

# VULNERABILITY MANAGEMENT

Bytes' fully managed Vulnerability Management Service helps businesses protect the integrity of their applications and data by proactively identifying potential attack vectors in their environment thus providing visibility into potential exposure areas within a distributed network.

The service may be delivered as either an external or internal solution. When both scanning types are combined, clients are able to differentiate between which vulnerabilities are from the outside, the inside or from both locations.

## Internal Scanning

Internal scanning allows the client to assess the state of vulnerabilities within their enterprise. A large percentage of network-based attacks originate unknowingly from inside a protected or private network.

Internal scans are launched from a scanner located at the customer's premises and requires the customer to provide the appropriate hardware and operating system. Credentialed scanning for internal assets provides a comprehensive view of vulnerabilities and patching status. Credentials can be provided for Windows, Database, SNMP and SSH configured assets.

## The Solution

External scanning presents the hacker's eye view of the network perimeter and highlights open risk exposures. External scans identify and assess only devices with routable IP addresses. Scans are scheduled by the CSOC and launched from the SecurityHQ Secure Data Centre environment. External scans do not require setup or hardware/software investment. External scanning is delivered based on the number of IPs and the frequency of scanning.

## Stay Ahead of Attackers



### Accurate Scanning

Non-invasive, intelligence-gathering scanning system emulates techniques used by attackers, as they build upon knowledge from prior exploits.



### Information Monitoring

Generate reports, submit and view vulnerability exceptions, perform on-demand scans and quickly gain insight into risks across your environment.



### Risk Prioritisation

With automated asset classification and risk prioritisation, assess and manage risks more effectively.



### Expert Support

Let our team of Security Experts respond to, and remediate, identifiable vulnerabilities.

## Benefits

- **Complete visibility** of known and unknown assets residing on your network.
- **Remediate** discovered vulnerabilities in your environment.
- **Prioritise and Assess** discovered assets.
- **Receive Detailed Reporting**, including recommendations for remediating discovered vulnerabilities.
- **Verify and Re-scan** to confirm remediated vulnerabilities that have been correctly patched.
- **Receive Round the Clock Support** from experienced and dedicated Security Engineers.

## Service Features



### Customisable Reporting

Receive reports that focus on the status of vulnerabilities within your enterprise, including protection measures employed, security activities, subordinate activities and service summaries.



### Single Pane of Glass Dashboard

Receive an overview Dashboard, via a CSOC portal, to provide administrators with a comprehensive overview of the vulnerabilities within your network, broken down by severity and current scan results.



### Flexible Policies

To provide flexibility for each scheduled scan, multiple policies are available for both internal and external scanning. These policies allow customers to assess vulnerabilities and exposures that exist across a variety of device types, with varying degrees of intrusiveness.



### Accredited & Assured

We use ISO 9000 / 20000 / 27001 certified processes. Our analysts have CISSP, CCNS, CompTIA; ITIL V3; CoBIT 5.0 certifications & multiple vendor accreditations - Qualys, Check Point, Cisco, Microsoft, VMWare, BlueCoat and more.



### Prioritisation & Assignment

One of the challenges of vulnerability management is properly prioritising which vulnerabilities should be remediated first. As well as tracking and recording the prioritisation. Vulnerability Management service displays the severity of identified vulnerabilities, their impact and relationship to business criticality.



### Instant Scan Result Accessibility

Results of each separate scan can be viewed independently through the "Scan Results" option of the portal. This distributed manner of archiving and storing scan data allows authorised personal to quickly review the results of a single scan, while also reviewing the overall state of assets and their respective vulnerabilities across the enterprise.



**Have a question? We would love to hear from you.**

#### Reach us

tellmemore@bytes.co.uk | 01372 418 500  
[bytes.co.uk/security](https://bytes.co.uk/security)

#### Follow us

f in t

©2020 Bytes | All rights reserved