SKYBOX SECURITY

Solution Brief

Vulnerability discovery

Skybox Vulnerability and Threat Management

Overview

Effective vulnerability and threat management starts with the ability to discover vulnerabilities in your network anywhere, anytime. Traditional scanning is performed at intervals of days, weeks and even months, leaving gaps in understanding the company's vulnerability status in-between scans. Certain parts of the live network may also be off-limits to scanners, creating blind spots during vulnerability assessments.

Skybox takes a comprehensive approach

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. Skybox uniquely combines traditional scanner data with passive vulnerability assessment technology to reach "unscannable" network devices and systems. Passive vulnerability assessment can be performed on-demand so you have visibility into vulnerability status within minutes.

Summary

Solution
Skybox Vulnerability and Threat Management

Capability
Vulnerability discovery

Technical challenges
+ Gaps in understanding vulnerability status in between scans
+ Blind spots where scanners can't reach
+ A trade-off of either having infrequent scans with high coverage or frequent scans with poor coverage
+ Incomplete data from a "scan only" approach that leads to ineffective prioritization and limited remediation

Technical benefits
+ Discover vulnerabilities on demand, including in unscannable network zones and devices
+ Identify vulnerabilities in hybrid and multi-cloud networks, including containers
+ Merge and normalize vulnerability data from multiple discovery methods and hybrid environments such as corporate networks, cloud and OT networks
+ Ensure analysis and remediation priorities are based on accurate and comprehensive discovery data

Consolidate and centralize data for thorough analysis

Skybox integrates with all the leading IT vulnerability scanning vendors as well as operational technology (OT) security vendors. Skybox collects and merge data from these vendors into a central repository, enabling a complete and thorough analysis. This repository includes:

+ Results from multiple vulnerability scanners interrogating on-prem assets, as well as scanners interrogating cloud assets approved by the cloud service provider (CSP)
+ Results from app and web scanners
+ Data from OT security platforms that passively assess OT networks
+ Asset configuration weaknesses
+ Custom vulnerabilities

Fill in the scanner blind spots to get a complete picture

Skybox fills in blind spots of unscannable network devices and zones through our unique passive assessment. We utilize data collected from integrations with asset repositories and network information sources and compare the information to our intelligence feed to deduce vulnerability occurrences in your network. Skybox also uses collected environment data to identify "rogue," unscanned assets.

The intelligence is supplied by the Skybox research lab; a team of security analysts who scour data daily from dozens of security feeds and sources and investigate sites on the dark web. The research lab validates and enhances data through analysis, based on their knowledge of attack trends, cyber events, and the TTP of today's attackers. Their ongoing investigations determine which vulnerabilities are being exploited in the wild and used in distributed crimeware, such as ransomware, malware, exploit kits, and other attacks exploiting client and server-side vulnerabilities.

