SKYBOX SECURITY

Solution Brief

Risk-based vulnerability prioritization and remediation

Skybox Vulnerability and Threat Management

Introduction

Digital transformation has accelerated, organizations have rapidly migrated to the cloud and security has elevated to become a board-level concern. Attack surfaces are expanding, threat actors growing in sophistication and new vulnerabilities continuing to mount. Security teams are faced with a growing challenge of finding and fixing vulnerabilities that pose the greatest business risk, and their existing programs can no longer rely on simplistic prioritization efforts and volumetric patch management. Vulnerability management programs need to mature with multi-factor prioritization that is centered around exposure risk analysis that accounts for hybrid network context and includes simulation of all potential attack paths. With the continuing increase of vulnerabilities, having an accurate representation of exposure is fundamental to keep remediation focused on eliminating the most critical risks.

Business challenges

Security organizations are dealing with a widening skills gap, increasingly fragmented networks, growing attack surfaces, increasing workloads, visibility and remediation gaps, and ineffective, incomplete scanning.

The ever-increasing volume of vulnerabilities is outpacing capacity to effectively remediate. This volume makes it very difficult to prioritize and remediate those that post the highest risk.

Further, most enterprises typically have legacy infrastructure, a growing proliferation of different products and device types, and a long list of unattended vulnerabilities that increases risk: seventy-five percent of exploited

Summary

Solution

The Skybox Vulnerability and Threat Management solution provides a centralized, automated and vendor-agnostic approach for enabling full-lifecycle vulnerability management across hybrid and multi-cloud infrastructures.

Business challenge

+ Increasing volume of new vulnerabilities
+ Poor visibility with proliferation of new technologies and devices
+ Limited resources

Business benefits

+ Increased accuracy of vulnerability assessment
+ Prioritize and identify optimal remediation options
+ Reduction in overall network risk profile
+ Investment protection

Business value

+ Reduced time to remediation
+ Reduced resource cost
+ Reduced cyber threat exposure
+ Accelerate time to value
+ Reduced operational burden with Vulnerability Control Cloud Edition

vulnerabilities in 2020 were more than two years old.[1] Also, advanced and multi-stage attacks are growing as evidenced by the increasing number of ransomware attacks now predicted to happen at a rate of every 11 seconds.[2]

Based on these current circumstances corporate security teams need to increase their focus on eliminating specific vulnerabilities that are exposed to potential attacks with more mature assessment, prioritization, and remediation capabilities. Without timely and accurate identification of high-risk vulnerabilities, remediation efforts will end up closing large volumes of vulnerabilities and yet still fail to reduce business risk.

Enjoy investment protection, accelerated time to value, and reduced operational burden with Vulnerability Control Cloud Edition, a scalable, modern solution for managing vulnerability risk and exposure in hybrid environments.

Traditional approaches leave gaps

Traditional approaches don't take into account all factors that influence vulnerability risk. This leaves security teams wasting resources on issues that attackers may never find or know how to exploit. Relying on spreadsheets and manual analysis to gain this insight leads to frustration and futility as massive volumes of vulnerabilities continue to be released weekly. Further, the scan-and-patch approach omits crucial elements of the vulnerability management workflow, especially in how remediation priorities are set. Scanners do not provide a comprehensive understanding of network topology and therefore can't identify the organization's actual exposure.

To date, prioritizing vulnerabilities by CVSS score and exploitability level has been the most common technique. However, this approach does not address important questions such as:

+ How important is this asset to our organization?
+ Is this vulnerability an imminent threat due to its exposure to a malicious or accidental insider or an external threat actor?
+ If it is exposed, how quickly can an attacker exploit it and move laterally through the network?
+ Can I quickly close off critical and exposed assets from this threat within moments of being alerted to the presence of the vulnerability or in the event of a breach?

Risk-based vulnerability prioritization

To intelligently prioritize remediation of vulnerabilities, Skybox® Security takes a fundamentally different approach based on analysis of exposure and business risk.

Skybox helps customers extend remediation efforts well beyond patch management with risk-based prioritization that yields multiple options for eliminating exposure risk in the most effective and efficient way possible.

By viewing vulnerabilities through multiple lenses— including asset importance, threat activity in the wild and network exposure to threat origins — Skybox gives you the power to target action where it matters most, proactively reducing your risk of attack.

