complex network changes or stored privileged credentials.

Direct Internet or Proxy Communication

- Agents communicate securely with the Vulnerability Scanning Portal over the internet or via a proxy, reducing dependency on internal network configurations.

Reduced Network and Server Load

- Scans run locally on each device, lowering impact on network bandwidth and server performance during scanning periods.

Optional Traditional Scan Engine

- Supports hybrid environments by offering traditional scan engine deployment for assets that cannot use host-based scanning, such as network infrastructure.

STAGE 1

Define your assets

STAGE 2

Deploy Scanning Agents

STAGE 3

Continuous Monitoring

STAGE 4

Actionable Risk Reports

STAGE 5

Ongoing Support & Review