Vulnerability Management

Medium	MQTT Broker vulnerable
Critical	Operating System at the end of life
Low	New asset found

Navigating the digital world safely is crucial, and that's where our Vulnerability Management Solution comes in. Designed for ease of use and effective protection, our solution helps you discover and manage potential security weaknesses in your network. Whether through physical devices or virtual systems, we make sure you have the tools needed to identify risks before they become actual threats.
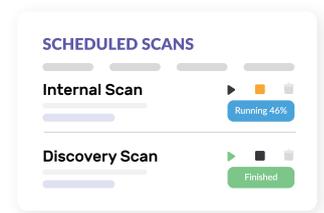
How does it work

1

INSTALLING

Install

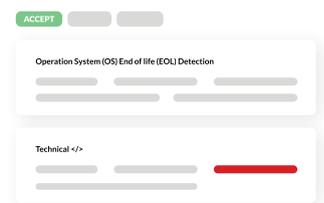Import the Virtual Appliance or plug in the Physical Scanner to your network.

2

SCHEDULED SCANS

Internal Scan — Running 46%

Discovery Scan — Finished

Scan

Set up and launch your scan. Choose single hosts, multiple hosts, or a range of IPs.

3

ACCEPT

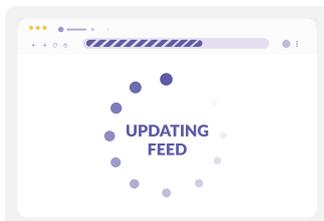Operation System (OS) End of life (EOL) Detection

Technical </>

Review

Receive an email summary. Manage details via the dashboard for prioritizing fixes.

4

UPDATING FEED

Update

Regular scans keep your defenses up-to-date with the latest threat data, and helps you stay compliant.

Configuration

Our Vulnerability Management Solution is designed to be flexible, adapting to your specific security needs.
Here's what you can configure:

- **Authenticated Scanning:** Gain deeper insights by scanning as an authenticated user to discover vulnerabilities that are visible only with proper credentials.

- **Discovery Scanning:** Identify and catalog all devices on your network, including previously unknown or unmanaged assets.

- **Website and External Host Scanning:** Extend your security perimeter by scanning external IPs and websites to assess vulnerabilities exposed to the wider internet.

- **Custom Schedules:** Automate scanning at regular intervals that suit your business hours and workload, ensuring continuous security monitoring.

- **Up-to-Date Security Feed:** Regularly updated to include the latest vulnerabilities, ensuring your defences are always ahead of potential threats.

- **Integration:** Seamlessly integrate with existing security tools and platforms for a unified approach to vulnerability management.

- **Workload Management:** Accept vulnerability risks if you can't patch them now, and automatically mark resolved vulnerabilities to lower your workload, helping you keep a clear oversight of your network.

These configuration options ensure that you have complete control over how and when your network is scanned, providing you with tailored security insights that align with your organizational needs.

Frequently Asked Questions

How does the solution help in compliance and audits?

The solution provides detailed reports and an audit trail for all scanned assets and discovered vulnerabilities, which is crucial for compliance. It helps in demonstrating due diligence and in making informed security decisions that align with regulatory requirements.

What is authenticated scanning and why is it important?

Authenticated scanning allows the scanner to perform checks as a logged-in user, providing deeper visibility into each host's security posture. This type of scanning can detect vulnerabilities that are only visible with user credentials, offering a more thorough assessment.

Do I have to deploy a scanner?

No, you do not have to deploy your own scanner if you want to scan external targets. Our external scanner platform allows you to use our scanners out of the box to scan any external IP or website, providing flexibility and ease of use.