With a risk-based vulnerability approach, prioritization is enhanced through:

+ Automating vulnerability analysis based on severity, asset importance, exploitability and exposure, among other factors
+ Assigning straightforward, trackable risk scores to vulnerabilities, assets and groups
+ Prioritizing patches that will have the biggest impact on risk reduction

[1] Cybersecurity vulnerability statistics: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

[2] Cybersecurity Ventures predictions: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

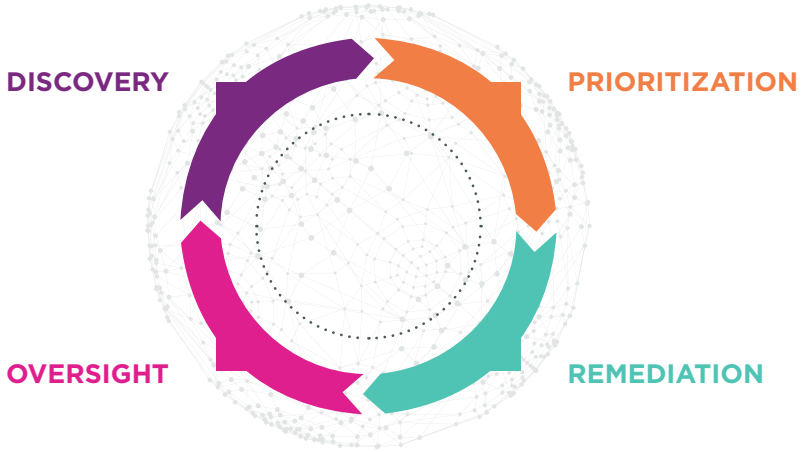
Full-lifecycle vulnerability and threat management

The Skybox Vulnerability and Threat Management solution provides a centralized, automated and vendor-agnostic approach for enabling full-lifecycle vulnerability management across hybrid and multi-cloud infrastructures. Our unique threat and context aware analytics engine aggregates a wide range of data from multiple sources including scanners, security and network infrastructure, various configuration databases, and non-scannable assets.

We don't just serve up this data and information, we provide risk scoring and remediation prioritization of vulnerabilities based on asset prioritization, exploitability, and exposure analysis. With Skybox, security teams can automatically map and visualize their attack surface to determine the best remediation options to reduce cybersecurity risk exposure on a continuous basis.

Skybox Vulnerability and Threat Management

An intelligent approach to full-lifecycle vulnerability threat management



DISCOVERY

+ **All scan data***
+ **Patch & EDR data***
+ **CMDB data***
+ **Security controls***
+ **Network data***
+ **OT vulnerabilities***
+ Threat intelligence

***Skybox supplements over traditional vulnerability management programs**

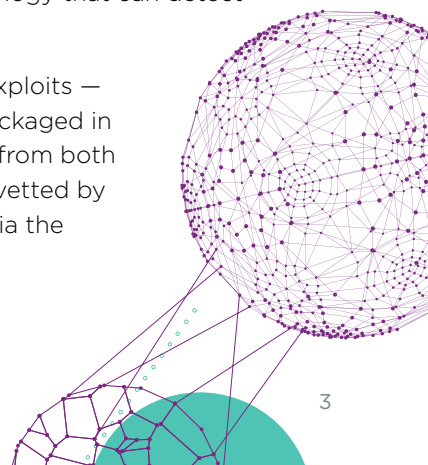
Vulnerability discovery

Accurate vulnerability prioritization starts with good data. Active scanning is an important component of vulnerability discovery but can leave blind spots in "unscannable" network zones and devices, as well as rapidly changing cloud environments.

With its threat and context-aware analytics engine, Skybox aggregates data from over 150 sources including scanners, security and network infrastructure, configuration databases and non-scannable assets. This extensive data is the foundation of a network model that is precise, accurate and targeted at addressing your highest risk.

The Skybox approach to vulnerability discovery enhances scanner data, consolidating results from third-party scanners, app and web scanners, OT platforms and more. It also fills in blind spots using unique passive assessment technology that can detect vulnerabilities in off-limits network zones and devices.

Further, Skybox ingests information on the characteristics of exploits — active exploits in the wild, sample exploit code and exploits packaged in distributed crimeware. Skybox's threat intelligence is acquired from both public and private sources on an ongoing basis, analyzed and vetted by the Skybox® Research Lab and delivered to Skybox products via the Skybox intelligence feed.



PRIORITIZATION

+ **Business impact***
+ **Exposure***
+ Exploitability
+ Severity
+ **Density***
+ Age
+ **Proximity***

***Skybox supplements over traditional vulnerability management programs**

Vulnerability prioritization

Skybox uniquely prioritizes vulnerabilities based on asset importance, CVSS scores, exploitability and exposure analysis. This comprehensive approach is required in order to produce accurate risk scoring. Vulnerability intelligence comes from extensive databases of information on known vulnerabilities and includes details such as:

+ Conditions such as operating systems, versions and other applications installed that would affect the exploitability of a vulnerability
+ Exploitation effect on confidentiality, integrity and availability (CIA) values
+ Research on the vulnerability, such as the National Vulnerability Database (NVD) listing, vendor bulletins, etc.
+ History of changes in the vulnerability as it relates to severity, exploitation, available patches, etc.
+ List of remediation and mitigation solutions
+ Severity ratings from multiple sources (NVD, IBM X-Force, scanning vendors, etc.) and Common Vulnerability Scoring System (CVSS) scores

Vulnerability context

By modeling the environment in which a vulnerability occurrence exists, teams can understand the exposure of vulnerabilities to threat origins — a critical component of risk- based vulnerability prioritization.

