



Reduce cyber exposure and mitigate threats with a risk-based vulnerability management framework

Improve threat detection and response times with automated workflows for vulnerability risk prioritization and mitigation.

Challenges

Cybercrime inflicted cumulative damages of 6 trillion USD in 2021, according to Cybercrime magazine. This means that if cybercrime were an independent national entity, it would have ranked 3rd after USA and China in terms of GDP.¹ In the same year, 20,175 new software vulnerabilities were discovered, representing an all-time high.² This increased the burden on Vulnerability Management teams, and the cyber security talent gap left small teams struggling with complex manual VM workflows in sprawling IT environments.

A silo-ed environment means that Threat Hunting and Vulnerability Management teams do not achieve a shared understanding of the vulnerabilities that are linked to a specific malware. So, it becomes difficult for organizations to achieve in practice the improvement in Mean Time to Detect/Mean Time to Remediate that should result in theory from proactive vulnerability management practices.

Use cases

- Automated workflows for vulnerability discovery, prioritization, remediation, and reporting
- Vulnerability risk scoring based on CVSS scores, exploitability, asset importance, and network exposure
- Ability to find vulnerabilities by malware name for targeted threat mitigation
- Quantification of cyber risk in economic terms based on asset loss impact and probability

¹ Cybercrime to cost the world \$10.5 trillion annually by 2025, Cybercrime Magazine, November 2020

² Vulnerability and threat trends report 2022, Skybox, April 2022

The four pillars of Vulnerability Management are discovery, prioritization, remediation, and reporting. Security operations teams struggle to execute these four pillars due to the challenges listed below:

Vulnerability discovery	Vulnerability prioritization	Vulnerability remediation	Vulnerability reporting
<p>Fragmented attack surface visibility resulting from haphazard growth of visibility tools without integrations between them, rapidly multiplying cloud workloads and non-scannable assets, and blind spots resulting from time gaps between active spans.</p>	<p>No consistent framework for pinpointing those vulnerabilities most likely to generate a breach, VM teams grappling with spreadsheets and manual analysis to eliminate large volumes of critical or high-severity CVEs, increased alert fatigue, too many false positives.</p>	<p>State of constant urgency, excessive dependence on patches and software updates as the sole methods for mitigating vulnerability risk, an increasing burden on overworked IT teams who struggle to plan, test, and deploy patches and updates.</p>	<p>Lack of consistent, automated reporting processes for monitoring VM program efficacy; no consistent mechanism for tracking performance against SLAs; no way to deliver scheduled reports to executives and stakeholders to demonstrate continuous compliance against internal benchmarks or regulatory mandates.</p>



Solution

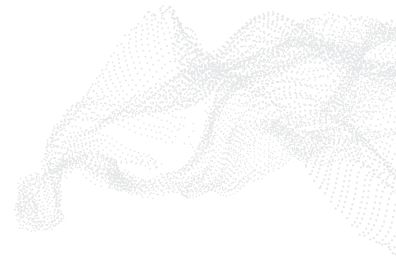
The Skybox Platform helps customers solve these challenges with context-driven automation and actionable threat intelligence.

Vulnerability Discovery

The Skybox Platform employs multiple techniques for ingesting asset and vulnerability information,³ which is then normalized:

- + Active VA tools (Qualys, Tenable, Rapid7)
- + OT passive scanning solutions (Nozomi Networks, Claroty, Forescout, Tenable.ot, Cyberx)
- + Various asset, configuration, and patch management databases

