SKYBOX SECURITY

RISK-BASED VULNERABILITY MANAGEMENT

Through Exposure, Exploitability and Business Context

E-BOOK

THE PROBLEM

Many vulnerability management programs fixate on patching as many critical-severity vulnerabilities as possible. This traditional approach relies on active scans to discover vulnerabilities, looks at generic severity scores, maybe adds in some exploitability info and sets about deploying the patch (if one's available).

While vulnerability assessment and remediation are fundamental pieces of a security program, the "scan and patch" approach leaves out crucial elements of the vulnerability management workflow, especially in how remediation priorities are set. Without the proper content and context, traditional approaches do little to reduce risk over time or enable rapid response to imminent threats.

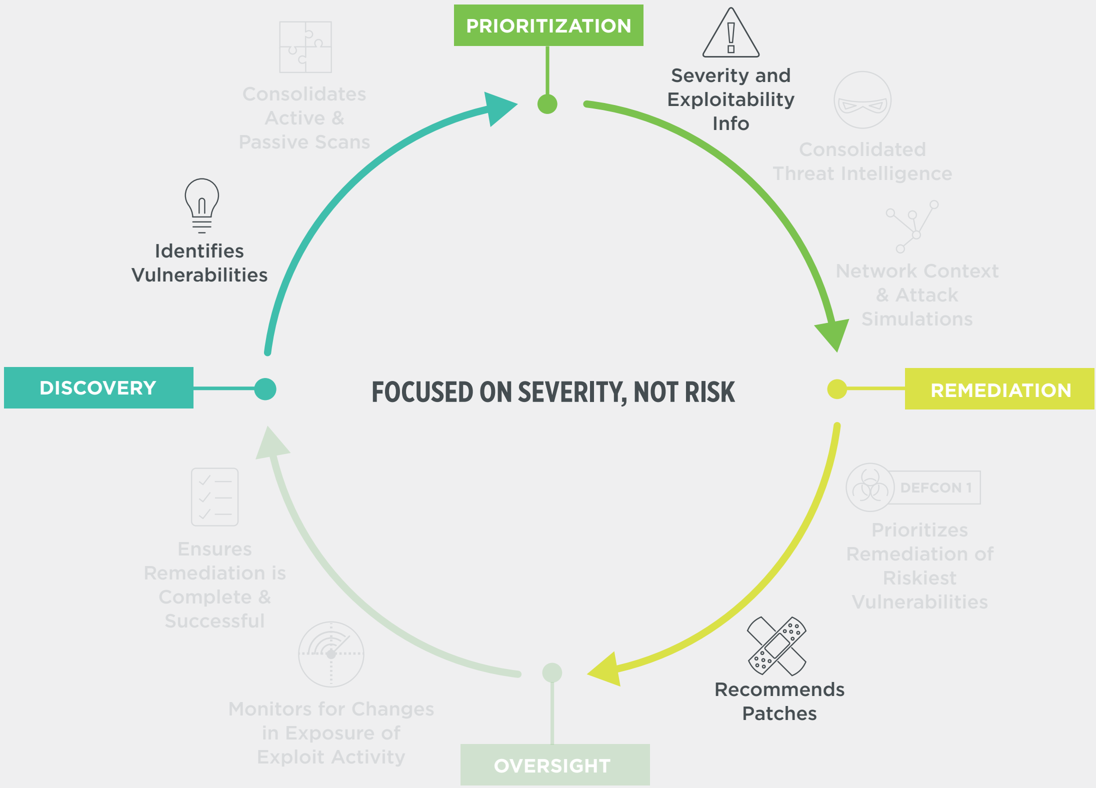
DRAWBACKS OF THE "SCAN AND PATCH" APPROACH

☒ **No exposure context:** Scanners don't understand the network topology and security controls that impact a vulnerability's exposure in your organization. As such, remediation efforts may be wasted on vulnerabilities posing little to no risk while ignoring those likely to be used in an attack

☒ **Incomplete and stale data:** Active scanners leave blind spots in vulnerability assessments from "unscannable" network devices and zones. Scanning an enterprise environment also takes time and scan data can be stale by the time it's acted upon.

☒ **Data silos:** To combat coverage gaps, many organizations use multiple scanning vendors, creating incongruous data that has to be normalized and merged.

TRADITIONAL VULNERABILITY MANAGEMENT


PRIORITIZATION
Severity and Exploitability Info
Consolidates Active & Passive Scans
Consolidated Threat Intelligence
Identifies Vulnerabilities
Network Context & Attack Simulations
DISCOVERY
FOCUSED ON SEVERITY, NOT RISK
REMEDIATION
DEFCON 1
Prioritizes Remediation of Riskiest Vulnerabilities
Ensures Remediation is Complete & Successful
Recommends Patches
Monitors for Changes in Exposure of Exploit Activity
OVERSIGHT

THE SOLUTION

Skybox® Security's risk–based vulnerability management takes a fundamentally different approach to significantly reduce the risk of attack on your organization. It uses the context of your infrastructure, business and threats to highlight the vulnerable assets most likely to be attacked. This way, you can focus on fixing your biggest risks — **exposed and exploitable vulnerabilities on critical assets.**

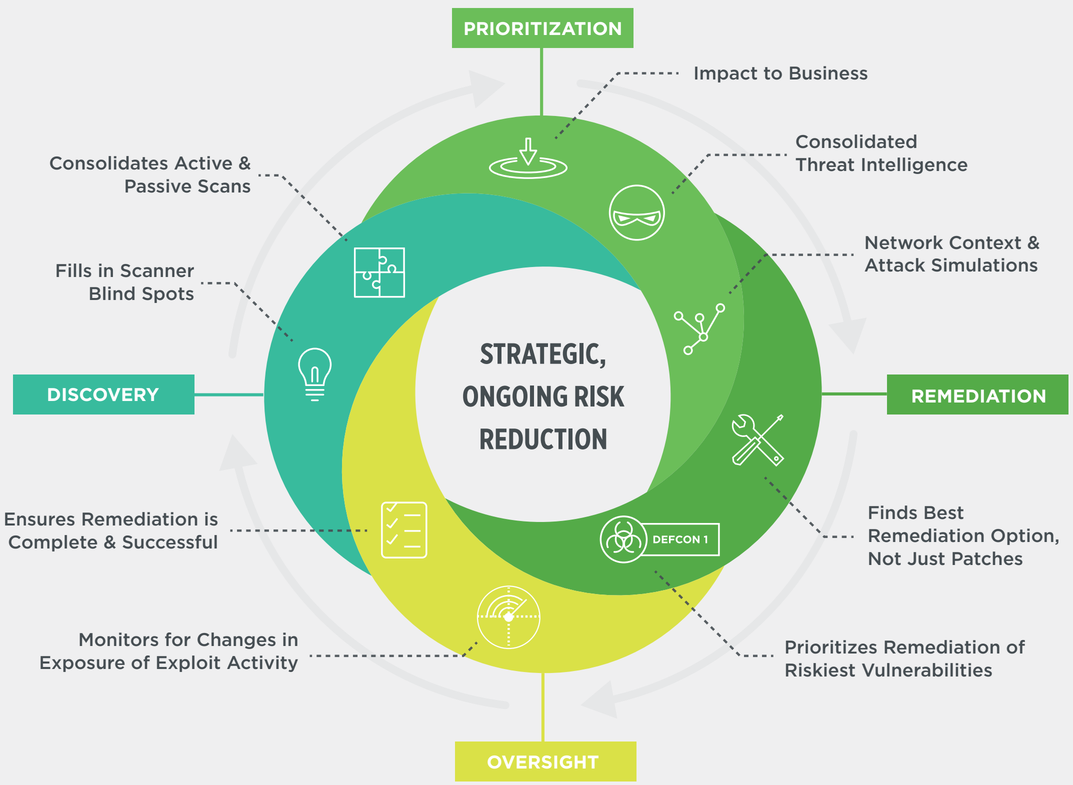
BENEFITS OF RISK–BASED VULNERABILITY MANAGEMENT

☑ **Fewer successful attacks:** Cuts the risk of successful attacks by focusing on exposed, vulnerable assets in your network with an active exploit in the wild.

☑ **Better efficiency:** Automates tasks throughout the vulnerability management workflow, reduces the need for unnecessary patching, and leverages network–based changes that may be a more efficient response option.

☑ **Increased ROI of existing investments:** Enhances data from a variety of solutions and strategically uses firewalls and IPS systems in the mitigation process.

RISK-BASED VULNERABILITY MANAGEMENT



PRIORITIZATION

Impact to Business

Consolidated Threat Intelligence

Network Context & Attack Simulations

REMEDIATION

Finds Best Remediation Option, Not Just Patches

Prioritizes Remediation of Riskiest Vulnerabilities

OVERSIGHT

Monitors for Changes in Exposure of Exploit Activity

Ensures Remediation is Complete & Successful

DISCOVERY

Fills in Scanner Blind Spots

Consolidates Active & Passive Scans

STRATEGIC, ONGOING RISK REDUCTION

SEVERITY DOESN'T EQUAL RISK

Traditional vulnerability management approaches prioritize vulnerabilities based on generic severity scores or exploit activity only; they don't consider if a vulnerable asset is shielded or exposed to attack based on the surrounding security controls and network topology.

This leaves IS teams with a laundry list of critical– and high–severity vulnerabilities and no clear plan of action. Two scenarios may ensue:

SCENARIO 1

Efforts are wasted on patching a "critical" vulnerability — in name only — that is already protected by security controls

SCENARIO 2

Prioritization ignores a "medium" vulnerability exposed in your network with an exploit proven in other attacks, leaving the asset a sitting duck

To make informed remediation choices and target risk with precision, you need to consider the complete context in which vulnerabilities exist.

More Content, Better Context

Skybox treats vulnerabilities as a piece of a larger puzzle, influenced by a variety of internal and external factors. We collect and model data from dozens of data sources — including networking and security solutions — to truly understand the risk vulnerabilities pose.

Network devices such as routers, switches, application delivery controllers and the vendor tools that manage them

Security controls such as firewalls and cloud security tags, intrusion prevention systems (IPSs) and virtual private networks (VPNs)

Public and private cloud services such as Amazon Web Services, Microsoft Azure, Cisco ACI and VMware NSX, as well as their provided management tools

OT networks common in critical infrastructure organizations and smart buildings

Asset repositories including endpoint security systems (EDRs), patch management systems, configuration management databases (CMDBs) and homegrown databases

Vulnerability occurrence data from vulnerability scanners, web and app scanners, asset configuration weaknesses and custom vulnerabilities.

Once the data is collected, similar data between like products is automatically normalized and merged. This step will yield a centralized, fresh repository for vulnerability occurrences and a merged asset record.

VULNERABILITY MANAGEMENT BUILT TO REDUCE RISK

DISCOVERY

PRIORITIZATION

REMEDIATION

OVERSIGHT

Skybox® Security takes a smarter, more innovative approach to reducing the risk of attack. It uses the full context of your attack surface to prioritize remediation in a way that makes sense for your organization.

Our approach gives you a comprehensive, accurate picture of the vulnerabilities in your environment at any time and aligns remediation urgency to risk, greatly reducing the chance of a successful attack.

Now let's take a closer look at the phases of the risk-based vulnerability management workflow and how Skybox enables and accelerates them.

Discovery

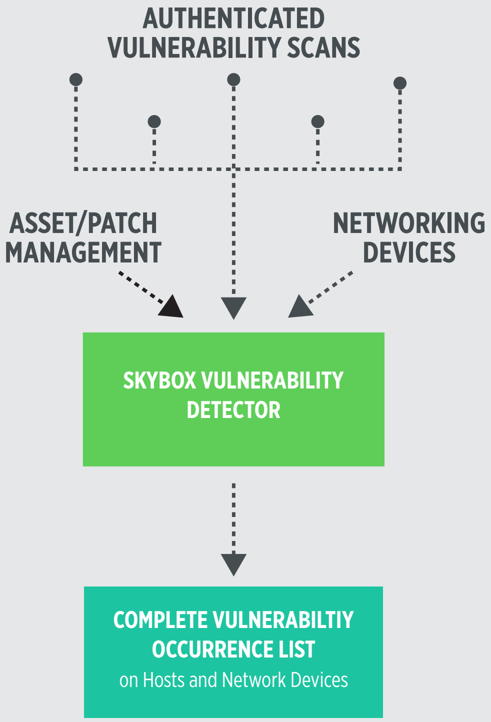
A successful vulnerability management program starts with accurate vulnerability data. Active scanning is an important component of the discovery phase, but it has its limits.

Scanner technology has been around for roughly 30 years. But today's networks — encompassing cloud and operational technology (OT) — look much different than those of the '90s.

- **Scanning in the cloud:** Cloud networks change constantly, meaning assets may be offline or changed since the last scan. In addition, many organizations use more than one cloud service provider, resulting in data silos.
- **Scanning in OT networks:** OT networks may limit active scanning, leaving them with legacy and unpatched devices out of reach of active scanners.

You need to have an alternative solution to fill in the blind spots left in dynamic cloud environments, OT networks and even the unscannable network devices and zones in your on-prem IT network.

The Skybox® Vulnerability Detector feature provides scanless vulnerability assessment that can be run on demand, assessing the entire network in a matter of minutes. Skybox correlates Vulnerability Detector results with that of all of your third-party scanners, including purpose-built OT scanners, to centralize vulnerability data and lay a strong foundation for the rest of the vulnerability management process.


AUTHENTICATED VULNERABILITY SCANS
ASSET/PATCH MANAGEMENT
NETWORKING DEVICES
SKYBOX VULNERABILITY DETECTOR
COMPLETE VULNERABILTIY OCCURRENCE LIST
on Hosts and Network Devices

Skybox Discovery Approach

- Uses data repositories such as patch and asset management systems and configuration data to infer the presence of vulnerabilities with 99 percent accuracy
- Passively detects vulnerabilities in dynamic, multi-cloud environments and OT networks
- Normalizes information and compares it to vulnerabilities in the Skybox intelligence feed
- Delivers complete and up-to-date vulnerability data in a matter of minutes
- Fills in blind spots left by active scans and consolidates data from multiple third-party scanning vendors

Combining Vulnerability, Business and Network Data

The ability to query your infrastructure to accurately assess its assets and vulnerabilities is a cornerstone of risk-based vulnerability management. It's vital to understanding the security controls in place, where critical data resides and potential attack paths.

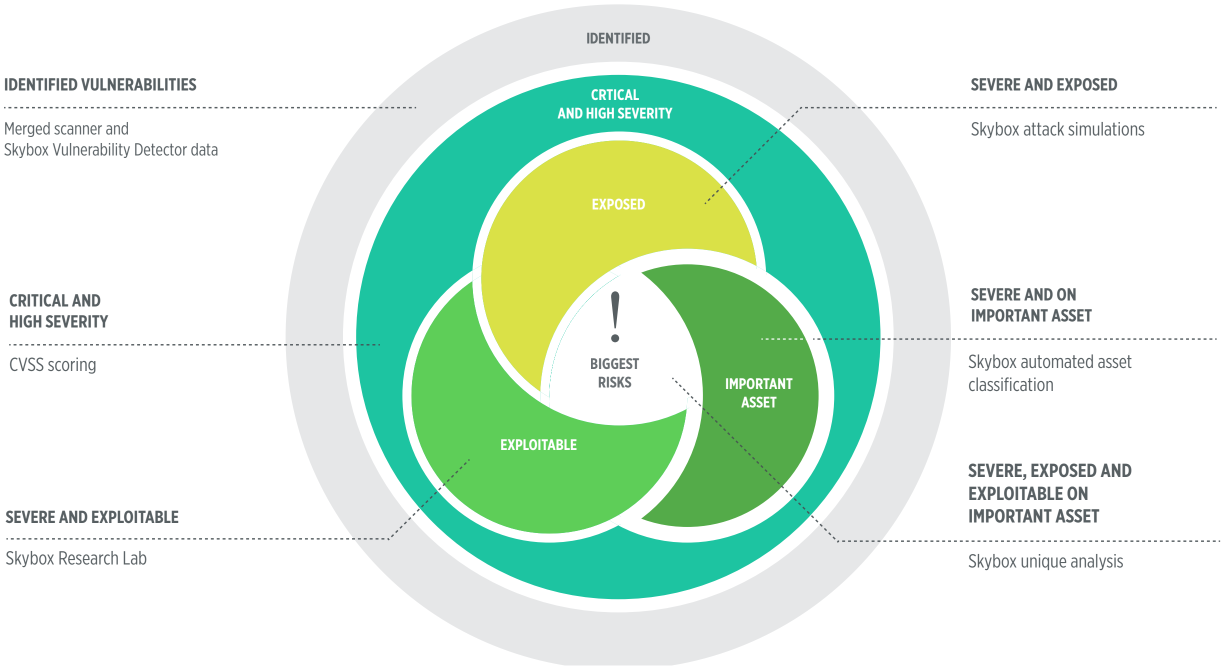
While active scans can collect a variety of information useful in vulnerability discovery, they can't ingest data from the full spectrum of factors that determine risk, remediation priorities and remediation options.

- **Incomplete, decentralized data:** Many organizations have multiple scanners and other sources for security weaknesses (e.g., endpoint detection response systems, application scanners, web scanners), but no single scanner can serve as the central repository of this information. Scanners also typically don't have the means to import and merge asset data from multiple sources.
- **No network context:** Scanners usually don't take into account the network security devices that can shield against potential exploits. Without this vital understanding of the network context, scanners may direct remediation resources to protected assets while ignoring ones that are exposed. Additionally, they can't recommend remediation outside of patches, which may not be available or not be the best option.

Skybox is uniquely vendor agnostic, importing and centralizing a variety of data sources, including data from network security devices, threat intelligence feeds and multiple asset and vulnerability sources. By combining these data sets with the results of our own scanless assessments, you can be sure discovery is accurate, covers your entire environment and provides the best content and context for the entire vulnerability management workflow.

Prioritization

THE BIGGEST DIFFERENCE between traditional approaches and risk-based vulnerability management is in the analysis that determines prioritization. Instead of focusing on vulnerability severity alone, Skybox analyzes more factors than any other solution to determine the risk a vulnerability poses.



IDENTIFIED VULNERABILITIES

Merged scanner and
Skybox Vulnerability Detector data

CRITICAL AND HIGH SEVERITY

CVSS scoring

SEVERE AND EXPLOITABLE

Skybox Research Lab

SEVERE AND EXPOSED

Skybox attack simulations

SEVERE AND ON IMPORTANT ASSET

Skybox automated asset classification

SEVERE, EXPOSED AND EXPLOITABLE ON IMPORTANT ASSET

Skybox unique analysis

GARTNER'S 10 FACTORS FOR UNDERSTANDING VULNERABILITY RISK

1 VULNERABILITY SEVERITY

2 COMPLIANCE

3 AGE

4 LOCATION

5 EXPLOITABILITY

6 PREVALENCE (DENSITY)

7 ASSET ROLE

8 ASSET VALUE

9 THREATS

10 NETWORK TOPOLOGY

Without proper asset management and network context, it becomes impossible to consider all these factors.

Source: "A Guidance Framework for Developing and Implementing Vulnerability Management," Gartner, June 22, 2017. https://www.gartner.com/en/documents/3747620

SECURITY ANALYST–VALIDATED THREAT INTELLIGENCE

Skybox researchers scour dozens of security data sources every day and investigate sites in the dark web, putting analyst–validated, current threat intelligence at your fingertips. They also provide information regarding exploitability levels, add exploitation preconditions and effects, and configure attack patterns to be used in Skybox's patented attack simulations. Such intelligence is used not just in vulnerability management process, but throughout the Skybox® Security Suite.

Learn more abou the Skybox Research Lab >

1. Vulnerability Presence

The Skybox prioritization approach starts with information about your organization's current vulnerabilities learned in the discovery phase.

2. Vulnerability Intelligence

Skybox uses vulnerability intelligence to better understand the implications of your current vulnerabilities. This 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.
- 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
- History of changes in the vulnerability as it relates to severity, exploitation, available patches, etc.

3. Threat Intelligence

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.

4. Network Intelligence

Next, Skybox analyzes information about your organization's assets and networks and their importance to the business to provide a contextual understanding of your attack surface. Collecting the details of your environment, Skybox builds a comprehensive model of your attack surface, including:

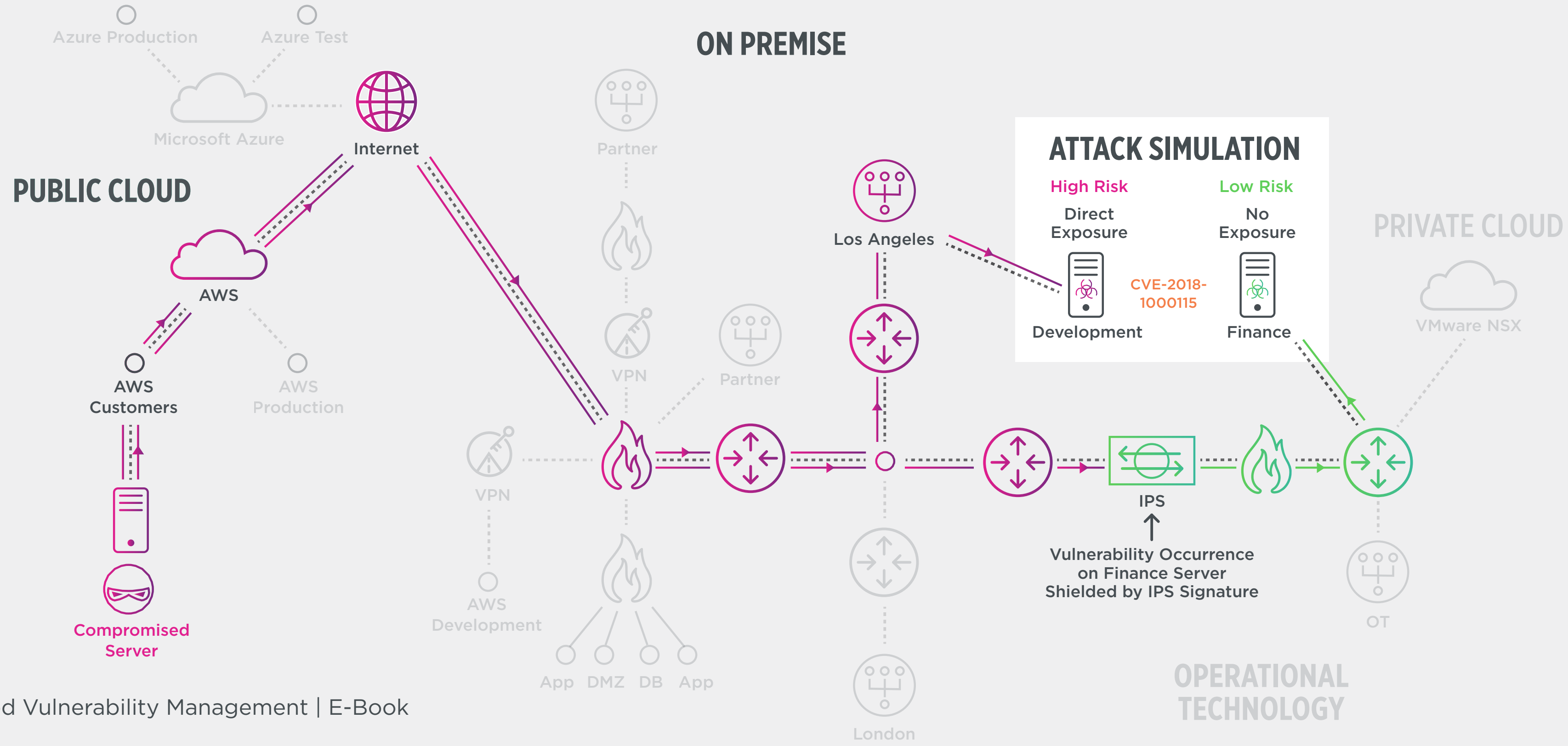
- Network topology (routers, load balancers, switches)
- Security controls (firewalls, IPSs, VPNs)
- Assets (servers, workstations, networks — including traditional IT, multi-cloud and OT environments)

The model is regularly and automatically updated to reflect the actual state of your network.

5. Exposure Analysis and Attack Simulation

The most critical step of vulnerability analysis is determining its exposure in your network. By understanding exposure, resources can be devoted to vulnerabilities accessible to threats or identify mitigation options to cut off attack paths.

Using the intelligence gathered to this point, Skybox determines the exposure of the vulnerability by simulating attacks on the network model. Automated simulations are run from all threat origins (ingress points) and assess all access scenarios 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 and Mitigation

The result of the first two steps of the workflow (discovery and prioritization) is a smaller, manageable number of vulnerabilities that should be dealt with immediately. Vulnerabilities on important assets, exposed to a threat origin and with an active exploit are top priorities.

But Skybox provides response options for all vulnerabilities and can also prioritize patches based on risk — this option is particularly helpful for operations teams who often think in terms of patches rather than the vulnerabilities they address. It can also provide insight on which patches will have the biggest impact on risk.

Choosing the Best Response

The Skybox approach recognizes that there are multiple options to deal with vulnerabilities. Some may be more expedient, cost-effective or lower risk to undertake than patching, depending on the nature of the vulnerability, your environment and exploitation conditions.

With Skybox, your team has complete visibility into the range of response options as well as the best choices to improve both day-to-day operations and incident response. These options include patches, IPS signatures, upgrades and changes to firewall rules, security tags and configurations.

PATCH–22 IN OT NETWORKS

OT networks common in critical infrastructure and manufacturing organizations avoid downtime at all cost.

While cyberattacks are a concern, so are patch deployments, as the system changes could disrupt services, cause damage, endanger employees or void equipment warranties.

The Skybox risk-based solution provides remediation guidance that prioritizes patches for vulnerable exposed and exploitable assets in the OT network.

This approach helps IT security inform OT engineers of their greatest cyber risks while coordinating important fixes to occur during planned downtime.

IPS SIGNATURES

Rely on existing security controls such as IPS signatures or endpoint protection suites to stop attacks.

FIREWALLS RULES & SECURITY TAGS

Change firewall rulesets or cloud security tags to prevent attackers from reaching a vulnerable asset.

CONFIGURATION CHANGES

Reconfigure vulnerable software using built-in security measures to prevent exploitation.

UPGRADES

Upgrade from an older version of the software to eliminate the vulnerability.

PATCHES

Use the Intelligence Feed to learn about available fixes and prioritize patching based on risk reduction impact.

Oversight

With so many assets and vulnerabilities, it’s easy for something in your environment to be overlooked. With Skybox, you can significantly reduce risk through centralized oversight that includes:

TRACKING

Risk scores provide a straightforward and objective way to track risk levels over time and ensure risk reduction efforts are having the desired impact

MONITORING

Checks for changes in network exposure and exploit activity, escalating vulnerabilities to imminent threats when necessary

REPORTING

Fully customizable dashboards are turned into reports with the click of a button, and can be exported as .csv, .pdf or .html

Oversight is also about accountability, ensuring remediation plans are carried out effectively and accurately. To understand if a vulnerability is truly eliminated from your network, the oversight phase should include discovery processes, beginning the entire vulnerability management process again for any unaddressed occurrences.

BUSINESS BENEFITS

Only Skybox brings together the technologies that make risk-based vulnerability management possible, including automation of data gathering and normalization, vulnerability prioritization based on attack surface context, remediation guidance and oversight.

SIMPLIFY VULNERABILITY MANAGEMENT

managing the entire vulnerability life cycle from a centralized solution, whether they exist on-prem, in the cloud or in OT networks

SAVE TIME AND RESOURCES

through operational efficiencies via automation, and through the reduced risk of data breaches which disrupt business revenue and damage reputation

FOCUS ACTION

on the small subset of vulnerabilities most likely to be used in an attack — those on critical exposed assets in your network with proven exploits

RESPOND FASTER AND SMARTER

to threats with on-demand intelligence of vulnerability and asset details, exploit activity, potential business impact and best response options

GAIN VISIBILITY AND INSIGHT

of your network — across traditional IT, multi-cloud and OT environments — and its most critical risks

THE SKYBOX SOLUTION

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 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.

All modules of the Skybox Security Suite work together and share information to ensure all recommended actions are consistent with compliance requirements and take into account the context of your organization's risk posture.

The automation embedded in the Suite helps your organization:

Automate collection from enterprise network and asset repositories to ensure a strong foundation for your security program

Centrally manage security data from hybrid network environments, their security controls, assets and vulnerabilities

Visualize your attack surface with an always up-to-date network map and an offline model to analyze and troubleshoot issues

Proactively identify issues most likely to be exploited in an attack and continuously monitor for policy violations

Prioritize vulnerabilities and security weaknesses in context to target action where it's needed most

Intelligently plan response to systematically reduce your organization's risk of cyberattack and meet compliance requirements

For more information on the Skybox Security Suite and Skybox's analytics-driven automation, please visit skyboxsecurity.com or schedule a demo today.

SKYBOX® SECURITY