



# Help STOP HACKERS with our Vulnerability Platform

- In 2024, there were over 40,000 new vulnerabilities per day (3,300 pm).
- Most vulnerabilities can be fixed (remediated), once identified.
- You can't secure what you can't see - which is why this service is critical.

Vulnerabilities are essentially a 'hole' in software code that a hacker can leverage to breach and move within your organisations' infrastructure - Almost every device can have vulnerabilities

**Vulnerability Management-as-a-Service** is a low cost, high value monthly subscription

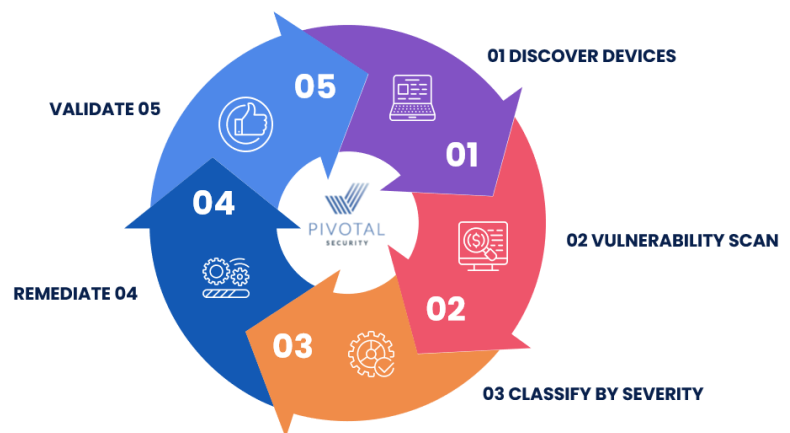
We discover vulnerabilities across your entire organisation, rank them by level of criticality and optionally remediate them, or provide the report to your existing IT team or MSP for them to remediate

## Key Features

- Internal, external vulnerability scans are available.
- Continuous vulnerability scans identify newly added devices on the network and new vulnerabilities.
- Build remediation plans to reduce effort required to fix vulnerabilities.
- Manually or schedule automatic remediation of vulnerabilities.
- Delivered a self-service (software only) or managed service model.
- Delivered as a cloud service.
- Extensive reporting.
- Deploys in minutes with near instant Time to Value

## VULNERABILITY LIFECYCLE

CONTINUOUS VULNERABILITY SCANNING



**How many critical and exploitable vulnerabilities do you have in your network right now, today?**

Our team of cyber experts deploy and manage our cloud-based **Breach Minimisation Platform** of which vulnerability Management-as-a-service is a component.

We focus on security, so your IT team are freed up to keep your business up and running. Our objective is to help stop hackers and breaches to protect your business and your private and regulated data.

### Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

**Critical**

289 were unique critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems

289

**High**

5651 were unique high severity vulnerabilities. High severity vulnerabilities are easy to exploit and may provide access to affected

5651

**Medium**

1798 were unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a

1798

**Risk Detected: High Risk Score**

## AT A GLANCE VULNERABILITY STATUS

Remediate In	EPSS Score
3 days	0.95
15 days	0.90-0.95
30 days	0.85-0.90
	0.80-0.85

**PRIORITISE REMEDIATION BY CURRENTLY BEING EXPLOITED**

## Remediation Plan – new vulnerabilities appear every day

New Company

View Assets View Evidence Integration Action Snooze

Overview Assets Depreciated Assets Firewalls Vulnerabilities Compliance Active Directory Azure Active Directory Microsoft Secure Score Alerts

External Scan Standard Reports Application Baseline Notification Rules Settings

Remediation Plan (47)

Status Remediated Search

Action	Application / OS	Recommended Version	Vulnerabilities	Asset(s)
Remediated	Putty	Version 0.74	184 371 555 vulnerabilities	2
Remediated	Google Chrome		555 vulnerabilities	2
Remediated	Microsoft Office Professional 2016	Version 5002005	555 vulnerabilities	2
Remediated	Microsoft Exchange Server 2016	Version 5004779	555 vulnerabilities	1
Remediated	Microsoft Silverlight		555 vulnerabilities	1
Remediated	Mozilla Firefox 84.0.1 (x86 en-US)	Version 92.0	555 vulnerabilities	1

## BUILD AND REMEDIATE VULNERABILITIES WITHOUT EFFORT

## Compliance Reports

Report Name
CIS Compliance
CIS_8.0 Compliance
Consolidated Compliance
Essential_Eight Compliance
GDPR IV Compliance
GPG 13 Compliance
HIPAA Compliance
ISO 27002 Compliance
NIST 800.171 Compliance
NIST 800.53 Compliance
PCI DSS Compliance

**50+ REPORTS**

### Table of Content

- Vulnerability Assessment
- Endpoint Assessment
- Compliance Report Card
- Compliance Assessment
- Patch Assessment
- IT Infrastructure Assessment

### Security Assessment

Assessment report for Customer Name provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. The findings generated during the security control assessment provide important information that facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities.

### Risk Dashboard

The Consolidated Risk Report aggregates risk analysis from various sources to provide a comprehensive view of the organization's risk profile.

## POWERFUL REPORTS AND SECURITY ASSESSMENTS

## Application Vulnerability Trending



**TRACK VULNERABILITIES OVER TIME**

## Application Baseline

New Company

View Assets View Evidence Integration Action Snooze

Overview Assets Active Directory Alerts Jobs Probes / Agents Remediation Plan Network Scan Findings External Scan Standard Reports Application Baseline Notification Rules Settings

Remediation Plan (10)

ACTION

Remove	Google Chrome	Denied Application
Install	Oracle Windows VirtIO Drivers	Mandatory Application
Remove	WinSCP 5.17.10	

**CREATE AN APPLICATION BASELINE**