³ Device Support Table, Skybox, 2022



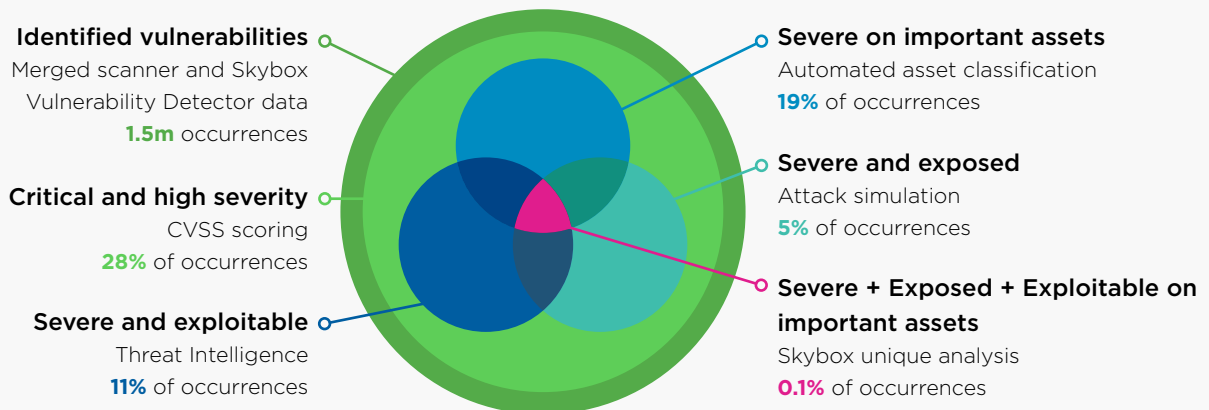
- + Public cloud environments (AWS, GCP)
- + Container security solutions (Twistlock/Prisma Cloud)
- + EDR solutions (Microsoft Defender for Endpoint, CrowdStrike Falcon)
- + Unique scanless detection technology

Skybox scanless vulnerability detection expands coverage by correlating asset information from generic CMDB parsers and patch management repositories with updated vulnerability data from Skybox threat intelligence. The result is the continuous non-intrusive discovery of vulnerabilities on non-scannable assets (routers, switches, and sensitive OT devices), as well as filling in the gaps between active scan events on scannable assets. A new Skybox innovation called Deployed Product list extends scanless detection capabilities without requiring asset modeling or CMDB access - knowledge of the deployed technology stack is combined with Skybox threat intelligence to pinpoint vulnerable assets.

Vulnerability prioritization: risk scoring

Skybox uses a flexible and customizable algorithm to compute risk scores for assets and vulnerability occurrences (a specific instance of a vulnerability on an asset). By default, the framework uses 4 key criteria. The algorithm supports formula flexibility so that each organization can control the risk factors to be included in the formula and the weight for each factor. This approach facilitates a tailored risk posture based on an organization’s business logic. The factors are:

- 1 **CVSS scores**, assigned by NVD and affiliated bodies
- 2 **Asset importance**, assigned by the organization based on the value of an asset to an enterprise
- 3 **Exploitability**, based on Skybox threat intelligence, vulnerabilities that are exploited in the wild or have exploits available are assigned higher scores
- 4 **Asset or vulnerability exposure**, based on attack path analysis to determine the reachability of a target from potential threat origins



Skybox uses risk scoring to pinpoint the most harmful vulnerabilities

Vulnerability prioritization: exposure analysis

Exposure analysis uses the underlying network model and attack simulation between source/destination pairs to model the exposure of an asset or vulnerability to attackers. Exposure analysis results encompass much more than simple binary verdicts such as “exposed” or “not exposed”.

Possible verdicts of asset or vulnerability exposure include:

Direct exposure	One or more attackers have a direct network path to the vulnerable asset.
Presumed direct exposure	Same as direct exposure but unverified whether the service port is listening for incoming connections.
Indirect exposure	Asset can be exploited through lateral movement from other exploited assets.
Potential exposure	Vulnerability can be accessed but requires additional authentication on the asset for exploitation.
Protected	Vulnerability is protected by an IPS signature.
Inaccessible	Vulnerability is accessible over the network to attackers.