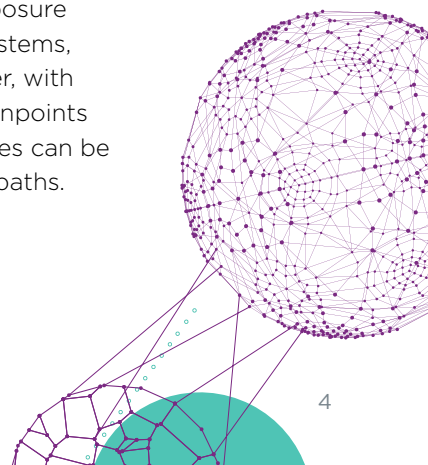
Skybox builds a network model which is a dynamic representation of the hybrid environment including corporate networks, private cloud, public cloud, and OT. It understands all of the devices, vulnerabilities and configurations within the environment and can be used to run assessments and attack simulations.

The network model provides security and network teams the ability to analyze network, cloud, IT/OT and security configurations together to proactively gain full context and understanding of the attack surface. Skybox aggregates data sets across security, cloud and network technologies to include:

+ Network topology (routers, load balancers, switches)
+ Security controls (firewalls, IPSs, VPNs)
+ Assets (servers, workstations, networks — including traditional IT, multi-cloud and OT environment

Exposure analysis and attack simulation

The most critical step of vulnerability analysis is determining its exposure in your network. Exposure analysis is possible when disparate data repositories, such as patch and asset management systems, configuration data, threat intelligence feeds and network security devices are brought together, with data normalized and modeled to infer the presence of vulnerabilities. This exposure analysis pinpoints assets that are accessible to internal and external threats. By understanding exposure, resources can be devoted to vulnerabilities accessible to threats or identify mitigation options to cut off attack paths.



Skybox determines the exposure of the vulnerability by simulating attacks on the network model. With a network model, enterprises can advance attack simulation capabilities to incorporate deeper attack context and insights to explore all possible attack paths, see all of the devices that could be touched by an attacker, and determine the best course of action to prevent breaches.

Automated simulations are run from all threat origins (ingress points) and assess all network paths to determine whether or not a vulnerable asset can be reached. Such vulnerabilities are flagged as direct exposures.

Directly exposed assets are used in secondary simulations to represent a compromised asset (as would be the case in multi-step attacks). Vulnerabilities reached in these secondary simulations are flagged as indirect exposures.

REMEDIATION

Planning:

+ Assess patch options
+ **Assess non-patch options***
+ **Mitigation recommendations***

Assignment:

+ Generate ticket
+ ITSM workflow
+ **Provide context***
+ Provide SLA
+ Communicate to ops team

***Skybox supplements over traditional vulnerability management programs**

Smart and automated remediation

Skybox presents the most effective options for remediating the most vulnerabilities or the most impacted assets. With our new Solutions View, teams can instantly see solutions that improve the asset risk score by the highest percentage.

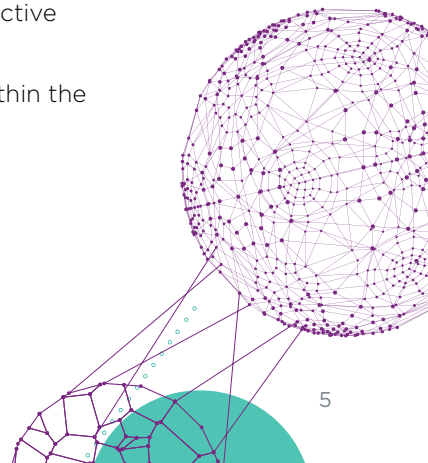
This view of vulnerabilities by solution provides enterprises with possible alternatives to patching. Skybox proposes changes to firewall rules, updates to IPS signatures and other alternatives to select the remediation approach that best aligns with your unique environment and change management processes. As a result, customers benefit from increased flexibility, a significantly reduced mean time to remediate, and most importantly a reduction of business risk.

Skybox also integrates with 3rd party ticketing systems to provide closed-loop remediation accountability. When vulnerabilities have been prioritized based on the elements mentioned above, enterprises can quickly work to remediate the ones that are highest priority.

