HARMONY PURPLE

# Vulnerability Management Solution Guide

The marketplace for vulnerability and risk management solutions keeps getting more complex. Customers have many point solutions to choose from, and the point solutions often integrate to improve manageability. The result is almost limitless choice in terms of solution combinations.

This solution guide provides a summary of the main types of vulnerability and risk management solutions. It explains what they do, how they work, and their strengths and limitations. It also provides an in-depth view of Harmony Purple, the vulnerability and risk management solution from Orchestra Group. This guide will be useful to security and IT personnel responsible for managing vulnerabilities and risk who operate in an environment of increasing threats combined with constraints on time, personnel and budget.

## VULNERABILITY ASSESSMENT – A BRIEF SUMMARY

Vulnerability assessment is the process of identifying exposures in the IT environment that could lead to loss of availability, theft/release of confidential information, or data tampering (integrity). These exposures are usually a result of outdated or unpatched software, and lack of proper security controls such as weak password policies, unencrypted data, etc.

## THE THREE TYPES OF SOLUTIONS

There are three primary types of solutions in this space:

1. Vulnerability Management (VM)
2. Breach and Attack Simulation (BAS)
3. Vulnerability Prioritization Tools (VPT)

The following summarizes each type and references some leading providers.

## VULNERABILITY MANAGEMENT

Virtually all organizations (businesses, government, non-profit) conduct some form of vulnerability management. In many cases they are mandated to do so for regulatory compliance. As IT estates grow larger, the tasks of keeping track of assets, vulnerabilities, software patch levels and compliance reporting are too burdensome to handle manually. Vulnerability Management (VM) tools address this need.

© Orchestra Group 2021 | All Rights Reserved

Vulnerability management (VM) tools automate several tasks. VM relieves IT personnel from the need to research new vulnerabilities, track which systems are exposed and generate compliance reports for auditors. There are three basic components of a VM system. First is the external threat feeds (e.g. CVEs, Mitre Att&ck) that keep an up-to-date data base of known vulnerabilities and attack methods. Second component is the scanning function in which the VM reaches out to all systems in the IT estate and determines which known vulnerabilities in its database are applicable to which systems. The third component is the reporting function. It presents the information with some level of prioritization – typically based on the severity level assigned to the vulnerabilities.

Vulnerability management is a must have for all organizations and VM solutions have been around for many years. The large vendors in this space (Rapid7, Tenable, Qualys) have invested years of development into their products. Primarily they have focused their investments in offering very broad coverage in terms of the types of systems they can scan and report on, the breadth of the threat feeds they can ingest, scalability, management and reporting, and integrations with workflow/ticketing systems. Their products have grown in size and functionality to address the needs of the largest, most complex enterprise clients. However, they have not fundamentally changed what they do. Essentially, they address the reporting needs of large organizations (where are the vulnerabilities, how many are there, what are the trends, etc.). However, they have minimal capabilities with respect to assessing which vulnerabilities present the most significant threats to the organization. Priority is typically based on the common vulnerability scoring system (CVSS) classification of the vulnerability (critical, high, medium, low). There are issues with this approach which have resulted in organizations, even those with comprehensive vulnerability scanning and remediation regimes, falling victim to successful data breaches.

## THE VULNERABILITY MANAGEMENT PROBLEM

The problem most organizations face is there are more vulnerabilities than they can address in a timely fashion. As a result, they prioritize which vulnerabilities to address based on the CVSS assigned severity. However, assigned severities do not factor in the context of an organization's IT environment. That context can result in a high severity vulnerability posing minimal risk, while a low severity one may pose a high risk. The result is CVSS based patching strategies fail to reliably target the right vulnerabilities. Organizations keep getting breached. A recent survey found that 60% of breaches would have been prevented if the right systems had been patched.

VM vendors have tried to improve their prioritization capabilities. An approach many have adopted is to augment vulnerability severity classifications with threat intelligence feeds. These feeds provide some added context by identifying which vulnerabilities are being actively used by attackers, and by gathering external evidence that a given organization is under elevated threat of attack. This may enable some marginal improvement in risk mitigation, but the macro trends are undeniable – organizations are not effectively protecting themselves from data breaches.