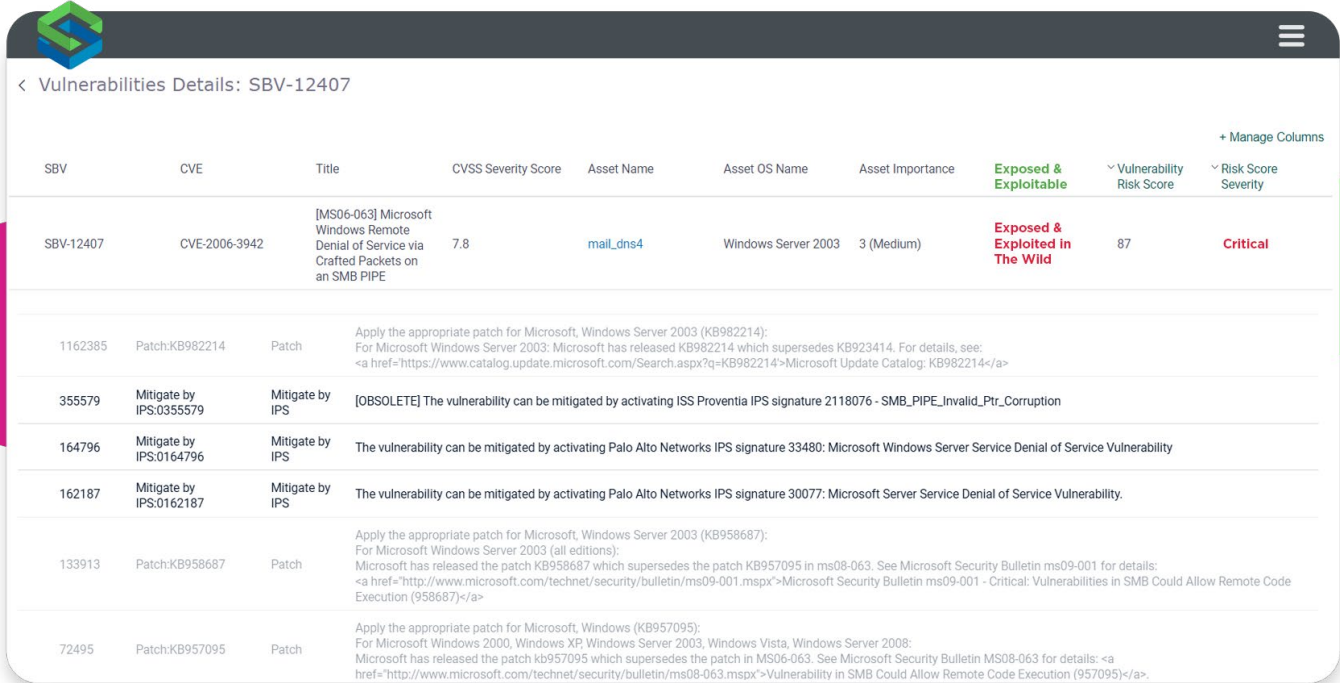
Standard commoditized solutions for vulnerability risk scoring have no understanding of network exposure and so introduce false positives. With these legacy solutions, vulnerability occurrences that are exploitable in the wild would be attributed a high risk score even if they are inaccessible to attackers.

Vulnerability remediation

The Skybox Platform, based on contextual analysis of IT, multi-cloud, and OT environments, can recommend diverse remediation solutions:

- + Patching
- + Software updates
- + IPS signature
- + Configuration changes, such as disabling a service

Network-based security controls such as IPS signatures and configuration changes can relieve the urgency around patch applications. This buys Vulnerability Management teams much-needed time for planning, testing, and deployment of patches. Commoditized vulnerability management solutions that do not understand network topology cannot recommend network based security controls for vulnerability remediation. Skybox Vulnerability Control has its own ticket management system and can also be integrated with leading ITSMs such as ServiceNow.