Unlike traditional vulnerability management programs, Skybox provides contextual remediation options based on deep insight into the network infrastructure and understanding of communication paths, attack paths, potential blast radius and the level of sophistication of a threat actor. This allows organizations to consider alternative ways to deal with systems that are mission-critical or cannot be taken offline for long periods of time.

Through smart remediation, Skybox customers benefit from:

+ Automation to enable rapid closure of security gaps
+ Insight from integrated data to accelerate decision-making
+ Breach and attack simulation capabilities to develop proactive defenses
+ Connected remediation processes to break down silos within the security stack



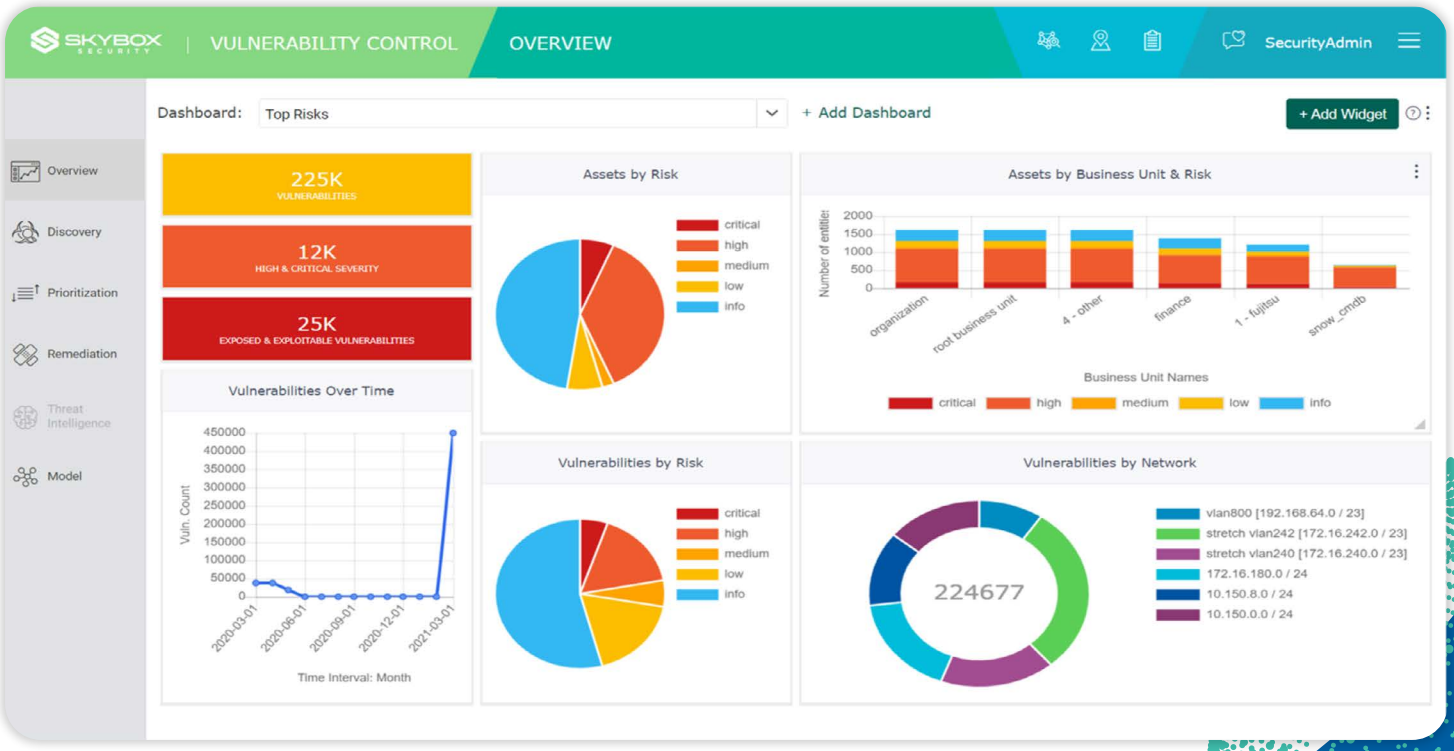
Audit and Oversight

As you adopt a mature vulnerability management program, it will be critical to consistently validate and refine the data aggregation processes that build and maintain the corporate network model. Accurate reporting and an understanding of trends over time will improve the predictability that is vital to successfully preventing attacks.

With Skybox, executive reporting is simple and easy. Fully customizable, you can view insights most relevant to your business to drive informed decision making. Cross-functional teams can reference a single source of truth to access to the insight needed for their organizations.

Skybox provides reports on trends over time and emphasizes downward trends that could negatively impact risk scores such as:

+ Decrease in scan frequency
+ Decrease in the number of machines scanned
+ Increase in high-risk vulnerabilities or exposed vulnerabilities



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 their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization.