COMPREHENSIVE VULNERABILITY DISCOVERY

WITH SKYBOX SECURITY

Solution Brief

Effective vulnerability management starts with the ability to discover vulnerabilities in your network anywhere, anytime.

Traditional scanning is performed at intervals from days to weeks to months, leaving vulnerability status in the time between scans a mystery. Certain parts of the live network may also be off–limits to scanners, creating blind spots during vulnerability assessments.

Skybox takes a different approach, combining traditional scanner data with scanless vulnerability assessment technology to reach “unscannable” network devices and systems. Scanless vulnerability assessment can also be performed on demand so vulnerability status can be known at all times and in minutes.

Consolidating Third–Party Discovery Data

Skybox integrates with all of the major IT vulnerability scanning vendors as well as operational technology (OT) security vendors to collect and merge their information in a central repository. This repository includes:

- Results from 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

SKYBOX® SECURITY

Total visibility.
Focused Protection.™

BENEFITS OF SKYBOX APPROACH TO VULNERABILITY DISCOVERY

Discover vulnerabilities on demand, including in unscannable network zones and devices

Identify vulnerabilities in rapidly changing cloud and virtual networks, including container vulnerabilities

Unify vulnerability data from multiple discovery methods and hybrid environments — on–prem, cloud and OT networks

Ensure analysis and remediation priorities are based on accurate and comprehensive discovery data

Scanless Vulnerability Assessments

Skybox also fills in blind spots of unscannable network devices and zones through our unique scanless assessment. It utilizes data collected from our integrations with asset repositories and network information sources, comparing the information to our analyst-backed intelligence feed to deduce vulnerability occurrences in your network. Skybox is also able to use collected environment data to **identify "rogue," unscanned assets**.

How it Works

To conduct scanless vulnerability assessments, Skybox first performs product profiling. Product configuration information is automatically collected, merged and normalized into a comprehensive list of the systems and products installed in a network environment. For example, Skybox pulls data from asset and patch management software such as Microsoft's System Center Configuration Manager, Symantec Altiris, Red Hat Satellite and McAfee ePO, as well as configuration data from networking devices (Cisco, Juniper, Check Point, HP, etc.).

Skybox then performs vulnerability profiling. The collected, normalized data — known as the "product catalog" — is converted into accurate vulnerability data. To do this, Skybox uses a proprietary library of tens of thousands of logical rules contained in the Skybox intelligence feed. The feed, updated daily, is used to test the product catalog and determine if a set of pre–conditions are met for the existence of a vulnerability.

The rules of the intelligence feed take 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 Adobe Reader, 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 — compatible with MITRE's CVE and NIST's CPE standards — that can be updated automatically and continuously without requiring an active scan. The approach greatly reduces false positives and is beneficial to day–to–day security operations as well as incident response planning.

Know All Occurences All the Time

Skybox can also run scanless 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.

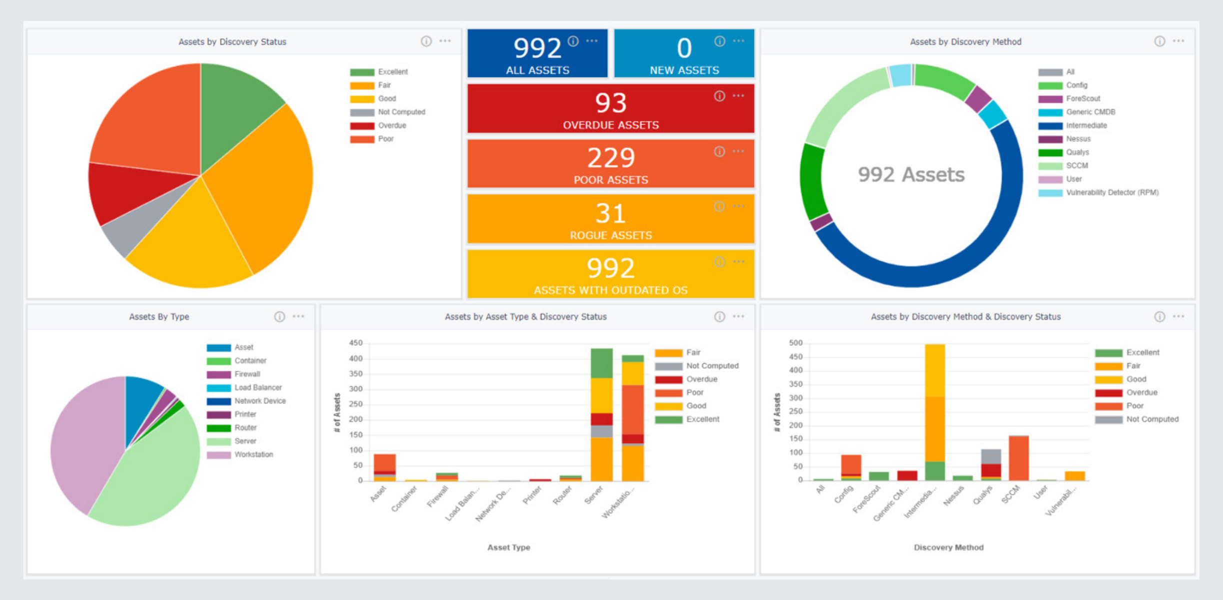

FIG 1: Dashboards, widgets, filters and other mechanisms in Skybox's discovery module enable an organization to see the the efficacy and SLAs of asset and scanning technologies — often a key compliance criteria.

To learn more about our vulnerability discovery capabilities, schedule a demo of our risk-based vulnerability management solution, Skybox® Vulnerability Control, or check out the below resources:

- Vulnerability Control Datasheet
- Skybox Research Lab Datasheet
- Skybox Intelligence Feed Tech Brief
- Risk-Based Vulnerability Management E-Book

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with over 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060