## BREACH AND ATTACK SIMULATION (BAS)

One of the limitations of VM solutions is they lack insight into how attackers could exploit weaknesses in the security defenses of an organizations. On a periodic basis some organizations conduct penetration testing exercises, often using the services of external penetration testing experts. Manual pen tests have their place, such as to pass a required audit. However, they are expensive, time consuming and because they are basically onetime events, they do not address the day-to-day secops problems that VM solutions have not solved.

BAS tools provide a way to automate pen testing. They enable IT teams to test more frequently and without the need for external consultants. The results they provide help IT teams identify weaknesses in their security defenses and determine required remediations. While BAS tools don't directly augment VM solutions or improve vulnerability prioritization, they provide a valuable "attackers eye view" that help teams establish and maintain more effective security defenses. Some of the tools and techniques used by BAS solutions work by testing

© Orchestra Group 2021 | All Rights Reserved

known exploits within the live network. This can be disruptive to normal operations. As a result, BAS tools need to be scheduled during off hours or during specially scheduled times. Some BAS functionality might need to be disabled, or confined to testing in labs that are set up to mimic production environments.

## VULNERABILITY PRIORITIZATION TOOLS (VPT)

As the previous sections have made clear, a fundamental shortcoming with VM solutions and their add-on features/integrations is the inability to accurately identify which vulnerabilities pose the greatest risk to the organization. A core element missing from these solutions is the limited context with which vulnerabilities are assessed. An open vulnerability may pose a large risk at one organization while only minor risk at another. VPT tools seek to bring that needed context to existing VM and associated solutions.

VPT take several approaches to this problem. Some aggregate threat information from across the IT estate – output from VM scans, application testing, and threat intelligence, and apply machine learning/AI techniques to the data. In addition, they may use network discovery techniques to apply attack path scenario analysis to determine which vulnerabilities are exploitable in the IT estate and determine the potential impact of a successful exploit.

The VPT approach does address an important gap in the overall Vulnerability Assessment landscape. However, VPT solutions were designed as add-ons to existing VM solutions. Therefore security and IT teams need the budget for yet another security tool, plus the time and resources to go through an often complex integration phase.

## WHERE DOES THIS LEAVE THE CUSTOMER?

The result of how VM products evolved and the emergence of additional solutions that address their limitations is a proliferation of products, especially within large organizations. A typical enterprise may have dozens of security solutions, including solutions whose only purpose is to makes all the other ones more manageable. Small and mid-sized organizations that lack budgets and staff to adopt all the latest best of breed security tools need to stick to the basics of what they need for compliance and reasonable security hygiene. Organizations large and small still share problems in common – they lack a practical means of minimizing the risk and impact of data breaches.

## HARMONY PURPLE – A NEW APPROACH TO VM, BAS AND VPT

Harmony Purple is an all-in-one solution that combines the functions of vulnerability management, breach and attack simulation, and vulnerability prioritization in a single, tightly integrated platform. It addresses the needs of organizations that do not have budget and staffing to deploy, deploy, integrate and manage separate VM, BAS and VPT products. Harmony Purple was designed for ease of use and low operational impact while more effectively reducing risk than traditional VM solutions. The purpose of Harmony Purple is to enable resource constrained teams to effectively manage vulnerabilities and security exposures. The basics of how Harmony Purple works is as follows:

Harmony Purple includes an agentless, lightweight asset discovery and scanning function called “lean scanning”. Lean scanning has minimal impact on running systems which means IT teams have the flexibility to run vulnerability scans on production systems, without the need to schedule downtime for scanning. Harmony Purple takes a four phase approach combining VM, BAS and VPT functions, as described in the section below.

© Orchestra Group 2021 | All Rights Reserved

## HOW HARMONY PURPLE WORKS

Harmony Purple's four phase approach works as follows:

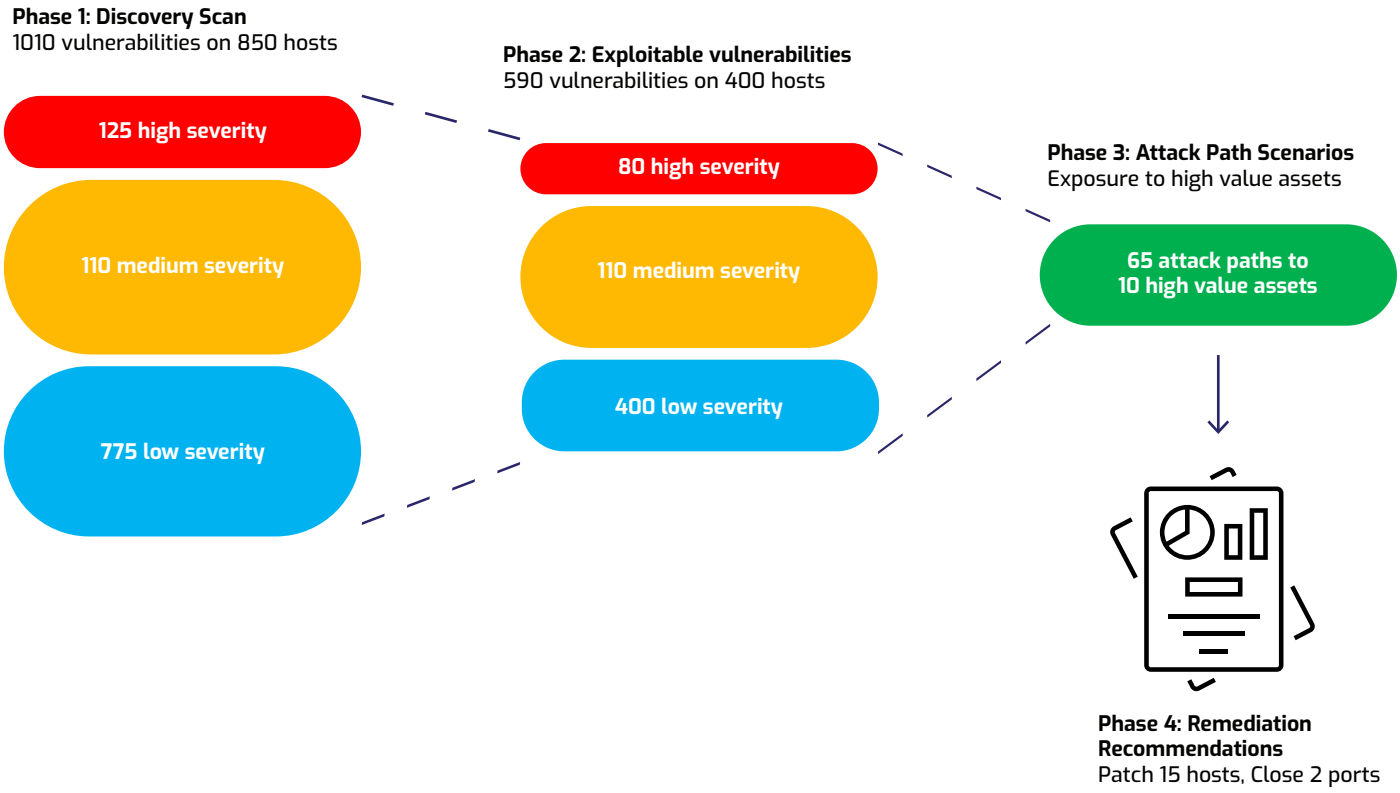
**Phase 1:** Harmony Purple performs a traditional VM scan. It identifies which systems are exposed to which vulnerabilities and the severity assigned to those vulnerabilities.

**Phase 2:** Harmony Purple applies its knowledge of the configuration of the scanned systems to determine whether vulnerabilities are exploitable on those systems. For example, if a vulnerability requires specific open ports or running services and those are not present, then the vulnerability (and required patch) is given a lower priority.

**Phase 3:** Attack Path Scenarios (APS) identify how an attacker could use an open, exploitable vulnerability to move laterally in the network and what assets would be at risk or breach. This capability works similarly to breach and attack simulation (BAS) in that it discovers the weaknesses in defenses and their potential consequences.

**Phase 4:** This final phase provides reporting and remediation recommendations. It identifies which systems and vulnerabilities should be patched to maximize risk reduction. It also recommends compensating controls that can be applied in lieu of patching or which should be applied to safeguard high value assets. This information is detailed in a set of clear reports that meet the needs of different stakeholders in the organization – from operations personnel who need to implement the recommended actions, to security managers who need to communicate status/plans/rationales to audit committees, as well as executive summary reports that meet the needs of higher-level decision makers.

**The diagram below illustrates Harmony Purple's four phase process:**



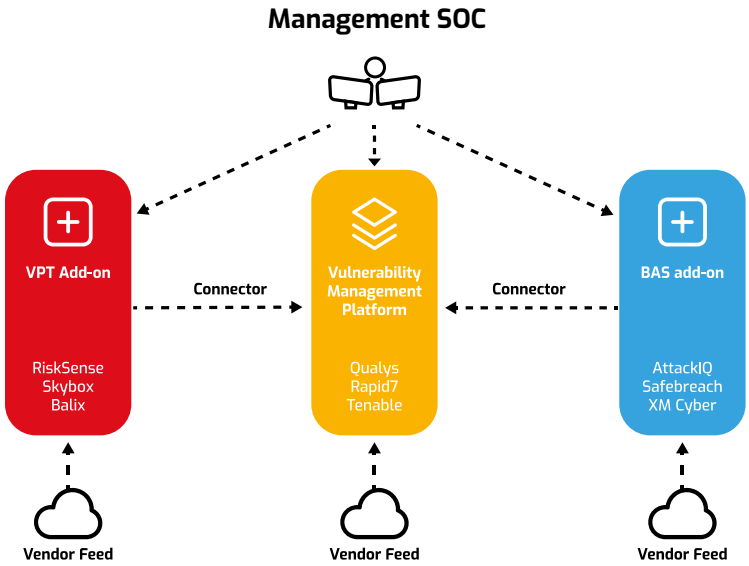

© Orchestra Group 2021 | All Rights Reserved

## WHAT MAKES HARMONY PURPLE DIFFERENT

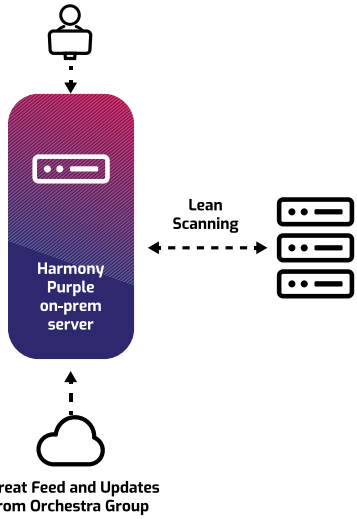
Harmony Purple addresses an important need that traditional VM, BAS and VPT solutions fail to address. Small and mid-sized enterprises including commercial, governmental and non-profit organizations lack the resources to deploy and operate a complete suite of security solutions. At the same time, these organizations are increasingly targeted by attackers. These attacks are sophisticated and automated. While in the past large organizations were primary targets of data theft attacks, SMBs are now also targets of ransomware attacks.

The leading VM solutions have evolved to address the needs of the largest enterprises – in terms of the scope of their scanning, analysis and their 3rd party integrations. Niche vendors in the VPT and BAS space have developed their products with a view of augmenting the big VM solutions. Thus, the needs of small to mid-sized organizations have largely been ignored.

### MULTI-VENDOR DEPLOYMENT OF VM, BAS AND VPT




### HARMONY PURPLE DEPLOYMENT




## SUMMARY

Harmony Purple is a fully integrated all-in-one solution. It is easy to deploy and use, and does not require feeds from an external VM system. Most customers are able to deploy and begin using Harmony Purple in two days. Organizations with small security staffs (or even organizations with no full-time security specialists) can easily use Harmony Purple to improve their security posture, meet compliance and reporting requirements, and intelligently apply the software updates and remediations to effectively reduce their risk of being breached or falling victim to ransomware.

© Orchestra Group 2021 | All Rights Reserved