


Vulnerability and Threat Management Solutions Buyer's Guide

Learn how to choose the right Vulnerability and Threat Management (VTM) solution. This guide helps you assess your needs, ask the right questions, and select the most appropriate vendor for your organization.

Introduction

The organizational attack surface is expanding exponentially. Digital transformation, cloud migration, remote working, rushed development schedules, inadequate validation, and greater software complexity - all create opportunities for cyber attackers to exploit.

In a world of heightened risk, organizations must find ways to manage their cyber exposure more effectively.

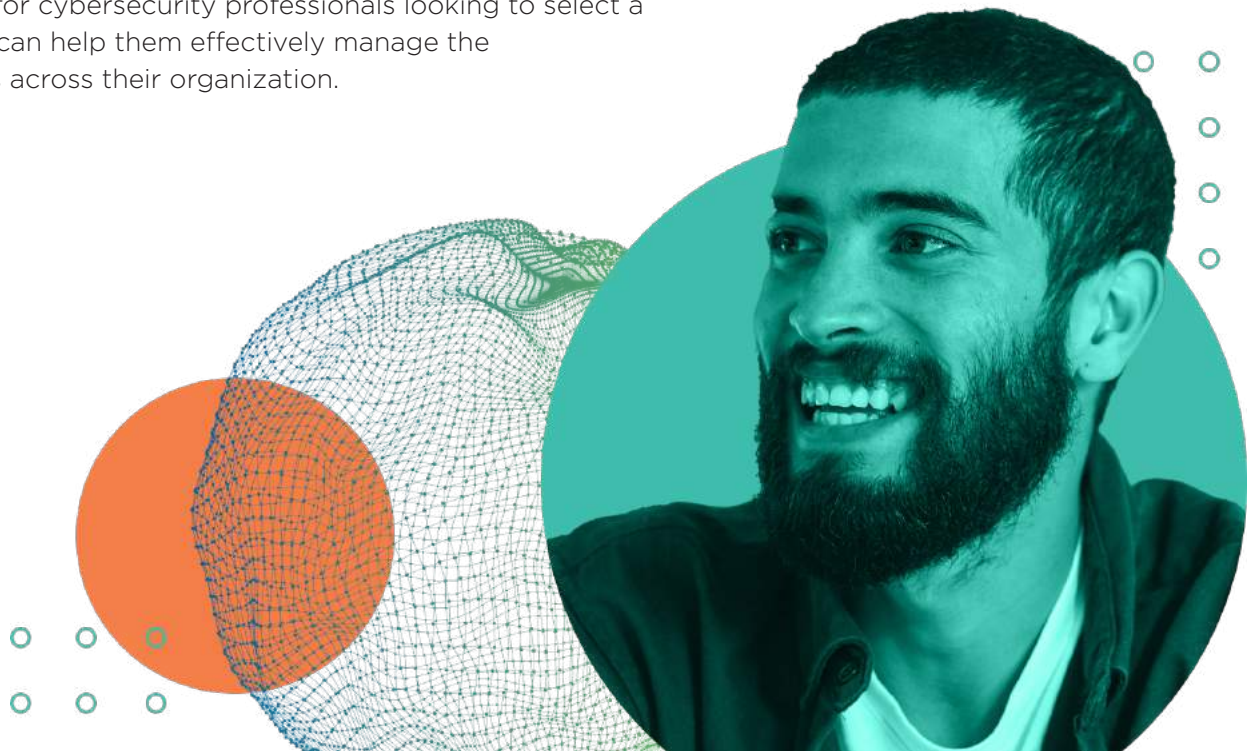


The 2023 Skybox Vulnerability and Threat Trends report noted that at the start of the year, the total number of vulnerabilities cataloged in the National Vulnerability Database (NVD) was nearing 200,000. New vulnerabilities are soaring - NVD added over 25,000 in 2022 - a 25% jump over the previous year. Vulnerabilities aren't just on the rise: **they're rising faster than ever before.**

Against the backdrop of the exponential rise in the number of vulnerabilities, one thing is clear. We no longer live in a "fix everything" era. There are simply too many vulnerabilities to fix and the traditional response - typically a combination of ad hoc vulnerability scans, spreadsheets, and periodic patch cycles - just can't keep up with the challenge.

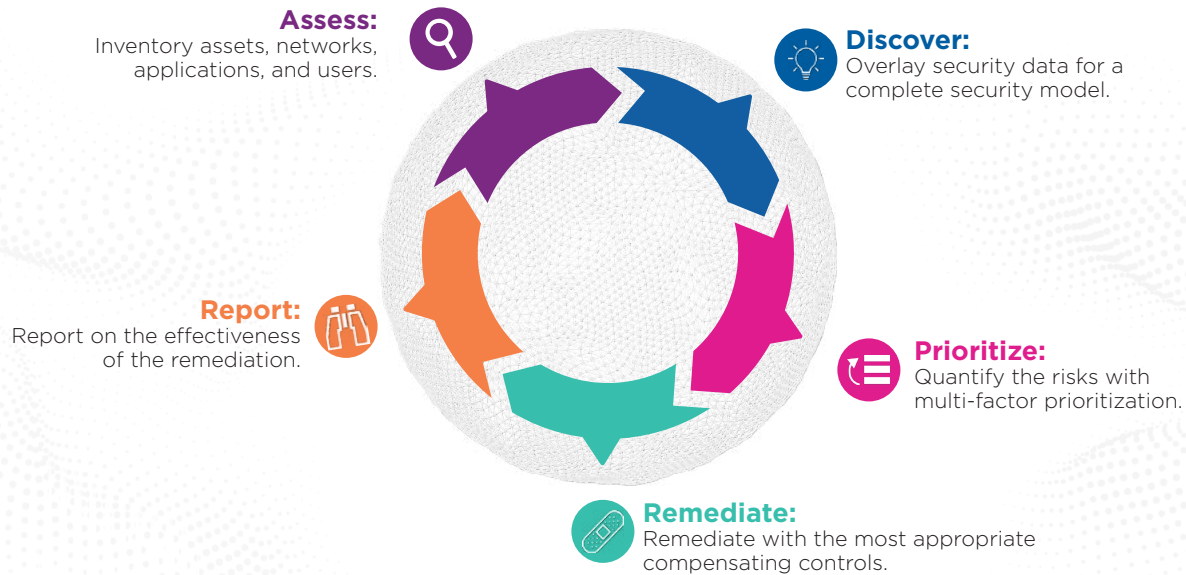
This is why more and more organizations are looking for vulnerability management solutions to help them address this challenge. However, not all vulnerability management solutions are created equal.

This guide is for cybersecurity professionals looking to select a solution that can help them effectively manage the vulnerabilities across their organization.



Vulnerability management program

An effective vulnerability management program combines technologies and procedures that typically span five phases.



LOOK FOR a vulnerability management solution that effectively supports each phase in the program:

1. Assess

In this phase, create an inventory of all the assets, endpoints, servers, network devices, cloud infrastructure, applications, and users, that need to be included in the Vulnerability Management program.

2. Discover

In this phase, overlay aggregated security data from a variety of sources, including the output from vulnerability scans, and threat intelligence feeds.

3. Prioritize

In this phase, quantify the cyber risks based on the individual exposures and prioritize those, ensuring you apply your technical resources where they can be most effective.

4. Remediate

In this phase, select the most appropriate remediation, and where a complete resolution is not possible, choose from a range of possible compensating controls.

5. Report

In this phase, report on the effectiveness of remediation efforts and communicate risk levels to relevant stakeholders.

Assess

In this phase, your organization gains a comprehensive understanding of your environment. This involves identifying the assets, systems, and data in scope for the Vulnerability Management program to ensure that it is well-defined, aligned with the business objectives, and can provide measurable value.

Attack surface model

For the Vulnerability Management program to be effective, it must be based on a thorough understanding of the organization's attack surface. This can only be achieved by gathering and aggregating data that is often held in separate silos across the technology estate, creating a master inventory and attack surface map that includes:

- + **Network device and infrastructure data.**

Interactions between network devices, servers, endpoints, users, and applications across networks help to identify potential access points.

- + **Firewall and IPS configuration.**

Identification, deployment, and configuration of security controls.

- + **Configuration and Management Databases (CMDBs).**

Aggregated asset data from separate silos.

- + **Cloud infrastructure.**

Including assets across the on-premise estate and out into multi-cloud infrastructures.

- + **Operational Technology (OT) as well as Information Technology (IT) data.**

Location, connection, and configuration of critical applications and assets across the organization.

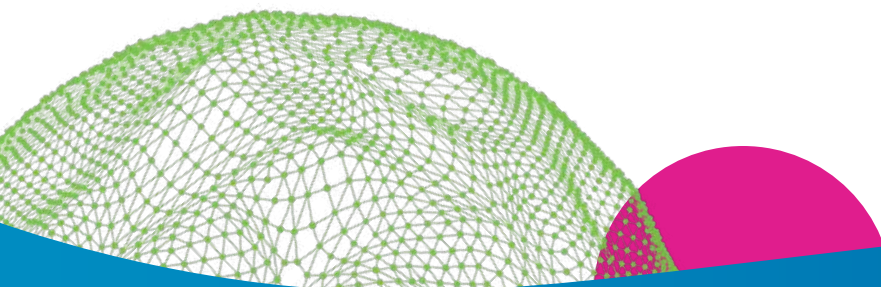


LOOK FOR solutions that provide a “dynamic security model” of the environment, incorporating all network security rules and access controls in addition to the inventory of assets. This type of model is a fundamental enabling technology for an effective vulnerability management program. In essence, the model acts as a “digital twin” of the real environment and provides a single source of truth that will inform the assessment, prioritization, and remediation of vulnerabilities based on the risk that is unique to your specific business environment.



ASK VENDORS:

Does the solution deliver a dynamic security model, incorporating not only an inventory of assets but also an attack map enriched with network security rules and access controls?



Discover

In this phase, your team overlays security data from various sources onto the dynamic security model, including the output from vulnerability scans, threat intelligence feeds, and attack surface analysis.

Aggregated vulnerability data

Many organizations use multiple vulnerability scanners to search for vulnerabilities in the IT estate that might expose them to compromise. This approach is designed to help identify the maximum number of vulnerabilities, but it has the unwanted side effect of producing reports containing large numbers of duplicate vulnerabilities from the different vendor's scanners.



LOOK FOR a vulnerability management solution that can consolidate the output from multiple scanners into a single view for better visibility of the overall picture.



ASK VENDORS:

Does the solution aggregate and consolidate scan data from multiple scanner vendors?

Scan frequency gaps

The data the scanners generate is vital, but alone, it is not enough to build a successful vulnerability management program. Frequent scanning can impact performance and may impose an unacceptable overhead on systems deemed critical to the operation of the business. As a result, scans are often run infrequently, leading to potentially dangerous gaps in awareness with months or even quarters going by before vulnerabilities are discovered.



LOOK FOR solutions that mitigate the “scanning awareness gap” by leveraging data aggregated from CMDB databases and other asset management tools to continuously uncover infrequently scanned devices and their vulnerabilities.

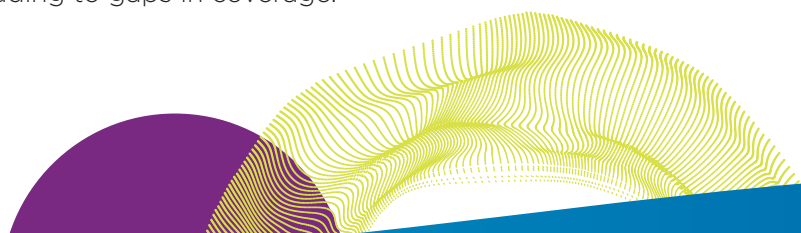


ASK VENDORS:

How does the solution ensure vulnerabilities are continuously discovered in the periods between scans?

Unscannable assets

Unfortunately, scanners do not cover all systems and networks across your attack surface. Scanners rely on agents installed on individual assets. Unfortunately, agents are not available for every type of asset. For example, scanners cannot scan many network devices for vulnerability data, leading to gaps in coverage.



Additionally, Operational Technology (OT) networks and air-gapped networks designed to process classified or high-value data are segmented to protect them from compromise from less secure or untrusted networks. These networks are hard or even impossible to scan for the presence of vulnerabilities, and yet it is these networks that routinely carry the organization's most valuable data.



LOOK FOR a solution that discovers unscanned devices and their vulnerabilities.



ASK VENDORS:
How does the solution deal with “unscannable” systems and networks?

Multi-source threat intelligence

An effective vulnerability management solution will enable your organization to manage these “unscannable” systems and networks, by maintaining a list of all the deployed products and assets and applying the latest threat intelligence to highlight vulnerabilities that exist on those systems.

The intelligence feed should enable the identification of vulnerabilities in standard operating systems, browsers, software, and databases using a combination of sources including the National Vulnerability Database (NVD), published vulnerability repositories, threat intelligence feeds and platforms, and vendor-specific security feeds.



ASK VENDORS:
Does the solution apply the latest threat intelligence from a range of built-in and third-party sources?

Prioritize

A vulnerability management program based purely on poorly filtered scanner output often overwhelms hard-pressed security teams with too many high or critical-priority tasks.

Large organizations routinely deal with 100s of thousands of vulnerabilities across the attack surface. It is not uncommon to see 65% of these vulnerabilities classified as “high or critical” severity. Without an understanding of the specific risk each vulnerability represents to your organization, your IT team simply doesn't know where to begin or how to best focus their limited time and resources.



LOOK FOR a solution that prioritizes vulnerabilities with the most risk to your organization, enabling your team to allocate resources effectively and efficiently to address them.

Business asset classification

There is no “one size fits all” when it comes to prioritizing vulnerabilities across an organization. Often, different business units will have very different views of the criticality of their specific business assets and applications.



LOOK FOR a solution that enables business units within the organization to categorize assets based on factors such as geography, technology, business function, applications, services, and owners.



ASK VENDORS:

Does the solution enable business units to customize the prioritization risk formula to my specific needs?

Multi-Factor prioritization

At the core of a vulnerability management program is a comprehensive risk assessment. This assessment is conducted to identify and evaluate vulnerabilities by considering various factors, including the likelihood of exploitation, potential impact on systems and data, and the criticality of affected assets. By carefully analyzing these elements, vulnerabilities are prioritized based on their level of risk, ensuring that the most critical and impactful vulnerabilities are addressed with the highest urgency. Risk assessment serves as a foundation for effective decision-making and resource allocation within the vulnerability management program.



LOOK FOR a solution that incorporates the following risk factors:

CVE severity - as identified by the Common Vulnerability Scoring System (CVSS) and derived from an assessment of the extent to which the vulnerability could compromise confidentiality, integrity, and availability, the likely attack vector, and the ease with which it could be deployed.

Criticality - the importance of the asset to your business or business unit. This can be difficult to estimate but a numeric value within a predefined range provides a relative measure that helps concentrate scrutiny on those assets that matter most to your organization.



ASK VENDORS:

How does the solution capture and leverage the importance of an asset to the business?

Exposure - the extent to which a given asset hosting a vulnerability is accessible to an attacker across the network. The most important factor in the prioritization calculation, this attribute can only be accurately assessed with an in-depth understanding of the underlying network, firewalls, and IPS devices. Factoring in exposure enables the organization to prioritize effectively, for example by catching vulnerabilities classified with a medium and/or low CVE score, but which may be high-risk due to their exposure.



LOOK FOR a solution that understands the accessibility of each vulnerability — based on the in-depth knowledge of the underlying network, firewalls, and IPS devices — from various threat origins.

**ASK VENDORS:**

Does the solution leverage attack paths to understand and prioritize the risk of specific vulnerabilities?

External and lateral attack paths

To manage cyber risk across the attack surface, it is vital that you can quickly see the links and dependencies between vulnerable assets.



LOOK FOR a solution with built-in attack path analysis based on an understanding of the network topology, segmentation, and network device configuration as well as all the vulnerable assets.

**ASK VENDORS:**

Is your solution capable of detailed attack path analysis both from external sources and laterally from within?

This information helps both the IT and the security teams drive the vulnerability management program, enabling the team to scrutinize firewall and network configurations, identify vulnerable assets, and run simulations to illuminate potential exploit routes.

**ASK VENDORS:**

Does the solution support attack simulation exercises?

Remediate

The key output of an effective vulnerability management program is a thorough remediation plan. This plan considers the risk level associated with each vulnerability, the available resources, and the potential impact on business operations. By considering these factors, the remediation plan ensures that the most critical vulnerabilities are promptly and effectively addressed, minimizing risks and safeguarding business operations.

Automated ticketing

In an effective program, the vulnerability management solution should provide an automated ticketing system that can be used to log vulnerabilities and track remediations. This system should be configurable according to risk score so that vulnerabilities above a certain threshold automatically generate a ticket that can be used to track the progress of the remediation.

**ASK VENDORS:**

Does the solution automatically generate tickets for vulnerability tracking and resolution?

SOAR/ITSM integration

Many organizations utilize Security Orchestration Automation and Response (SOAR) and IT Service Management (ITSM) solutions. The chosen vulnerability management solution should integrate seamlessly with these systems so the organization can orchestrate the entire process from identification, through prioritization, to remediation and resolution.

**ASK VENDORS:**

Does the solution integrate with your chosen ITSM/SOAR system for ticketing and remediation?

Alternative compensating controls

Scanners identify vulnerabilities for subsequent patching. While this is essential, the cadence between patching cycles is often a matter of weeks or even months, leaving a vulnerable asset exposed to potential compromise for lengthy periods.



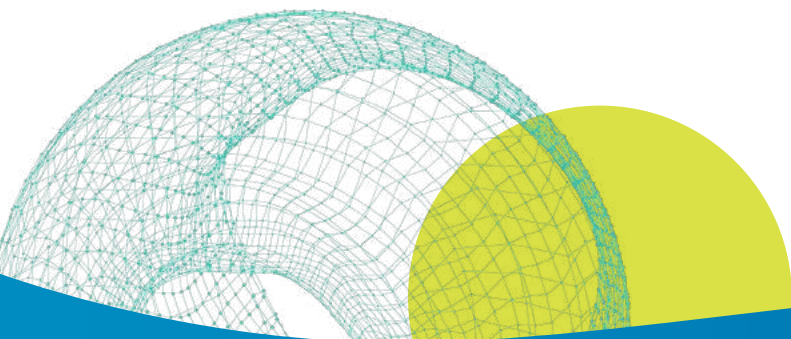
LOOK FOR a solution that analyzes each exposure and suggest alternative compensating controls that can be used to mitigate the threat until the asset can be patched.

These alternative compensating controls will typically include:

- + **IPS signatures** - can be used to quickly close exposure to potential attacks.
- + **Firewalls rules and security tags** - can be changed to prevent attackers from reaching a vulnerable asset.
- + **Software upgrades** - to older versions of software can eliminate vulnerabilities across multiple assets exposed to a potential exploit.
- + **Software patches** - will fix known vulnerabilities across various assets that are exposed to a potential exploit.

**ASK VENDORS:**

Will the solution automatically suggest alternative compensating controls for situations where immediate patching is not possible?



Report

Reporting metrics play a vital role in a vulnerability management program. These metrics help demonstrate the organization's capabilities in vulnerability management, providing valuable insights that inform decision-making and enable stakeholders to assess overall cyber exposure.



LOOK FOR a solution that reports on prioritization focus, detailed risk analysis, and vulnerability ticketing status. By incorporating these metrics, organizations can track progress, and measure the effectiveness of remediation efforts against SLAs.



ASK VENDORS:

Can the solution report on patching and remediation against SLAs?

Can the solution identify, track, and report on open and overdue remediation tickets?

Compliance with legislative frameworks

Governments worldwide are broadening the definition of what represents Critical Infrastructure (CI) to include a wider range of sectors. Organizations within these sectors are required by legislative directives to implement stricter vulnerability assessment and management measures and report any incidents to the relevant authorities.



LOOK FOR a solution that provides executive reports on how risk is being managed that can be presented to internal/external auditors in line with legislative directives.



ASK VENDORS:

Does your solution provide clear and simple risk management executive reports?

Cyber risk quantification

Traditionally, vulnerability management programs have focused on delivering technical reports that show compliance with patching and remediation SLAs.

