Skybox Vulnerability Control

Product Tour

8.0.600

Revision 11
About Skybox Security, Inc.

Skybox gives security management and operations the tools they need to eliminate attack vectors and safeguard business data and services every day. With unparalleled visibility and context-aware intelligence of the attack surface, Skybox solutions drive effective vulnerability and threat management, firewall management and continuous compliance monitoring.

Established in 2002, Skybox is a privately held company with worldwide sales and support teams serving an international customer base of Global 2000 enterprises and government agencies.

Contact information

Contact Skybox using the form on our website or by emailing info@skyboxsecurity.com.

Customers and partners can contact Skybox technical support via the Skybox support portal.
# Contents

Overview ................................................................. 5  
  Summary of Skybox Security Suite .................................... 5  
  Introduction to Vulnerability and Threat Management ................ 6  
  About this Product Tour .................................................. 7  
  Skybox Vulnerability Dictionary ............................................ 8  

Launching Vulnerability Control ........................................... 10  
  Skybox Start Menu .......................................................... 10  
  Skybox Login Screen ........................................................ 11  
  License Management ......................................................... 11  
  Adding the License File ...................................................... 12  

Welcome Page ........................................................................... 13  

Skybox Vulnerability Control Dashboard ............................... 14  
  Discovery Center .............................................................. 15  
  Analytics Center ............................................................... 16  
    Security Metrics ............................................................ 16  
    Exposure ....................................................................... 17  
  Remediation Center ........................................................... 17  

Tools Options Menu ............................................................. 19  
  Options: Risk Configuration Settings ..................................... 20  

Network Map ........................................................................... 21  
  Network Map: Access Rules ............................................... 22  

Access Queries .......................................................................... 23  
  Access Query: Analysis ...................................................... 24  
  Access Query: Blocked Destinations ..................................... 24  
  Access Query: Viewing Results ............................................ 25  

Model ..................................................................................... 26  
  Model: Vulnerability Occurrences ........................................ 27  
  Model: Customize Current View .......................................... 27  
    Model: Adding a Column .................................................. 28  
    Model: Customizing the Table .......................................... 29  
    Model: Group by Column ................................................ 29  
    Model: CVSS Impact Scores ............................................ 30
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Dictionary</td>
<td>31</td>
</tr>
<tr>
<td>Vulnerability Dictionary: Additional Tabs</td>
<td>32</td>
</tr>
<tr>
<td>Vulnerability Dictionary: Sort by ID</td>
<td>32</td>
</tr>
<tr>
<td>Vulnerability Dictionary: CVSS Tab</td>
<td>33</td>
</tr>
<tr>
<td>Vulnerability Dictionary: Related Sources Tab</td>
<td>33</td>
</tr>
<tr>
<td>Vulnerability Dictionary: Skybox Dictionary Products Tab</td>
<td>34</td>
</tr>
<tr>
<td>Managing Business Asset Groups</td>
<td>35</td>
</tr>
<tr>
<td>All Assets: Servers</td>
<td>35</td>
</tr>
<tr>
<td>Business Units and Asset Groups: Business Impact</td>
<td>36</td>
</tr>
<tr>
<td>Business Impacts</td>
<td>36</td>
</tr>
<tr>
<td>Threat Origins</td>
<td>38</td>
</tr>
<tr>
<td>Network Vulnerability Risk Analysis</td>
<td>39</td>
</tr>
<tr>
<td>Analyses: Business Asset Groups by Risk</td>
<td>40</td>
</tr>
<tr>
<td>Analyses: Understanding Risk</td>
<td>41</td>
</tr>
<tr>
<td>Analyses: Vulnerabilities by Operating System</td>
<td>42</td>
</tr>
<tr>
<td>Model: Viewing Vulnerability Occurrences</td>
<td>43</td>
</tr>
<tr>
<td>Model: Vulnerability Occurrences by Severity</td>
<td>44</td>
</tr>
<tr>
<td>Application and Client-Side Prioritization</td>
<td>45</td>
</tr>
<tr>
<td>Analytics Center: Security Metrics</td>
<td>46</td>
</tr>
<tr>
<td>MS – Bulletin Level</td>
<td>47</td>
</tr>
<tr>
<td>Security Bulletins</td>
<td>48</td>
</tr>
<tr>
<td>Vulnerability Detector</td>
<td>49</td>
</tr>
<tr>
<td>Risk Analysis, Prioritization, and Remediation</td>
<td>54</td>
</tr>
<tr>
<td>Context-Aware Analysis</td>
<td>54</td>
</tr>
<tr>
<td>Prioritization</td>
<td>54</td>
</tr>
<tr>
<td>Remediation</td>
<td>55</td>
</tr>
<tr>
<td>Automated Analytics Prioritize Vulnerabilities and Speed Remediation</td>
<td>55</td>
</tr>
<tr>
<td>Product Tour Conclusion</td>
<td>57</td>
</tr>
</tbody>
</table>

Skybox version 8.0.600
Chapter 1

Overview

This chapter provides a short overview of Skybox and Skybox Vulnerability Control.

Summary of Skybox Security Suite

The Skybox Security Suite is a proven, award–winning security management platform with an attack surface visualization layer and a portfolio of 5 security analytics modules for vulnerability and threat management and security policy management. The Suite gives operational teams continuous visibility of the attack surface, enabling them to eliminate attack vectors and respond to security threats and incidents in minutes.

The foundation of the Skybox platform provides an integrated process for data collection, modeling, simulation and reporting on an enterprise scale for holistic insight to IT security and operations.

The remainder of this document focuses exclusively on the Vulnerability and Threat Management portion of the Skybox Enterprise Suite.
Introduction to Vulnerability and Threat Management

Enterprise networks under continuous threat can have thousands of vulnerabilities at any given time. With networks growing increasingly complex, being able to mitigate the most critical attack vectors prior to exploitation and respond effectively to new threat advisories can mean the difference between sleeping well at night and front-page news.

An effective vulnerability management program reduces the risks of cyberattacks and provides executives with consistent measurements of risk across the organization. But if too much raw data is generated, vulnerability management can become an operational headache rather than an effective security process. Without an approach suited to today’s business and threat landscapes, critical vulnerabilities can be left exposed for months and assessments can disrupt live business processes. Worse yet, these issues can cause risk levels to increase over time.

To deliver an effective vulnerability management program, security teams need a proactive, integrated approach that enables continuous vulnerability assessments, prioritizes response by business impact and helps plan and track remediation:

The Skybox next-generation vulnerability management solution demonstrates strong business value, helping to eliminate costly risks every day in an efficient manner:

- Non-disruptive vulnerability discovery uses automated, scanless deduction of vulnerabilities and Attack Simulation—no need for disruptive scanners or penetration testing
- Full metrics track remediation progress and risk levels
- Continuous risk mitigation cycles are conducted in days, not months—on a large scale, in a fraction of the time of other solutions
- Compliance reporting addresses PCI, FISMA, and other regulations
Skybox solutions for vulnerability and threat management deliver important business benefits:

**Increase Cost Savings**
- Reduce risk assessment costs by 90 percent by quantifying and prioritizing risk exposures, focusing on the critical 1 – 2 percent* of vulnerabilities
- Cut patch management costs by 80 percent or more by eliminating unnecessary patching
- Eliminate or significantly reduce the need for vulnerability scanners and associated costs

**Reduce Business Risk**
- Reduce the exposure time of critical risks to less than 24 hour—instead of weeks or months—by prioritizing vulnerabilities based on network context and eliminating unnecessary work
- Proactively reduce the chance of a cyberattack or data breach, which cost the average enterprise $3.8M in 2015
- Increase protection against advanced threats by using and fine tuning IPS signatures
- Automate a best-practice vulnerability management approach to meet PCI DSS, FISMA and other requirements

**Improve Processes**
- Make vulnerability management a mature, closed-loop process where results can be tracked
- Eliminate manual risk analysis, allowing security experts to be applied to other tasks
- Ensure that your security team can address vulnerabilities without business disruption with an automated, non-intrusive vulnerability detection that does not require a scanner

**Drive Better Communication**
- Communicate risk levels by organizational unit, and maintain consistent measurements of risk levels across the organization
- Align network and security teams by showing that an attack vector is exploitable and provide actionable steps for remediation

About this Product Tour

*The goal of scanning and vulnerability management is to ensure that risk-causing vulnerabilities exist in an organization’s environment for the shortest amount of time possible.*
There are 2 parts of the above sentence that we explore in this product tour.

- “Risk-causing vulnerabilities” means that the vulnerability management process provides more context than a simple severity score.
- “Shortest amount of time possible” means that discovery of vulnerabilities must happen daily for all assets. The current round-robin scanning paradigm is counterproductive to this goal.

This product tour focuses on the output achievable with a fully configured application. This consists of:

- Vulnerability and asset data imported from multiple sources
- Network device data imported from the devices themselves or management consoles that control those devices
- Business Unit and Business Asset Group classification information
- Data from an SCCM asset management database (which Skybox uses to deduce vulnerabilities)

**Skybox Vulnerability Dictionary**

The Skybox Vulnerability Dictionary consolidates comprehensive and up-to-date vulnerability and threat data from data sources such as: NVD (National Vulnerability Database); published vulnerability repositories; the organization’s vulnerability scanners; threat management feeds for worms, malware, and viruses; and vendor IPS signature feeds such as Palo Alto Networks, IBM Proventia, and Trend Micro TippingPoint.

The Skybox research team runs a detailed modeling of all newly published vulnerabilities and matches each vulnerability to its reported IPS signature and other severity information. Researchers characterize the levels of exploitability, adding exploitation preconditions and effects, and configuring attack patterns to use in Skybox Vulnerability Control’s patented Attack Simulation technology. The Skybox Vulnerability Dictionary significantly reduces false positives and increases accuracy in Attack Simulation by adding details of IPS exploits, vulnerability-based signatures, exploit commonality, severity, platform versions, research sources, worm and malware catalogs, and more.

The Skybox Vulnerability Dictionary represents each vulnerability in a standard, normalized format that correlates to industry scoring methods: CVE ID (Common Vulnerabilities and Exposures), CVSS (Common Vulnerability Scoring System) scores, and Skybox Vulnerability ID (SBV ID).
The Vulnerability Definitions also include references to scanners and plugin IDs, links to relevant sources that describe the vulnerabilities, affected platforms and versions, external product catalogs, and vendor suggested solutions.
Chapter 2

Launching Vulnerability Control

This section explains how to launch Vulnerability Control.

Skybox Start Menu

1. Install the software. Refer to the Installation Guide for step-by-step instructions on how to install Skybox.
2. Choose Skybox from the Skybox Start menu.
Chapter 3

Skybox Login Screen

Log in with the following credentials:

• User: skyboxview
• Password: skyboxview

Note: If this is your 1st time logging in to Skybox, it might take several minutes to start. In the lower left you see Connecting to server until the server starts.

License Management

At this point, you must add your Skybox license.

• Click Manage License.
Adding the License File

Click **Update License** and navigate to the location where you saved the license file. The file is named `license.xml`. 
Chapter 4

Welcome Page

The Welcome Page is displayed when you open Skybox Vulnerability Control. It provides the following useful links:

- **Load demo model**: Loads the preconfigured network model that ships with the software, which you use during this product tour.
- **Getting Started Guide**: Opens the Getting Started Guide, which provides a more in depth look into vulnerabilities and Vulnerability Control. After going through this Trial Guide, consult the Getting Started Guide to learn more.
- **On-line help**: Opens the on-line help for all Skybox products.

**Loading the demo model**

- Click **Load demo model** to bring in the demo model to use during this product tour.
Chapter 5

Skybox Vulnerability Control Dashboard

In the tree, make sure Vulnerability Control is selected and click the **Summary** tab. This is the Vulnerability Control dashboard summary page.

- **Discovery Center**
  - Average Scan Cycle: The average time since the last scan of each device. You can customize the ratings given to scan times as excellent, good, fair, or poor.
  - Last Reported Vulnerability Occurrence by Source: Shows how long it has been since the data was last brought in to the Skybox model. This chart enables users to understand the ‘freshness’ of their organization’s scan data.

- **Analytics Center**
  - Risk Level: Compares the overall vulnerability level and the exposure level (of vulnerabilities to attacks) to provide an overall risk level for the organization
  - Security Metrics chart: Gives you a high-level picture of which parts of the organization have the most risk

*Note: The Security Metrics chart is not always visible.*

- **Remediation Center**
  - In SLA: Shows how many of the vulnerabilities are within the organization’s SLA for remediation
Chapter 5    Skybox Vulnerability Control Dashboard

- Found Vulnerabilities by SLA: Gives you a picture of the remediation status of the organization

Discovery Center

The process used in Vulnerability Control involves 3 stages: discovery, analytics, and then remediation. The summary page shows this in a very brief format. There is also a dashboard for each stage that provides additional information.

The Discovery Center is the main area for understanding the health of your organization, and its assets and technologies.

1. Click the Discovery Center tab.

2. Look at the highlights at the top of the page. You can see such things as the average age of vulnerability occurrences, number of newly discovered vulnerability occurrences, and number of assets with overdue scans.

   The highlights area helps you understand whether the vulnerability information in your model is up to date.

3. Look at the 1st chart, Last Reported Vulnerability Occurrence by Source. You can see that vulnerability occurrence data in the demo model comes from 3 sources:
   - Qualys scans
   - Skybox Vulnerability Detector
   - Intermediate (imported configuration files)

   The chart displays how much of the vulnerability data each source is covering, and how old the data currently is.

4. The 2nd chart in the top row, Vendors by Vulnerability Definitions, helps you understand the breakdown of Vulnerability Definitions across different vendors (technologies).

   This can help security or systems managers understand where to focus for mitigation and remediation efforts.
5 The **Top New Vulnerability Occurrences by Definition** chart lists the most 'popular' (that is, the most frequently occurring) new Vulnerability Definitions.

6 The **OS Vendors by Number of Assets** chart helps you understand how many assets per vendor have been found with vulnerability occurrences. The chart shows the number of assets per vendor and highlights those that were scanned more than 90 days ago as overdue for rescanning or re-identification by Skybox Vulnerability Detector.

### Analytics Center

Skybox calculates risk and compliance data based on the vulnerability occurrences in your organization, and displays security metrics and exposure data for the organization.

The **Analytics Center** is the main area for viewing security metrics and exposure. It enables the security team to understand which threats pose the greatest risk and what your organization is doing about them.

The left side of the page shows how the organization looks in terms of security metrics, and how much change there was over the past week or month. The right side shows how exposed the organization is to threats (potential attackers).

### SECURITY METRICS

Security metrics are calculated based on the density and severity of vulnerability occurrences. They provide threat-level ranking for your organization as a whole and for each business unit. There are a number of predefined security metrics to cover different types of vulnerabilities, such as Microsoft Security Bulletins, Cisco Security Bulletins, and web browser vulnerability occurrences; you can define additional security metrics.

1. Click the **Analytics Center** tab.

2. Look at the **Security Metrics** section.

   Each metric displays your organization’s security statistics from a different point of view, and whether the statistics changed over the last week.
Clicking the link to a security metric brings you to more information about that security metric in the Analytics Center.

EXPOSURE

Exposure shows how close the vulnerability occurrences in your organization are to Threat Origins (locations of potential attackers). Direct vulnerability occurrences are those that are 1 step away from a Threat Origin.

1. The **Direct vulnerability occurrences by Risk** pie chart shows you the vulnerability occurrences that are 1 step away from a Threat Origin, grouped according to their risk.

2. The **Top 3 Threat Origins** chart shows you the Threat Origins that pose the most risk to your organization. For each Threat Origin, you can see how many vulnerability occurrences are directly exposed to this threat (1 step away from a possible attack), and how many are 2 steps away.

3. Click a direct vulnerability occurrences link in the Top 3 Threat Origins chart. This brings you to a list of the direct vulnerability occurrences for that Threat Origin.

Remediation Center

The Remediation Center tracks the pace of vulnerability occurrence remediation in your organization. The pace is monitored according to the organization’s SLA, which specifies how long it should take for vulnerability occurrences to be fixed. Vulnerability occurrences that still have time to be fixed are considered *in SLA*. After that, they are considered to be *out of SLA* with various delay levels. For example, if the SLA for critical vulnerability occurrences in your organization is 30 days, a vulnerability occurrence is considered *in minor delay* if it still has not been fixed within 60 days, *in medium delay* within 90 days, and *in major delay* after that.
To understand the pace of vulnerability occurrence remediation in your organization

1. In the tree, click **Vulnerability Control**, and then click the **Remediation Center** tab.

2. Look at the highlights at the top of the page.

3. Look at the **Remediation Overview** section.

   - The 1st chart shows the remediation rate of vulnerability occurrences in the organization.
   - The 2nd chart shows how many high and critical vulnerability occurrences are already out of SLA, and by how much.
   - The 3rd chart shows a comparison of how many high and critical vulnerability occurrences were found in the past months or weeks vs. how many were fixed. This helps you to understand whether you are keeping pace with the rate at which vulnerability occurrences are found in the organization.

4. Look at the **All Security Metrics** section.

   The table shows SLA-related information about all security metrics. The main column—**In SLA Vulnerabilities**—makes it easy for you to see which security metrics have a low percentage of vulnerability occurrences that are in SLA. Examine these security metrics carefully to see what happened.
Chapter 6

Tools Options Menu

To see more detailed risk scores, you can change the Risk Value Style from **Level** (Very Low to Very High) to **Score** (0 - 100).

1. From the menu choose **Tools > Options**.
2. Note: The Options menu is used to change various settings in Skybox.
3. Select **Manager Options > Risks Configuration**.

Note: The Options menu is used to change various settings in Skybox.
Options: Risk Configuration Settings

1. In the Options menu, find **Risk Configuration** on the left and select it.
2. From the drop-down list on the right, change the risk value style from **Level** to **Score**.
3. Click **OK** to save the change and close the dialog box.
A unique feature of Skybox is its ability to understand how vulnerabilities relate to the network security devices that mitigate the risk of those vulnerabilities being exploited. To do this, Skybox must import network device data. This data can then be displayed as a network map.

1 On the toolbar, click **Network Map**. It opens in a separate window.
2 In the Map field, select **Organization Map**.
Network Map: Access Rules

You can access some of the properties of the devices in your network from the map.

To view the access rules for main_FW, right-click main_FW in the map and select Access Rules.

You can see the firewall access rules in a separate window named Access Control List Editor.
You can create access queries to find all routes between a selected source and destination. You can create these access queries using the Network Map, to trace a route through the network to investigate the firewalls and access rules that network traffic traverses.

1. In the London group, right-click **financeUnixWS** and select **Set as Source**.
2. In the New York group, right-click **app0** and select **Set as Destination**.
Access Query: Analysis

1. To the left of the map, select **Access Query**.
   In the upper left you can see the IP addresses and names of the source and destination that you selected via the map.
2. Click **Analyze**.

Access Query: Blocked Destinations

When the analysis is complete, you can see that there is no access between the source and destination you selected. You can change the analysis to show where the route is blocked.
Change the value in the Show drop-down list from Accessible Destinations to Blocked Destinations.

Access Query: Viewing Results

1 In the tree on top of the map, click the arrows to fully expand the route and select Any Internet Protocol.

In the map, you can see that the source and destination are marked and the route between them is highlighted. The prod FW is highlighted in red, indicating that this is the device that is blocking the path.

2 To the left of the map you can see each step of the route, including the network device and rule (if applicable) encountered. Rule #13 of prod FW is the specific rule of the device that is blocking access; you can click either the rule or the device for additional information.
Chapter 9

Model

The Model workspace displays data about the entities in your organization that are modeled in Skybox. Data from all sources, including devices, scanners, and vulnerability sources, is normalized as it comes into the model, and is presented in a uniform manner.

> On the bottom left hand side, click the **Model** icon (≡).
In the tree, select **Vulnerability Occurrences**.

Note that the model currently includes over 5,000 vulnerability occurrences. A vulnerability occurrence is a single instance of a specific Vulnerability Definition that exists on an asset in your network.

**Model: Customize Current View**
The table in the workspace is customizable. You can change the order of the columns and display additional columns to help you understand the information from different perspectives. For example, you can add the Discovery Method column to see where the vulnerability occurrences have come from.

> Right-click a column header and select Customize Current View.

**MODEL: ADDING A COLUMN**

1. Scroll down the list and select **Discovery Method**.
2. Click **OK** to close the dialog box.
MODEL: CUSTOMIZING THE TABLE

Drag the **Discovery Method** column header over to the 2nd position in the row and move the **Asset** column header to the 3rd position.

MODEL: GROUP BY COLUMN

1. Right-click the **Discovery Method** column header and choose **Group by Column**.
2. Do the same for the **Asset** column header.
1. Expand **Discovery Method: Qualys**.
2. Find and expand **Asset: dmz_web_server_1 [192.170.33.2]**.
3. Click the **ID** column header to sort by ID (ascending order).
4. Select a vulnerability occurrence.
5. In the bottom pane, click the CVSS tab.

Skybox uses the CVSS impact data for Confidentiality, Integrity and Availability (CIA) to calculate the impact of the vulnerability on a specific asset. This value becomes part of the overall risk score for the vulnerability occurrence.
1. On the bottom left hand side, click **Vulnerability Control**. This moves you back to the Vulnerability Control workspace.

2. In the tree, select **Analyses > Public Analysis > Vulnerabilities > Dictionary > Vulnerability Dictionary**.

   This is a view of the Skybox Vulnerability Dictionary, which provides proprietary intelligence to accurately model the behavior of each detected risk and simulate all possible attack scenarios, so that you can mitigate critical vulnerabilities fast. This list is compiled from many feeds including iDefense, DeepSight, X-Force, CVE, and active scanner partners.

Various vulnerability dictionaries and vulnerability lists are available on the market. These lists include valuable textual information about the vulnerabilities and ways to fix them. They do not supply a formal modeling of the vulnerabilities, which is required for simulating the exploitation of vulnerabilities by an attacker. The Skybox Vulnerability Dictionary models the behavior of each vulnerability in attacks. The information for each vulnerability includes the Skybox ID number, preconditions for exploiting the vulnerability, what an attacker could gain by exploiting the vulnerability, and the difficulty level for exploiting the vulnerability. The Dictionary also includes cross-references to multiple vulnerability lists.
In the bottom pane, click the folder icon (｡ Pag) at the far right to open additional tabs.

When this icon has a “+” on it, clicking it opens additional tabs in the bottom pane. When the icon has a “-” on it, clicking it closes the additional tabs, leaving only the basic tabs.

Vulnerability Dictionary: Sort by ID

1. Right-click the ID column header and select Sort Ascending.

2. Scroll through the list until you find SBV-42288 (CVE-2013-5330).
Click the **CVSS** tab.

The Skybox Vulnerability Dictionary provides CVSS information for the base and temporal vector of each vulnerability. This standard enables users to easily analyze the impact of a vulnerability, including how it can be exploited (locally or remotely, with or without authentication, and so on) and its possible impact in terms of CIA (confidentiality, integrity, and availability).

**Vulnerability Dictionary: Related Sources Tab**

Click the **Related Sources** tab.

This list shows how the vulnerability is described in other products and databases, along with the original severity score as reported to Skybox.
1 Click the **Skybox Dictionary Products** tab.

This tab lists the application and operating system versions on which this vulnerability is known to exist.

2 Explore the **Solutions** and **External URLs** tabs as well. These tabs provide remediation suggestions and links to external reference information respectively.
Chapter 11

Managing Business Asset Groups

In Skybox, assets (hosts) are usually grouped into Business Asset Groups for easier management; you can view information about groups of related assets, in addition to the information provided on each asset separately.

All Assets: Servers

1. On the bottom left hand side, click the Model icon ( ).
2. In the tree, select All Assets > Servers.
3. In the workspace, sort the Name column in ascending order.
4. Find the dmz_web_server_1 server and select it.
5. In the bottom pane, click the Business Asset Groups tab.

Business Asset Groups enable you to categorize assets (hosts) according to how they are used. In our example, this web server is in the Front End Web Servers Business Asset Group. Categorizing assets is completely customizable and enables you to better understand the context of a vulnerability occurrence.
Now let’s look at how an asset is given a *Business Impact* weighting.

1. In the tree, select **Business Units & Asset Groups > US Headquarters > Corporate Services**.
2. Right-click **Front End Web Servers** and select **Properties**; in the dialog box that opens, click the Business Impacts tab.
A Business Impact is how Skybox captures the importance of an asset and quantifies the damage that would be caused by a loss of availability of the asset, or a loss of confidentiality or integrity of the data on the asset. In this example, you see a Critical/High/Medium/Low/Very Low scale. Damage can be described monetarily for environments where that quantification would be useful.

The Front End Web Servers Business Asset Group represents web servers that are easy to fix—damage caused by the loss of data integrity for this group is Low.

The assets in this group contain no confidential information, so no rating is given for loss of confidentiality.

These assets are commonly used, but not mission critical, so damage caused by the loss of availability of this group is rated as Medium.

Click Cancel when you have finished viewing.
In the tree, expand **Threat Origin Categories** and select **All Threat Origins**.

Threat Origins are used to determine the exposure of a vulnerability occurrence and therefore the likelihood that the vulnerability occurrence could be exploited in a specific environment. Threat Origins model automated attack sources, such as malware and worms, and human sources, such as internet hackers or a compromised workstation under the control of a person with malicious intent.
Network Vulnerability Risk Analysis

Network vulnerability risk analysis prioritizes vulnerability occurrences that are exploitable over the network. It is based on the classic risk equation $\text{Risk} = \text{Impact} \times \text{Likelihood}$ and is a much more accurate indicator of a vulnerability occurrence’s potential damage than only the severity score, which is commonly the only indicator offered by other vulnerability assessment vendors.

The impact portion of the score is a measure of how much potential damage a specific Vulnerability Definition could cause on a specific asset. This is calculated by matching the Confidentiality, Integrity, and Availability impact ratings from the CVSS scoring with the Business Impact damage ratings for an asset group.

The Likelihood portion of the score is measured using Attack Simulation. Threat Vector Analysis from a Threat Origin to an asset with vulnerability occurrences, calculates whether the vulnerability occurrence is directly exposed to a Threat Origin, indirectly exposed (via ‘pivot’ or ‘stair-step’ attacks), or not exposed at all.
Chapter 14

Analyses: Business Asset Groups by Risk

1. On the bottom left hand side, click Vulnerability Control.
2. In the tree, select Analyses > Public Analyses > Risks > Business Asset Groups by Risk.

This screen lists the portions of the network that have assets with vulnerability occurrences that are imposing risk.
Chapter 15

Analyses: Understanding Risk

1 In the table in the workspace, select Front End Web Servers.
2 In the bottom pane, click the Vulnerability Occurrences tab.
3 Right-click the Risk column header and select Sort Descending.
4 Use the scroll bar to scroll through the vulnerabilities.

You can see that of all the vulnerability occurrences in Front End Web Servers, only 10 of them with a severity of Critical impose risk on the network. Conventional wisdom (and traditional severity-based remediation SLAs) suggests that the critical severity vulnerabilities should be remediated first. However, there are several vulnerabilities with a severity of only High or Medium that also introduce risk into the network; these should be handled before the vulnerabilities with Critical severity but no risk.

By managing remediation based on Risk instead of Severity, you can ensure that risk-causing vulnerability occurrences exist on their network for the shortest amount of time possible.
In the tree, select **Vulnerabilities > By Operating System > Windows**. This is another perspective you can use to put vulnerability occurrences in context.
Chapter 17

Model: Viewing Vulnerability Occurrences

1. Return to the Model workspace by clicking **Model** below the tree.
2. Click vulnerability occurrences in the tree.
3. Right-click anywhere on the **Discovery Method** or **Asset** header and select **Clear all Group by** to bring back an unsorted list of vulnerability occurrences.
Right-click the **Severity** header (the 1st column, with the exclamation point) and select **Group by Column**.

As you saw in the previous steps, using a traditional, severity-based remediation program on this set of vulnerability occurrences would have the remediation team fix thousands of critical vulnerability occurrences before they got to the High, Medium, and Low severity vulnerability occurrences that are actually imposing risk! Working with Skybox gives you several ways to find the vulnerability occurrences that need the most urgent fixing.
Chapter 19

Application and Client-Side Prioritization

Attack Simulation is a very accurate way to quantify the risk imposed by exploitable network vulnerabilities. In many networks, though, these vulnerabilities only account for about one-third of the total vulnerability occurrences seen on the assets (hosts). The other two-thirds are client-side and application vulnerabilities. Skybox has multiple ways to represent these vulnerabilities using various types of security metrics. Security metrics help you to categorize the vulnerabilities in your networks based on organization, technology, or custom metrics.

› General security metrics:
  Overall and new – measuring density of vulnerabilities in your organization, and what’s new, regardless of technology.

› Technology-specific security metric:
  Microsoft, Adobe, Oracle, and others – enabling technology stakeholders to understand security status and patch level by technology. You can also choose to view the security status of specific browsers.

› Custom security metrics
  You can add custom security metrics to enable users to view security metrics for their specific needs. For example, adding an anti-virus security metric to the Skybox model enables users to view the security status of end-point security controls.
Chapter 20

Analytics Center: Security Metrics

Security metrics provide threat indicators for your organization as a whole and for specific Business Units, enabling the security team to help management understand which threats pose the greatest risk and what you are doing about them.

Most security metrics in Skybox measure the status of vulnerabilities in the organization. However, some security metrics measure the status of applying security bulletins from vendor-based catalogs, such as Microsoft, Adobe, and Cisco.

1. Return to the Vulnerability Control workspace by clicking Vulnerability Control below the tree.

2. In the tree, select Security Metrics.
Security metrics are customizable and there are many that are included as part of the installation.

1. To see the available security metrics, click the drop-down button next to the currently selected security metric towards the top of the workspace.

2. Select **MS – Bulletin Level**. This security metric is designed to enable users to understand which Microsoft Security Bulletins have the greatest impact on vulnerability remediation.

3. In the bottom pane (Top Security Bulletins), click **MS14-037**.
You can see that there are a number of security bulletins that can be applied to fix this issue. The bulletin that you selected in the previous screen is highlighted.

1. In the bottom pane, click the Vulnerability Occurrences tab.
   
   You can see that rolling out Microsoft Security Bulletin MS13-021 would remediate many vulnerability occurrences in this environment.

2. Clear the grouping in the Status column and then group by the CVE column.
   
   You can see that there are only 4 different Vulnerability Definitions (4 CVEs) altogether that are causing these vulnerability occurrences.
Chapter 21

Vulnerability Detector

Most organizations today use traditional active scanning to discover vulnerabilities, which requires a remote scan of each network-attached device. But this approach to vulnerability assessment is often constrained by:

- **Limitation of access**: Some network assets and services are so critical that organizations are very hesitant to permit scanning access because it might impact availability. This becomes the paradox of vulnerability assessment; the assets that need it the most are those that we are most reluctant to assess.

- **Distribution of assets**: Other assets and services are difficult to identify or access due to location, such as cloud assets or mobile devices.

- **Information overload**: Vulnerability scanners drown IT security teams in data and are notorious for producing ‘300-page reports’ with long tables of vulnerabilities but no network context, risk prioritization, or options for fixes.

Because of these constraints, most organizations only scan portions of their networks or scan in segments, which leads to lengthy scan cycles. Both the frequency and scope of vulnerability management become inadequate. If the goal is to ensure that risk-causing vulnerabilities exist in an environment for the shortest amount of time, traditional active scanning (as practiced by most worldwide corporations) is not the tool to achieve that goal.
Our observations suggest that the most common remediation SLA for a critical vulnerability is 14 days. If you scan an asset every 30 days, it is possible that a critical vulnerability could exist on the asset in an exploitable state for 29 days before you even know that the vulnerability is there. Only then does the 14-day remediation clock start.
Skybox takes a different approach to vulnerability discovery. Rather than relying on vulnerability scanners, Skybox Security created a patented scanless discovery approach that can be used independently to discover vulnerabilities, or used with existing scanners to augment vulnerability discovery. When used together with an active scanner, Vulnerability Control augments weekly or monthly active scans with continuous, daily updates from Vulnerability Detector for accurate and up-to-date security intelligence.

Skybox Vulnerability Control with Vulnerability Detector leverages data from system and network operations management systems which are already deployed in most organizations. While these systems don’t report on vulnerabilities, they have accurate information about the OS of the asset, the installed products, the installed patches and the missing patches. This information is typically refreshed daily. Using this data, Vulnerability Detector deduces the vulnerability occurrences on each asset; this becomes a source for vulnerability occurrences in Skybox Vulnerability Control.
Although the deployment is simple, it is complex to deduce vulnerability occurrences in a reliable way using product and patch information. For that purpose, Skybox developed a unique approach named *rule-driven profiling technology*, which formalizes the product and version information in an accurate way (patent pending), and then determines the vulnerability occurrences associated with each product, considering the exact product version, service pack, OS version, and patch information. Rule-driven profiling uses extraction rules that are available in Skybox’s proprietary Vulnerability Dictionary, which is distributed on a daily basis.

Vulnerability Detector can be used on a daily basis across the entire organizational network. Using Vulnerability Detector, you have same-day knowledge of exposed vulnerability occurrences, enabling you to begin remediation steps far earlier than traditional scanning can provide.

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Vulnerabilities</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Scanners</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Skybox Vulnerability Dictionary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Management Database</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(SCCM / WSUS / AD Dis Fix / etc..)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Scanner data contains a matchup between vulnerabilities and assets.
- Skybox provides an extensive vulnerability database.
- Skybox imports asset data from the network infrastructure and from asset management databases.
Vulnerability Detector matches up the assets with the vulnerabilities.

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Vulnerabilities</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Scanners</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Skybox Vulnerability Dictionary</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Asset Management Database</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(SCCM / WSUS / AD BigFix / etc...)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Chapter 22

Risk Analysis, Prioritization, and Remediation

Vulnerability discovery is one aspect of an effective vulnerability management program. To reduce the risks of cyberattacks, support continuous monitoring, and provide executives with useful measurements of risk, organizations need a proactive approach that prioritizes vulnerabilities by business impact and automates and tracks remediation activities. This approach enables you to find and resolve critical risks in a single day instead of months, eliminating unnecessary patching and drastically reducing security management time.

Skybox Vulnerability Control provides a closed-loop solution that identifies network vulnerabilities, eliminates vulnerabilities that are not exploitable, prioritizes remediation based on business impact and exploitability, and integrates actionable remediation steps to mitigate the most significant risks before they can be exploited.

Context-Aware Analysis

Multiple vulnerability feeds can be merged. You can specify how they are merged and, in a conflict, which feed takes precedence. Once this fresh vulnerability data is available on a continuous basis, the next challenge is automating analysis of the vulnerability occurrences so that the subsequent prioritization can focus on the critical risks and ignore low-risk exposures. The idea is to create a short list of action items that can be executed quickly to eliminate the risk of exploitation by attackers.

How can you determine which vulnerability occurrences are critical and which can be skipped? There are 2 approaches, which are commonly used together for analysis:

- **Hot Spot Analysis**: Find groups of assets on the attack surface with a high density of severe vulnerabilities, which can be fixed *en masse* by broad action items, such as patching
- **Attack Vector Analysis**: Use a surgical approach that finds specific, high-risk attack vectors around a few assets that require quick remediation (patching, shielding, network configuration) to eliminate exposure of specific targeted assets

Prioritization

Context-aware prioritization challenges a vulnerability occurrence’s severity rating, asserting that the criticality of a vulnerability occurrence depends on several factors, including existing security controls, threat data, the business asset, and the impact of a potential attack.
Today’s attacks often incorporate multiple steps that cross several different network zones—an isolated view of any of these steps could appear innocuous. Attack Simulation technology looks at the holistic network and identifies what would happen if the steps are put together. Attack Simulation can also determine the best point in the attack to deploy security controls.

Attack Simulation technology looks at network context, asset criticality, business metrics, and existing security controls when determining the impact of a potential attack. For example, if an asset runs an application that is crucial to maintaining the business and requires continuous availability, a medium-level vulnerability that threatens to disable this asset might be a high-level risk to this particular business.

Remediation

The final step is remediating critical vulnerability occurrences. For effective vulnerability management, integrate remediation into the solution and consider all security controls:

▶ **Is there a patch available?** Can a patch be deployed or is it *unpatchable* due to system integration issues, location, availability requirements, custom application limitations, etc.?

▶ **Will system changes remediate the vulnerability occurrence?** For example, is it possible to reconfigure the network or change access controls to mitigate the vulnerability occurrence?

▶ **Are there other security controls available?** If a patch is not available, are there other security controls that can provide protection such as firewalls, IPS or anti-malware signatures, or other defenses?

Remediation should consider all security controls, not just patching, and the availability of security controls should be part of the prioritization process. For example, with a list of critical vulnerability occurrences for the organization, it makes sense to prioritize easy-to-remEDIATE vulnerability occurrences over those that are resource intensive. This provides the most protection for the organization in the shortest amount of time.

Automated Analytics Prioritize Vulnerabilities and Speed Remediation

Skybox uses automated security metrics to prioritize vulnerabilities by severity, vendor, or Business Asset Group. This enables network teams to continuously analyze, track, and report progress towards risk level reduction. Additionally, Skybox Vulnerability Control provides actionable remediation steps—a ‘recipe for remediation’—and an integrated workflow to create support tickets and optimize patching activities.

Risk-based prioritization benefits:

▶ **Focus time and resources:** Automated vulnerability occurrence analysis eliminates lengthy cycles required to manually analyze long vulnerability reports
▶ **Optimize patching activities**: Reduces patch management time, improves patch scheduling, and avoids unnecessary patching

▶ **Track and measure remediation progress**: Provides executive-level visibility into your organization’s risk trends
Chapter 23

Product Tour Conclusion

This concludes the product tour guide for Vulnerability Control. To view a more detailed demo or to request a guided demo, contact your local sales team or send an email to info@skyboxsecurity.com