SKYBOX SECURITY

e-book

TRANSFORMING VULNERABILITY MANAGEMENT

Increase efficacy of prioritization and remediation with exposure analysis

Contents

THE ATTACK SURFACE

Do we know what we are dealing with?

Digital innovation and transformation move forward at the speed of light, challenging security teams to balance the needs of their business with an imperative to prevent cyber attacks. There is no question that advanced technologies help businesses across every industry expand into new markets and increase profits. However, they also introduce new vulnerabilities and threat exposures with expansions into the cloud, deployment of newly connected things and systems, increased mobile and distributed users, and a massive transformation of business processes.

Cyber threat actors are taking advantage of the resulting expansion across most organizations' attack surface with new threat vectors opening across their networks, as highlighted in the Verizon 2021 Breach Investigation Report:[1]

+ The median random organization now has 17 external internet-facing assets – each of these being a potential target of a cyber attack
+ External cloud assets were more common in 2020 than on-premise assets
+ **There were 10 times as many "unknowns"** as there were cloud assets – "unknown" meaning incidents where the information on the location of the assets was not available.

Identifying and fixing vulnerabilities and misconfigurations exposing businesses to cyber attacks is critical, but legacy vulnerability management tools are no longer effective. Despite continued reliance on these tools by enterprises, malware attacks and data breaches continue to accelerate, taking advantage of vulnerabilities across networks. For example:

+ New ransomware samples increased by 106% in 2020 and total ransomware payments reached a total of $312M[2]
+ In 2020, exploits of network devices with vulnerabilities increased significantly: a **1,916% increase** in attacks against Fortinet SSL-VPN devices and a **1,527% increase** in attacks against Pulse Connect Secure VPN.[3]

Significant increase in **exploits of network VPNs** in 2020

1,916%

increase in attacks vs. Fortinet SSL-VPNs[3]

[1] Verizon Data Breach Investigation Report, 2021
[2] Palo Alto Networks Unit 42 Ransomware Threat Report, 2021
[3] Nuspire Q1 2021 Threat Landscape Report

The link between routinely exploited vulnerabilities and network exposures

More than **18,000 new vulnerabilities** were discovered in 2020.[5] Still, according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), nine of the top 10 routinely exploited vulnerabilities from 2016 to 2019 were **at least one-year old**,[6] with one dating as far back as 2012. Enterprises are remediating vulnerabilities across their networks, but still missing a significant amount of continuously exploited vulnerabilities because they are not addressing network exposures.

Meanwile, the costs associated with cyber attacks continues to increase – now averaging $3.86M from a single data breach with an average loss of revenue totaling $1.52M.[7]

Enterprises spent
$123B
on cybersecurity in 2020[4]

Legacy vulnerability management programs fail to reduce attacks

+ **Incomplete data sets are used in vulnerability analysis.** With an over-reliance on scanning, businesses get an incomplete picture of their vulnerability exposure. Many devices are offline when scans run. Scanning is typically not frequent enough. There are too many devices and hybrid network infrastructure elements, including routers, switches, load balancers, VPNs, and more.
+ **Exposure risk is not factored into prioritization analysis.** Common vulnerability prioritization approaches fall short of finding the vulnerabilities most likely to be exploited because they are not factoring in a multi-dimensional analysis of the network. Enterprises using these legacy tools lack complete visibility and understanding of the configurations and controls across their networks, as well as the attack surface they are striving to reduce. Medium-and-low vulnerabilities often expose an organization to an attack, and legacy prioritization tools are entirely missing these vulnerabilities.
+ **Viable remediation solutions are not being utilized.** Patching an asset or groups of assets may not always be possible. Alternative ways to prevent vulnerability exploits include:
    - o reconfiguring security controls
    - o applying IPS signatures
    - o altering network topologies
    - o and determining the use of potential zero trust strategies or isolation technologies.

Legacy approaches with vulnerability analysis and prioritization primarily focus on patching and do not provide remediation recommendations that yield actual risk reduction.

Ineffective vulnerability management typically results in poorly utilized resources that expend energy and time on volumetric patch management and, yet fails to reduce exposure to risk. It also leads to significant investments in additional security controls to stop attacks while vulnerability exposures being exploited remain unchecked. Enterprises spent **$123B on cybersecurity** in 2020,[4] but the main result is continued increases in cybersecurity attacks and breaches.

[4] Gartner 1Q 2021 Update: Forecast: Information Security and Risk Management, Worldwide, 2018-2024
[5] Skybox Vulnerability and Threat Trends Report, 2021
[6] U.S. Cybersecurity and Infrastructure Agency (CISA), May 2020
[7] IBM Cost of a Data Breach Report, 2020

DISCOVERY

Are we collecting and analyzing the right sets of data?

Discovery beyond the scan

Security teams relying solely on scan data to uncover vulnerabilities are often unable to catch those that expose their networks to a cyber attack. Here's why:

+ The frequency in which large enterprises run scans across their networks varies, but it's typically monthly or quarterly. This leads to obvious gaps in coverage considering new vulnerabilities are discovered every two hours based on the rate of discovery in 2020. Additionally, scanning does not account for assets that are disconnected during the time of scan – a growing issue since remote workers have inconsistent connectivity across different locations.
+ Many dark or shadow assets will not appear in scan reports since scanners require both an IP address and credentials. Data aggregated from CMDB databases and other asset management tools can help uncover rogue devices and their vulnerabilities.
+ Connected non-IT physical systems (OT/ICS, IoT, IIoT) are often unavailable to scan tools. A vulnerability management program that includes passive discovery techniques can supplement scan data and bubble high-risk and exposed vulnerabilities to the top of the remediation queue.

Enterprise-wide discovery means fewer silos and quicker resolution

Corporate security teams need to adopt new processes as they shift focus from being IT-centric to securing assets in the cloud and on disparate OT networks. Aggregating data from different domains with multiple security consoles slows vulnerability discovery and introduces manual effort and staff burnout. Cross-functional teams need to collaborate with a single tool that can precisely consolidate and normalize data from multiple sources and produce a single view of vulnerable and exposed assets wherever they are located across the organization's networks.

Threat intelligence – the key ingredient

Mature vulnerability management tools incorporate accurate and up-to-the-minute threat and intelligence feeds to supplement the data collection and discovery process. A recent Ponemon survey showed that 79% of respondents say threat data feeds are essential to achieving a strong cybersecurity posture.[8]

Enterprises need to incorporate up-to-date threat and exploit intelligence into their prioritization analysis to ensure accurate and pointed risk scores are calculated. This enables their teams to develop more effective remediation strategies that target exposure risk.

[8] Ponemon Survey, The State of Threat Feed Effectiveness in the United States and United Kingdom, March 2021

PRIORITIZATION

Are we factoring exposure risk in our analysis?

"82,000

Exchange servers remained un-patched...[11]

[9] Palo Alto Networks, The State of Exploit Development, August 2020
[10] ZDNet Blog, Everything you need to know about the Microsoft Exchange Server hack, April 2021
[11] Palo Alto Networks: Remediation Steps for the Microsoft Exchange Server Vulnerabilities, March 2021
[12] Edgescan 2020 Vulnerability Statistics Report
[13] Skybox Vulnerability and Threat Trends Report, 2021

The race to exploitation

In 2020, threat actors raced to exploit the 18,341 newly discovered vulnerabilities before defenders could respond. A recent report published by Palo Alto Networks highlights that 80% of exploits were made public before vendors published the related CVEs. As noted in the report, "there is a good chance that an exploit is already available when the CVE is officially published – illustrating one more way that attackers are too often a step ahead of security professionals."[9] The speed at which threat actors develop exploits means security teams need greater precision with patch management and as many viable remediation techniques as possible. Many vulnerabilities remain unpatched long enough to be exploited; quickly determining where these are located and exposed is imperative.

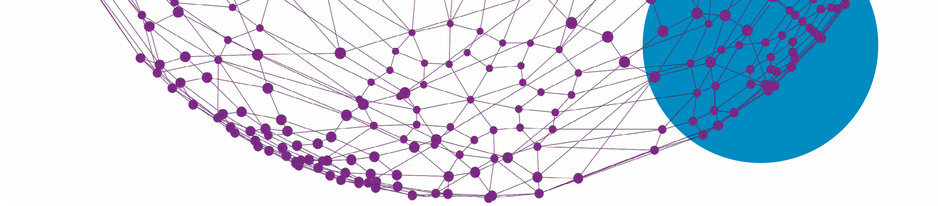
For example, the vulnerabilities detected in Microsoft Exchange servers. A researcher reported the findings on January 5, 2021.[10] By January 6, network monitoring services were reporting anomalous activities on Exchange servers. Microsoft released patches to address these vulnerabilities on March 2. Palo Alto Networks weighed in with statistics from their telemetry to indicate that the estimated number of potentially compromised organizations was in the tens of thousands globally.[11] Clearly showing the challenges in immediately patching application servers like these, an estimated **82,000 Exchange servers remained un-patched on March 16.**

Traditional vulnerability prioritization isn't working

The massive, ongoing barrage of new vulnerabilities makes prioritizing them challenging and overwhelms organizations with limited resources and business constraints. More than 60% of security professionals estimate that their organization's security function spends over 3 hours per day validating false positives.[12]

False positives are often the result of relying on risk scores that are too broad in their definition. The traditional approach to prioritizing vulnerabilities involves risk scoring based on only three key factors: 1) asset importance, 2) CVSS severity, and 3) vulnerability exploitability. Although the first factor is subjective and customizable for each organization, the CVSS score and exploitability factors are publicly defined and accepted standards.

In 2020, over a third of vulnerabilities (7,000+) were considered critical.[13] Organizations expend their time and energy chasing large volumes of critical and high-risk vulnerabilities exploited in the wild and found on essential assets, all without vital knowledge of their exposure to a threat actor.



How network modeling redefines your risk score

Network modeling leverages rich sets of data collected from across your hybrid network architecture and provides full context and understanding of configurations, access, and interaction. This hybrid network context enables security teams to answer questions such as:

+ I have hundreds of thousands of vulnerabilities on my network. Which ones are exposed to a threat actor and truly causing risk to my organization?
+ If a host on network X was compromised, what other systems in the network are reachable via lateral movement in a potential multi-stage attack?
+ What kind of risk is associated with making this specific change to a firewall? What vulnerabilities will be accessible? What policies would be violated?
+ How can my SIEM understand which hosts are at the highest risk given constant changes in the network and ongoing vulnerability discovery?

Security teams can take vulnerability prioritization and remediation to another level by leveraging a network model. It enables them to precisely calculate exposure levels of various assets through hybrid networks across multiple attack paths. Risk scoring includes a combination of asset importance, CVSS score, exploitability, and advanced exposure analysis. Teams gain the granular insight needed to bypass vulnerabilities that are not an imminent threat and can devote attention and resources to fix the ones that are a threat.

Network modeling helps to redefine risk scoring by enabling a flexible and comprehensive methodology that is described below. This allows for customizable risk scoring so security teams can refine the score to satisfy unique business outcomes. Risk scores for vulnerabilities can then determine immediate triage of those with the highest risk across the enterprise. Additionally, risk scores can be segmented by asset type, allowing business units or asset owners to plan remediation by device.

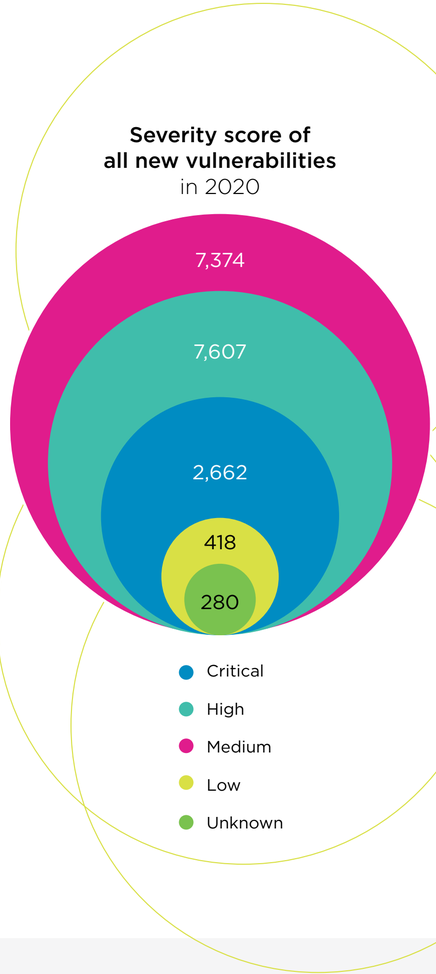
Medium-and-low severity vulnerabilities are being exploited, so risk scores need to account for ones that are exposed

Sophisticated attackers exploit the vulnerabilities that help advance multi-stage attack campaigns. They are using lower severity flaws as “door openers” to gain access into a network. Once they are in, they move laterally within the network by exploiting other vulnerabilities until they can achieve their end goal: to exfiltrate sensitive data, launch a ransomware attack, or disrupt a network from operating. Over 40% of new vulnerabilities in 2020 were classified as medium or low severity, but many are still being exploited.[14]

The most precise risk scoring yields a technical severity index of each entity across the organization (reflecting the likelihood of damage to the organization), i.e. vulnerability rating or asset vulnerability rating. To accurately assess the severity of vulnerabilities and prioritize and remediate risk, scoring methodology must include:

+ CVSS base score
+ Exploitability level – exploited in the wild, exploit available, no exploit, etc.
+ Asset importance
+ Exposure analysis – directly exposed, indirectly exposed, potentially exposed, protected and inaccessible., etc. This can only be derived by utilizing a comprehensive hybrid network model.

Exposed vulnerabilities, regardless of CVSS base score, will get a higher risk score. The scoring also should accurately pinpoint risks by asset type or by groups of assets that may be deployed across the organization’s network.



[14] Skybox Vulnerability and Threat Trends Report, 2021

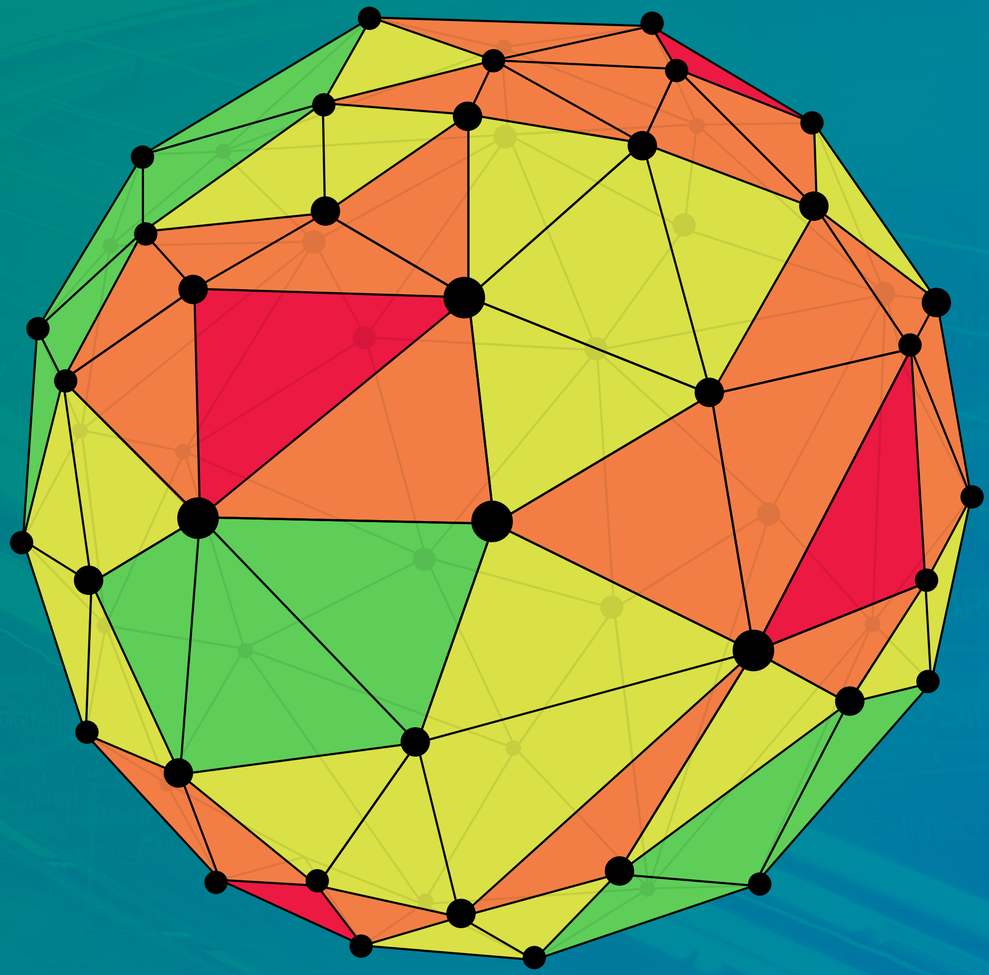
An accurate risk score requires the right formula with factored-in network context

A modern risk scoring methodology must be flexible to allow organizations to control the risk factors and weight of each factor. Risk scoring must also factor network context into the formula so organizations can determine precisely where vulnerabilities are exposed to a potential cyber attack, including those which may have low or medium CVSS scores.

Factor exposure analysis into risk scores

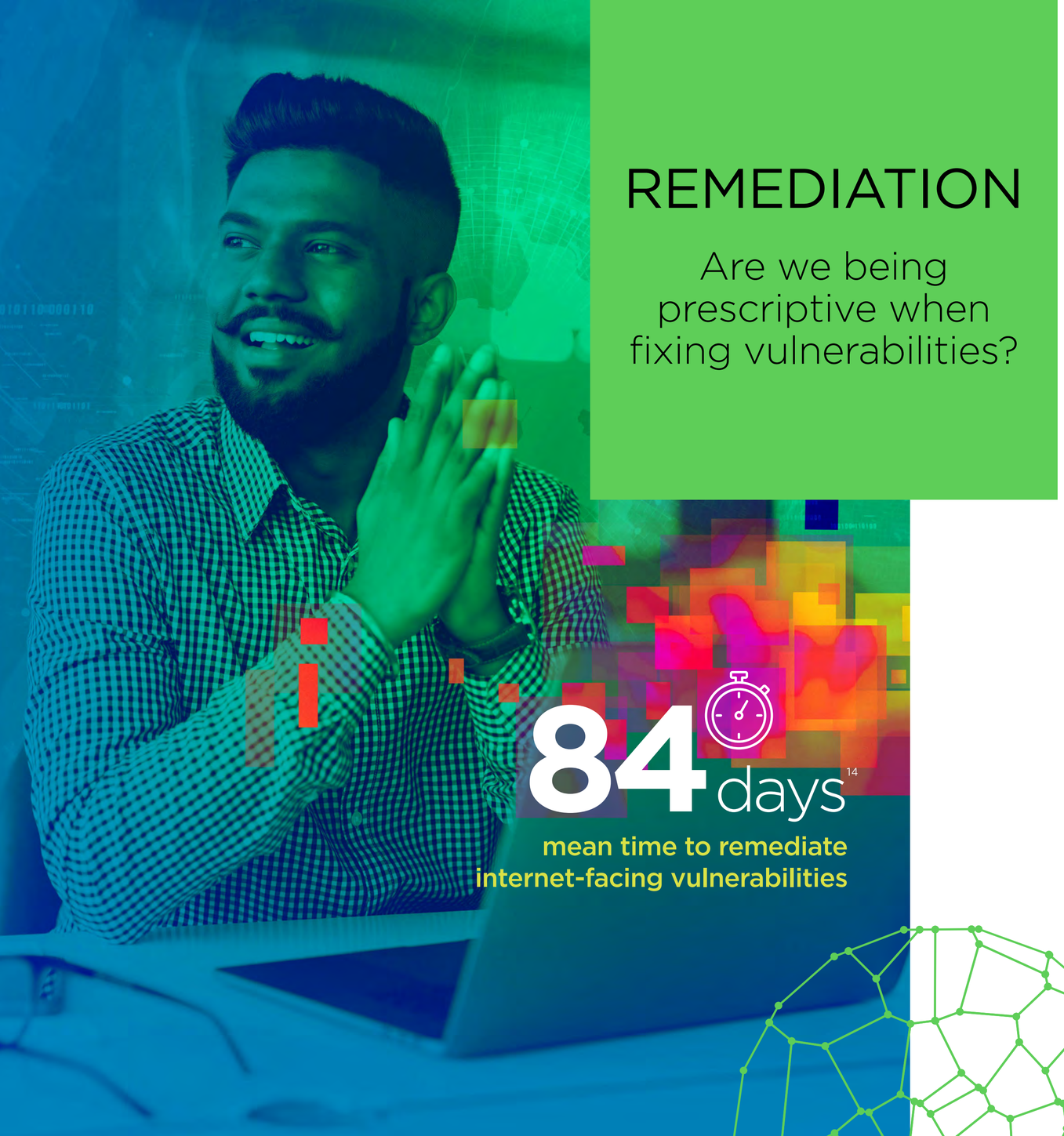
Utilizing a hybrid network model

A hybrid network model learns your network infrastructure inside-out by collecting data from various sources and aggregates and refines this information into actionable prioritization and remediation insight. Sources include:



ATTACK SURFACE

+ **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 (ISPs), 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
+ **Extensive threat and exploit intelligence**



REMEDIATION

Are we being prescriptive when fixing vulnerabilities?

Break the remediation catch-22

Just as the discovery of large volumes of vulnerabilities can overwhelm IT security teams, the process of remediating these vulnerabilities involves time-consuming internal processes of notifying asset owners, collaborating through ticketing systems, and ensuring accountability. Bottlenecks in the workflow further increase the mean time to remediate. Currently, the **mean time to remediate (MTTR) internet-facing vulnerabilities is 84 days**,[15] and traditional remediation practices reliant on patch management will likely miss fixing lower severity vulnerabilities being used in chained attacks. Alternative remediation solutions need to be assessed to determine which can best prevent opportunistic threat actors from exploiting vulnerabilities.

Remediating across a mixed IT/OT environment

In an analysis of more than 1,800 production industrial control system (ICS) networks across diverse industries, including energy utilities, manufacturing, and others, **62% of sites have unsupported Microsoft Windows systems**, such as Windows 2000 and Windows XP. These systems no longer receive regular security patches from Microsoft,[16] making them especially vulnerable to ransomware and destructive malware which can pivot from IT systems to the OT network. In these mission-critical or non-IT environments, passive vulnerability detection and non-patch remediation may be the only options.

Prescriptive remediation by solution is the new way forward

While most tools tout patching as the primary (and often, the only) remediation option, mature vulnerability programs must involve decisive effort to find and fix exposed vulnerabilities using the best means available. A solid network model is aware of firewalls, routers, and access paths, and can propose remediation suggestions such as updating IPS signatures or blocking access to a particularly high-risk and exposed vulnerability.

Prescriptive recommendations help resolve vulnerabilities on systems that cannot be patched, such as legacy systems, ICS systems, or mission-critical systems with zero downtime. Often a critical business asset that is at risk can be attacked via a multi-step approach. It is vital to understand remediation options that include patching a less critical asset upstream to effectively protect that key asset until it can be individually remediated.

[15] Edgescan 2020 Vulnerability Statistics Report
[16] Microsoft Digital Defense Report, September 2020

Prescriptive remediation solutions should be prioritized based on their overall impact to risk reduction

Solutions include:

+ **IPS signatures:** Quickly leverage existing security controls such as IPS signatures or endpoint protection suites to close exposure to potential attacks.
+ **Firewalls rules and 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.
+ **Software upgrades:** Upgrade older versions of software to eliminate vulnerabilities across multiple assets exposed to a potential exploit.
+ **Software patches:** Apply patches to assets that fix known vulnerabilities across various assets that are exposed to a potential exploit.

Prescriptive remediation automation

Prescriptive remediation solutions within vulnerability management programs help security teams to see the options that instantly 1) remediate the most vulnerabilities, 2) address vulnerabilities across the most significant number of assets, or 3) pursue a remediation strategy that provides the greatest risk score reduction. By stack ranking the activities that are the most expedient, cost-effective, or more efficient than patching, teams can reduce exposure windows and address risk based on the nature of the vulnerability, the corporate network environment, and exploitation conditions.

With prescriptive remediation capabilities, security teams have complete visibility into the range of response options as well as the best choices to improve both day-to-day operations and incident response.