SBV	CVE	Title	CVSS Severity Score	Asset Name	Asset OS Name	Asset Importance	Exposed & Exploitable	Vulnerability Risk Score	Risk Score Severity
SBV-12407	CVE-2006-3942	[MS06-063] Microsoft Windows Remote Denial of Service via Crafted Packets on an SMB PIPE	7.8	mail_dns4	Windows Server 2003	3 (Medium)	Exposed & Exploited in The Wild	87	Critical
1162385	Patch:KB982214	Patch	Apply the appropriate patch for Microsoft, Windows Server 2003 (KB982214): For Microsoft Windows Server 2003: Microsoft has released KB982214 which supersedes KB923414. For details, see: Microsoft Update Catalog: KB982214						
355579	Mitigate by IPS:0355579	Mitigate by IPS	[OBSOLETE] The vulnerability can be mitigated by activating ISS Proventia IPS signature 2118076 - SMB_PIPE_Invalid_Ptr_Corruption						
164796	Mitigate by IPS:0164796	Mitigate by IPS	The vulnerability can be mitigated by activating Palo Alto Networks IPS signature 33480: Microsoft Windows Server Service Denial of Service Vulnerability						
162187	Mitigate by IPS:0162187	Mitigate by IPS	The vulnerability can be mitigated by activating Palo Alto Networks IPS signature 30077: Microsoft Server Service Denial of Service Vulnerability.						
133913	Patch:KB958687	Patch	Apply the appropriate patch for Microsoft, Windows Server 2003 (KB958687): For Microsoft Windows Server 2003 (all editions): Microsoft has released the patch KB958687 which supersedes the patch KB957095 in ms08-063. See Microsoft Security Bulletin ms09-001 for details: Microsoft Security Bulletin ms09-001 - Critical: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)						
72495	Patch:KB957095	Patch	Apply the appropriate patch for Microsoft, Windows (KB957095): For Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008: Microsoft has released the patch kb957095 which supersedes the patch in MS06-063. See Microsoft Security Bulletin MS08-063 for details: Vulnerability in SMB Could Allow Remote Code Execution (957095)						

IPS signatures mitigate vulnerability risk, relieving the urgency to deploy patches

Vulnerability reporting

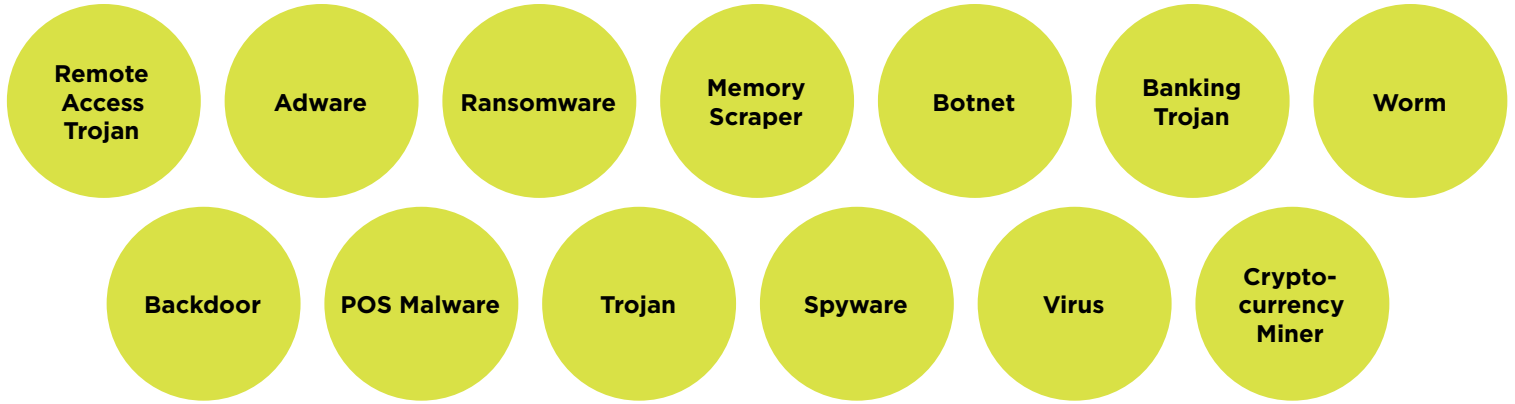
The Skybox Platform enables extensive codeless reporting or WYSIWYG reporting with customizable out-of-the-box dashboards and reports. Prebuilt templates allow administrators to query underlying Elasticsearch clusters quickly and intuitively for a vast range of asset and vulnerability attributes. Assets can be grouped by business units for granular visibility by each business owner. Some useful reports for continuous trend analysis and program benchmarking include :

- + Remediation of high risk-score vulnerabilities within SLA
- + Decrease in scan frequency
- + Assets with overdue scan status
- + Increase in high-risk vulnerability occurrences or exposed vulnerabilities

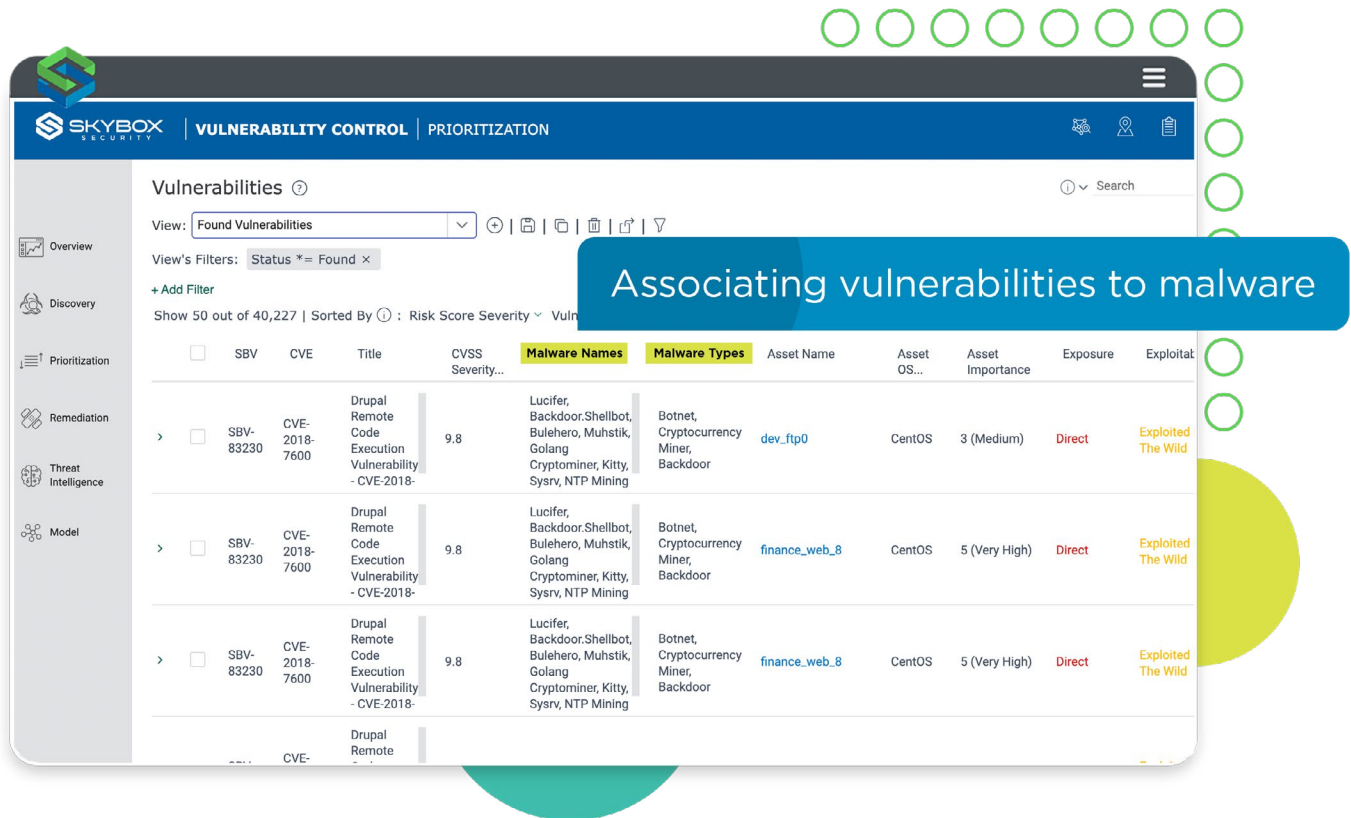
Malware and vulnerability correlation

Advanced Persistent Threats (APTs) and polymorphic threats continue to proliferate. Yet, Vulnerability Management and Threat Hunting teams often work in silos, lacking a common platform or integrated, coordinated remediation workflows. Threat hunting teams engage in time-consuming searches to prosecute Indicators of Compromise and Indicators of Attack, which by their very nature, are reactive activities (as malware has already infiltrated the enterprise). Skybox explicitly associates vulnerabilities to malware by name and family, becoming the only player in the Vulnerability Market

that can solve this problem in this manner. The common types of malware families that Skybox associates with vulnerabilities are:



Searching for a specific malware and understanding the associated vulnerability occurrences is possible in the Skybox platform.