With cybersecurity increasingly the subject of board-level scrutiny, security practitioners are now looking at ways to report on vulnerability and risk exposure using the financial vernacular of the boardroom, expressing risk in monetary terms.



LOOK FOR a solution that takes the output from multi-factor prioritization and combine it with an understanding of asset value, to report on the risk exposure of a given asset or set of assets across the business in terms of dollars and cents. These reports enable security leaders to articulate risk in terms the boardroom can readily understand and appreciate.



ASK VENDORS:

Can your solution quantify the cyber risk in financial terms?

Other considerations

Deployment Options

Different organizations have differing views as to their preferred deployment model – on-premises or in the cloud.



LOOK FOR a solution that offers flexibility over how you can deploy the vulnerability management solution to match your preferred deployment model.



ASK VENDORS:

Can your solution be deployed as an on-premises appliance-based solution, or in the cloud, either as a virtual image or as a SaaS offering?

Innovation

The threat landscape is constantly evolving. As cyber criminals look to embrace new tools and techniques such as Artificial Intelligence (AI) to help them, vendors should be constantly responding with innovations designed to combat the latest threats.



ASK VENDORS:

What is your strategy for innovating? How are you planning to respond to new threats such as the use of AI?

Professional services

Working with an expert professional services team can help you get the most out of your vulnerability management solution. Look for a vendor that offers a proven and documented methodology for deployment, together with experience in integration, assessment, training, and rollout services.



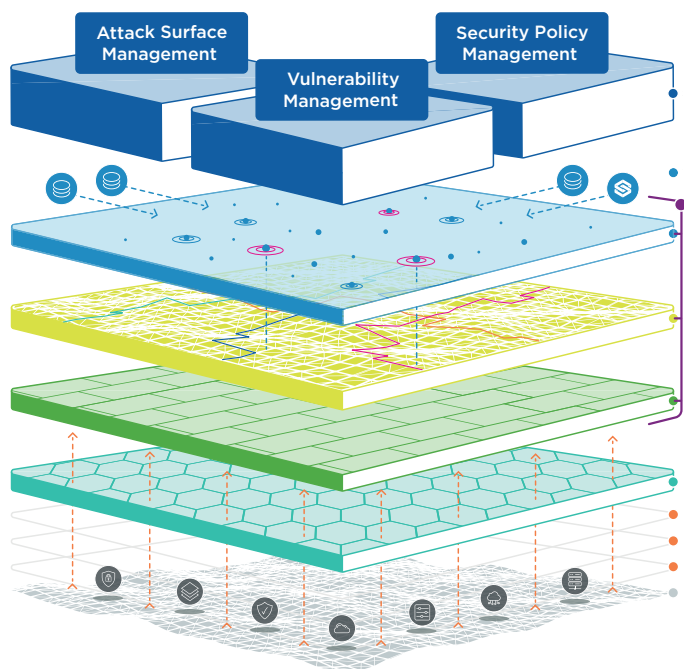
ASK VENDORS:

Does the vendor offer best-in-class processes for deployment, integration, and adoption?



About Skybox Continuous Exposure Management

The Skybox Vulnerability Management solution is part of the Skybox Continuous Exposure Management (CEM) platform. Our CEM package is a set of modular solutions designed to help customers implement continuous exposure management programs across the organization.



Attack Surface Management

Manage cyber risk with a complete visual inventory of the assets, applications, and users across your hybrid attack surface. Use step-by-step attack path analysis and simulation, to detect exposures and pre-empt attacks.

Vulnerability Management

Focus the security team, with multi-factor risk assessments that combine vulnerability scanner data and aggregated threat intelligence, combined with smart prioritization based on severity, importance, exploitability, and network exposure.

Security Policy Management

Take control of network security policies across the attack surface. Analyze network zoning and connectivity, manage, and optimize firewall rule bases, assess, and automate firewall changes, and generate the reports vital for compliance audits.

**Want to learn more?
Get a demo or talk to an expert:**

skyboxsecurity.com/request-demo 

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of dynamically changing attack surfaces. Our SaaS-based Exposure Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization. The vendor-agnostic solution intelligently optimizes security policies, actions, and change processes across all corporate networks and cloud environments. With Skybox, security teams can now focus on the most strategic business initiatives while ensuring enterprises remain protected.