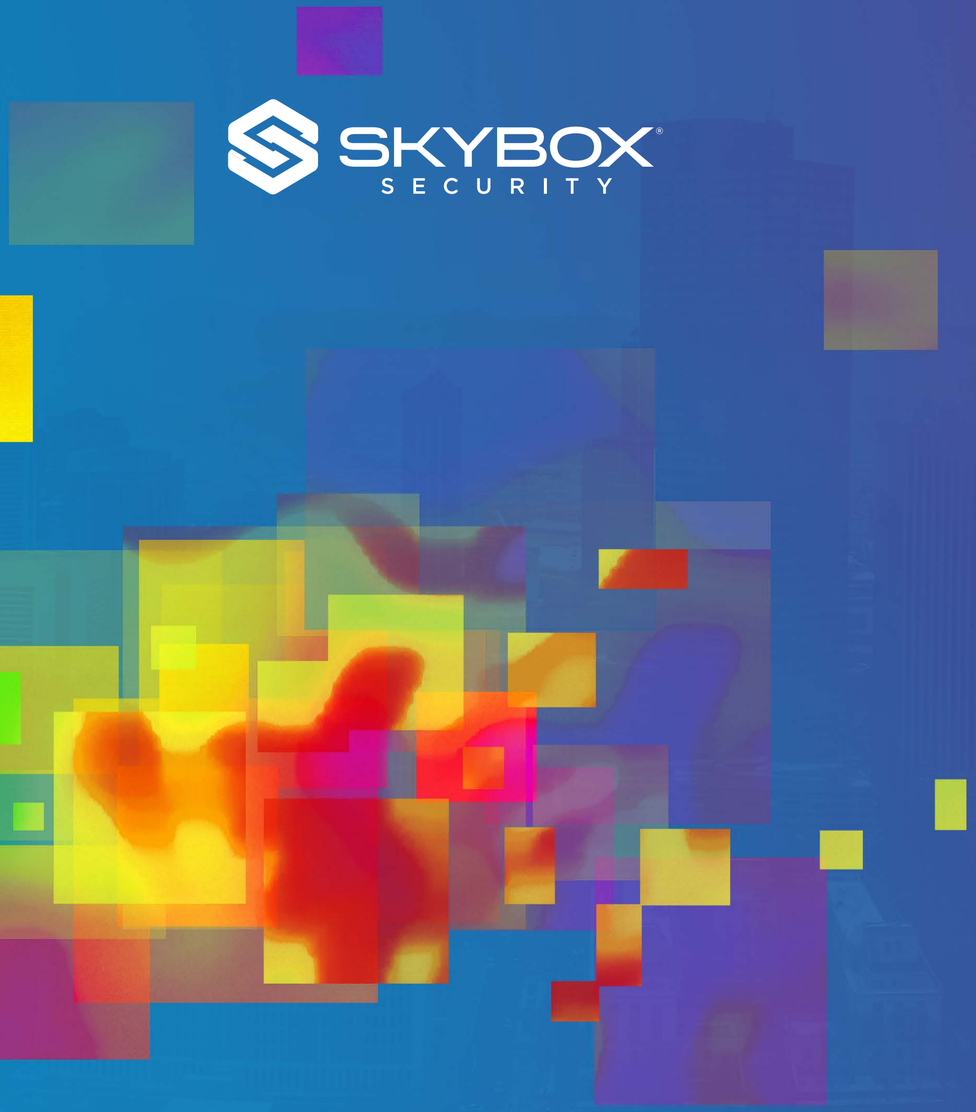
Remediation scenarios

Proactive:

Your teams can develop proactive strategies for preventing cyber attacks by having more granular prioritization powered by exposure analysis and prescriptive remediation. This empowers cross-functional teams to execute remediation playbooks with clear action plans assigned to appropriate asset owners or patch management teams.

Reactive:

As new vulnerability advisories become known, you can immediately analyze the impacts to your business by having a network model that can understand which assets are affected, where those assets are located, and the best course of action required to ensure exploits are prevented.



The Skybox Solution

The Skybox Vulnerability and Threat Management (VTM) solution provides a centralized, automated, and vendor-agnostic approach for enabling full-lifecycle vulnerability management across the entire attack surface of IT, OT and 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 customized and accurate 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 VTM includes:

+ **Skybox Vulnerability Control**: With Vulnerability Control, organizations have the full context of their attack surface - across their network, cloud, and security infrastructure – to find where they are exposed to cyber attacks, quantify the risks of exploitation, prioritize vulnerabilities, and provide optimal remediation options to reduce the highest levels of risk.

+ **Skybox Threat Intelligence**: The threat landscape is in constant change. The Skybox Research Lab has been at the forefront in analyzing the latest cyber vulnerabilities and threats across the industry for over two decades. Our customers leverage this verified and up-to-the minute contextualized threat intelligence by delivering insights on vulnerabilities, intelligence and remediation options in one consolidated source.

Schedule a demo.

skyboxsecurity.com