daisy.

VULNERABILITY MANAGEMENT IT DIRECTOR'S CHEAT SHEET

Faced with a snowballing variety of cyber vulnerabilities, today's IT departments often struggle to identify which are the most critical in the current threat landscape and act promptly to counter them. As the damage potential of these vulnerabilities constantly fluctuates, serious weaknesses can be overlooked while relatively trivial ones receive urgent attention.

To protect your business, high-quality **vulnerability remediation** has to be a priority – and with attackers growing ever more sophisticated, manual methods are no longer enough. Instead, cloud-based **Vulnerability Management (VM) technology** allows you to test and monitor your network environment simply and accurately, along with all connected devices.

This cheat sheet is intended to help IT Directors understand what to look for when selecting a vulnerability management solution. You can tick off the checklist to ensure you choose the right provider to get (and stay) on top of your vulnerabilities.

SELECTING A VULNERABILITY MANAGEMENT SOLUTION
YOUR CRITICAL CHECKLIST

What are the top features to look for?

Your Vulnerability Management (VM) solution is only as good as the data it receives.
Look for one that can:

□ Monitor your perimeter, cloud and internal systems

□ Discover devices that are lost or hiding in your network

□ Organise devices automatically using customisable rules

□ Scale seamlessly from a few devices to millions

□ Scan internal and external networks efficiently

□ Identify vulnerabilities based on Common Vulnerabilities and Exposures (CVE) guidelines

□ Track and record the fixing of vulnerabilities

□ Deliver Six Sigma accuracy as a minimum

□ Protect scan data against eavesdropping and tampering

□ Is it a software product or a cloud service?

Cloud-based VM solutions deliver increased benefits as they don't require new hardware, or ongoing updates and backups. Securely accessible through your browser, they can reach perimeter systems immediately, scale easily to handle new devices, users and locations, and store results in an objective, tamper-resistant way for audits.

□ Does it enable full monitoring, or is it just a scanner?

An up-to-date solution will track the state of your systems to provide an evolving picture of your security. They can also make predictions about emerging "Zero Day" vulnerabilities or "Patch Tuesday" issues without requiring new scans.

□ Does it scan all systems - perimeter, internal and cloud?

Look for solutions that can check all systems with a single tool, giving you a consolidated view of your security across the Internet, your private networks, and in the cloud.

□ How well does the VM solution handle multiple locations?

Modern, cloud-delivered VM solutions check multiple systems simultaneously. This is done using secure, remotely managed scanners (physical boxes or virtual machines) in different parts of your network, to make internal scanning efficient and minimise the impact on your infrastructure.

□ Will it require open holes in your firewall?

You should never have to compromise your security by opening special ports in your corporate firewall.

□ Does it integrate with other systems?

Consider solutions with robust APIs that enable easy integration with your existing security information and event management (SIEM), risk management (ERM), or governance (GRC) solutions.

□ Can it reach all of your systems?

With modern networks in a constant state of flux, your VM solution should be able to scan all systems as they move in and out of your network. Make sure it can handle cloud, perimeter and internal devices together in a consistent way.

□ Can the VM solution discover what's actually in your network?

Look for solutions that search through your perimeter and internal networks, as well as cloud environments like Microsoft Azure and Amazon Web Services, to discover and catalogue the devices running there.

□ Can it organise devices dynamically?

Best-in-class solutions use modern techniques like "tagging", which programmatically apply labels to each device you encounter (as opposed to older labour-intensive groups).

□ **Can it scan large numbers of devices efficiently?**
Modern VM solutions scan different parts of your network in parallel, automatically consolidating results into a single report. This accelerates scanning without overloading your network.

□ **Can scans be run automatically, or even continuously?**
Scans should be able to run according to your chosen schedule (for instance, to coincide with maintenance windows) or repeat continuously.

□ **Which vulnerabilities will the VM solution look for?**
The best solutions combine vulnerability data from industry-standard sources like computer emergency response team (CERT), software vendors such as Microsoft, as well as information from customers worldwide. Look for solutions that rigorously test each vulnerability definition for accuracy.

□ **How often are new vulnerability signatures added?**
New vulnerabilities are discovered every day. A quality VM solution should be able to respond as soon as these are published by your provider.

□ **Can this solution use authentication for deeper scanning?**
Only use VM solutions that allow you to specify credentials for securely logging into devices, databases or applications.