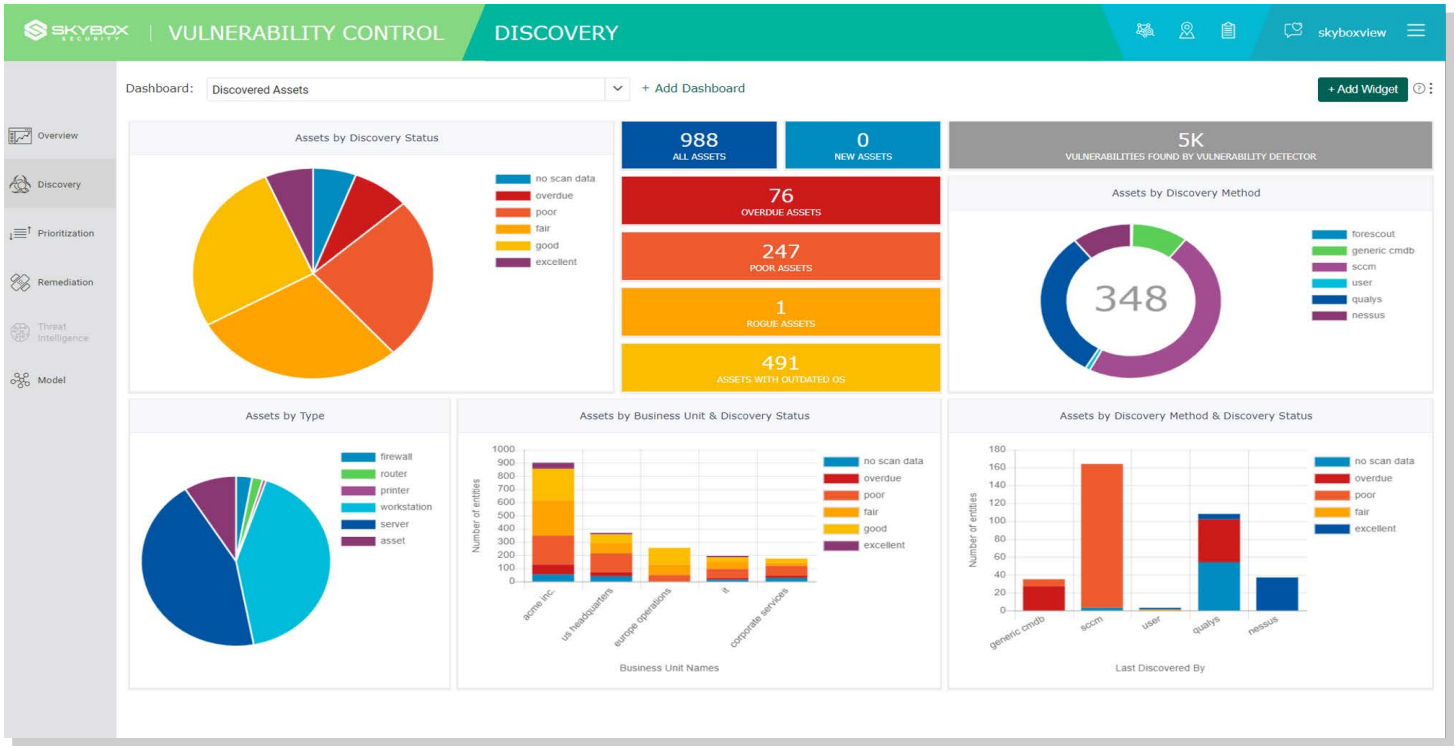
How Skybox conducts passive vulnerability assessments

+ Product configuration information is automatically collected, merged and normalized to create a complete picture of systems and products installed on the network. Skybox pulls data from asset and patch management software as well as configuration data from networking devices (Cisco, Juniper, Check Point, HP and others).
+ The collected, normalized data — known as the "product catalog" — is converted into accurate vulnerability data. Skybox uses a proprietary library of tens of thousands of logical rules within the daily Skybox intelligence feed to test the product catalog and determine if a set of pre-conditions are met for the existence of a vulnerability.
+ The intelligence feed takes multiple factors into account to deduce if a vulnerability truly exists in the environment. For example, a particular vulnerability may exist on a certain product, version and patch level of an application, but only when running in a particular operating system environment and in the presence or absence of other products or factors.
+ This results in a comprehensive and highly accurate product catalog and list of found vulnerabilities that can be updated automatically and continuously without requiring an active scan.

Increase reliability of vulnerability and threat management process

Skybox can also run vulnerability detection on collected scan results to fill in blind spots in time between scan cycles. For example, if you run a scan on Monday and on Tuesday a new vulnerability is announced, Skybox can enhance the stale scan data with this new vulnerability without the need for another scan.

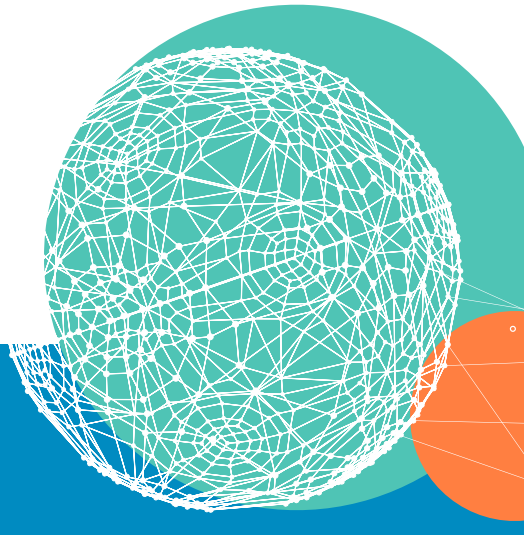
Importantly, Skybox monitors and manages your scan frequency, quickly identifying assets or groups of assets that are overdue for scanning. This visibility into scan frequency helps to increase reliability of the vulnerability management process, zeroing in on unscannable assets. Skybox provides remediation suggestions to protect systems that cannot be scanned due to being older, legacy systems, mission-critical systems or those with limited downtime.



Learn more

Schedule a **demo >**

Read about Skybox Vulnerability and Threat Management **solution >**



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.

skyboxsecurity.com

SKYBOX SECURITY