Associating vulnerabilities to malware

SBV	CVE	Title	CVSS Severity...	Malware Names	Malware Types	Asset Name	Asset OS...	Asset Importance	Exposure	Exploited
SBV-83230	CVE-2018-7600	Drupal Remote Code Execution Vulnerability - CVE-2018-	9.8	Lucifer, Backdoor.Shellbot, Bulehero, Muhstik, Golang Cryptominer, Kitty, Sysrv, NTP Mining	Botnet, Cryptocurrency Miner, Backdoor	dev_ftp0	CentOS	3 (Medium)	Direct	Exploited The Wild
SBV-83230	CVE-2018-7600	Drupal Remote Code Execution Vulnerability - CVE-2018-	9.8	Lucifer, Backdoor.Shellbot, Bulehero, Muhstik, Golang Cryptominer, Kitty, Sysrv, NTP Mining	Botnet, Cryptocurrency Miner, Backdoor	finance_web_8	CentOS	5 (Very High)	Direct	Exploited The Wild
SBV-83230	CVE-2018-7600	Drupal Remote Code Execution Vulnerability - CVE-2018-	9.8	Lucifer, Backdoor.Shellbot, Bulehero, Muhstik, Golang Cryptominer, Kitty, Sysrv, NTP Mining	Botnet, Cryptocurrency Miner, Backdoor	finance_web_8	CentOS	5 (Very High)	Direct	Exploited The Wild

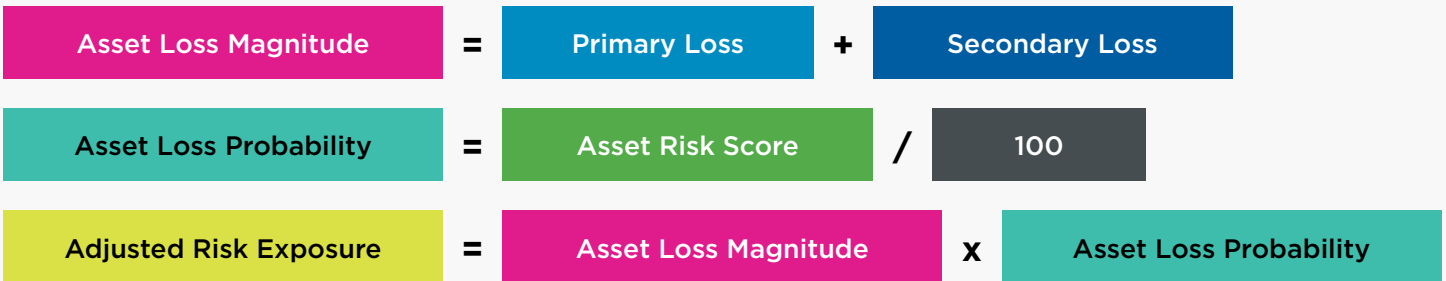
Vulnerabilities associated with the malware "Lucifer"

Cyber risk quantification (CRQ)

CRQ expresses cyber security and operational risk in quantitative terms based on Value-at-Risk (VaR) models that incorporate the financial impact of potential asset loss and statistical probabilities of loss events. It creates an objective framework for risk-based decision-making, while driving increased relevance with board and C-suite stakeholders. CRQ allows cyber security professionals to adopt the same vernacular as senior decision-makers and helps provide objective answers to questions like:

- + Should a specific risk be accepted?
- + Or mitigated with technology or process controls?
- + Or protected with cyber insurance?

Skybox CRQ formulas



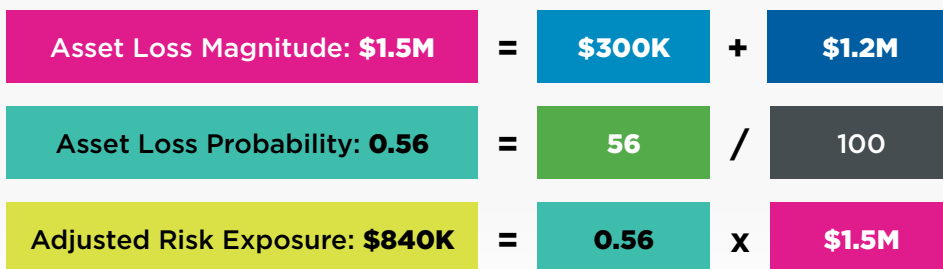
Primary Loss refers to losses incurred from the loss event itself, the results of the threat actor successfully impacting the asset, such as costs of incident response or server replacement - the cost of direct losses, i.e., interruption of operations, salaries paid to employees while operations are interrupted, cost of mobilizing service providers to mitigate the attack.

Secondary Loss refers to losses incurred from the reactions of outside parties to the loss event. Examples include negative brand impact and market share loss caused by a corporate data breach.

Asset Risk Score is derived from Skybox Risk Scoring Algorithm. So, in an illustrative example, if:



then:



Unit	Assets			Vulnerabilities
APAC	126 ASSETS COUNT	31,500,000 MAX EXPOSURE (\$)	2,067,500 ADJUSTED EXPOSURE (\$)	6,521 VULNERABILITIES
EMEA	38 ASSETS COUNT	19,000,000 MAX EXPOSURE (\$)	6,170,000 ADJUSTED EXPOSURE (\$)	25,477 VULNERABILITIES
US	473 ASSETS COUNT	68,250,222 MAX EXPOSURE (\$)	8,344,296 ADJUSTED EXPOSURE (\$)	28,092 VULNERABILITIES
Production	29 ASSETS COUNT	72,500,000 MAX EXPOSURE (\$)	17,425,002 ADJUSTED EXPOSURE (\$)	7,253 VULNERABILITIES

Cross-BU comparison of cyber risk

Organizations should approach Cyber Risk Quantification as a journey that matures with advancements in security posture.



Cyber Risk Quantification as a journey

Skybox solution benefits

- Complete attack surface visibility across IT, OT, and multi-cloud environments
- Customizable, multi-factor risk scoring algorithm for accurately pinpointing the riskiest vulnerabilities
- Detailed network-based exposure analysis reduces false positives
- Ability to detect vulnerabilities linked to specific malware variants, thus optimizing MTTD/MTTR
- Protection of non-scannable assets and ability to address active scanning blind spots
- Ability to quantify cyber risk in monetary terms for objective decision-making and board-level relevance
- Increased cyber resilience through the identification of control gaps like dated OS and applications
- Network-based controls for vulnerability risk mitigation relieving pressure on VM teams

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 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.