□ **Can it scan virtual images in public cloud environments?**
Public cloud environments operate strict rules for the scanning of virtual machines. Look for VM solutions that are pre-approved for scanning in Microsoft Azure, Amazon Web Services and Google Cloud Platform and often native integrations.

□ **Does it offer Six Sigma scanning accuracy?**
Accuracy is vital in a VM solution. A missed vulnerability can leave your network open to attack, while "false positives" will waste your time. Look for solutions that use industry-standard processes like Six Sigma and test them for accuracy in your own environment.

□ **Does the solution protect data for audits?**
Make sure your chosen VM solution stores vulnerability data away from users (e.g. in the cloud) to prevent tampering.

□ **Can it tailor reports for different audiences?**
Look for solutions that provide different levels of information, from executive scorecards to detailed, drill-down reports that meet your own needs and criteria.

□ **Does it offer predictive analysis?**
Advanced VM solutions track your devices to identify those that might be vulnerable to new "Zero-Day" attacks or "Patch Tuesday" issues. This should happen without the need for new scans.

□ **Can the solution highlight changes in vulnerability "status"?**
For efficient scanning, choose a VM solution that identifies whether any vulnerability it finds is new, being worked on, already fixed, or accepted as not worth fixing. The best solutions also provide differential reporting that highlights changes from one scan to the next.

□ **Are vulnerabilities prioritised in reports?**
Vulnerabilities should be ranked by severity, based on industry standards such as the Common Vulnerability Scoring System (CVSS). This can help you prioritise how and when to address each issue, and is particularly important if you need to give proof that severe vulnerabilities are being promptly identified and fixed.

□ **Does the solution offer patch-centric reporting?**
While all VM products will list individual risks, more advanced solutions will also organise those risks according to the patches that address them. This makes it quicker and easier for IT teams to eliminate vulnerabilities.

□ **Can reports be used to help demonstrate compliance?**
Look for VM solutions that provide native support for key mandates like Payment Card Industry (PCI), while allowing you to customise reports to your individual needs.

□ **What information does the solution provide about each vulnerability's underlying causes?**
A best-in-class VM solution will offer a detailed description of each vulnerability, as well as links to the vendor updates or patches needed to fix it.

□ **Does the solution have automated trouble-ticketing?**
A top VM system offers automated notification of tickets as well as comprehensive reporting on ticket status. Look for solutions that generate executive summaries across device groups, as well as detailed drilldowns for individual devices, vulnerabilities and users.

□ **Can you control how remediation tasks are scheduled?**
VM systems with remediation tracking can usually be configured to prioritise the most severe vulnerabilities. But it's also important to be able to control the relative priorities of issues across different systems. This allows your IT team to focus on fixing those with the biggest potential impact on your business.

□ **Does the solution work with external ticketing systems?**
If you already have a trouble-ticketing system in place, look for a VM solution that can work with it to generate, track and close tickets automatically.

□ **Is Vulnerability Management a core focus for the provider, or just one feature of another product?**
Vulnerability scanning is a sophisticated technology that requires deep expertise and commitment. Look for providers who view their VM solution as a core part of their business, not a bullet point on another product's checklist.

WHAT'S NEXT?

To develop a vulnerability management programme that truly fits your needs, you first need to determine what's most critical for your business. This takes time, resources and experience.

Daisy's **Vulnerability Scanning Management** service can help by harnessing the deep expertise of our Daisy Security Operations Centre (SOC) team. Our skilled experts will proactively highlight the vulnerabilities in your IT environment and create a prioritised schedule of actions to help you create and maintain an enhanced, fully compliant security posture.

We have partnered with industry leader **Qualys** to deliver an advanced and scalable vulnerability management solution that continuously scans your network to detect issues in real-time. This is enhanced by our specially designed **management and governance service**, which helps you mitigate vulnerabilities and optimise efficiency by providing deep insight into where your time and effort are being spent.

WHY DAISY?

Daisy has a 25-year track record of supplying managed security services:

- End-to-end expertise – from data centre to devices across cloud, connectivity and communications
- The best technology – highest levels of accreditation with the world's leading vendors
- UK-based Security Operations Centre with industry-leading accreditations such as Cyber Essentials Plus, ISO 27001 (Information Security Management), ISO 20000 (IT Services Management), Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM)

bsi. ISO/IEC 20000-1 Information Technology Service Management
ITMS 593451

bsi. ISO/IEC 27001 Information Security Management
IS 599749

Qualys.

To discuss your vulnerability management needs contact our experts:

enquiry@daisyuk.tech

0344 863 3000