Attack Your **Attack Surface**

How to reduce your exposure to cyberattacks with an attack surface visualization solution

MARCH 2016

SKYBOX™ SECURITY

Prepared for Skybox® Security by Jon Friedman, CyberEdge

Contents

The Expanding Attack Surface — An Unfair Advantage for Hackers

The average enterprise today must defend against exploitation of an attack surface composed of tens of thousands of potentially exploitable attack vectors on its networks and systems. The size and complexity of that attack surface expands daily, as companies roll out new applications and technologies and as cybercriminals and hackers find new vulnerabilities.

Also, in cybersecurity, attackers have an unfair advantage over defenders. Hackers can choose the time and place of battle and need to find only a single weak point in the defenses to exploit. IT organizations must monitor and secure the entire attack surface of the enterprise and don't have the luxury of focusing on any one portion of their long list of attack vectors.

Most enterprises are further disadvantaged by their inability to understand and systematically manage their attack surface as a whole. Usually they are forced to prioritize a few "hot" vulnerabilities or to operate in crisis mode, reacting to headlines about the latest cyberattack.

It's like sailing in a leaky wooden boat: water seeps into the bilge, nobody can see below the waterline, so instead of patching the most dangerous holes, everyone just bails.

But you don't have to operate blind. Attack surface visualization can change the game completely by enabling you to:

- Visualize and analyze the attack surface of your entire enterprise, including the network topology, tens of thousands of Indicators of Exposure (IOEs) and security controls
- Prevent data breaches by highlighting the areas of highest risk and prioritizing remediation efforts accordingly
- Respond faster to emerging threats by pinpointing and protecting the systems most vulnerable to those threats
- Systematically manage and reduce your attack surface by allocating security resources to where they are most needed, identifying security teams within the enterprise that need extra support, streamlining audits and demonstrating progress toward security and compliance goals

What Does an Attack Surface Look Like?

According to WhatIs.com: "An attack surface is the total sum of the vulnerabilities in a given computing device or network that are accessible to a hacker."[1]

That definition sounds simple, but it raises a question: how exactly can anyone visualize, much less analyze and manage, the attack surface of an enterprise?

TOPOLOGY

The first step in visualizing the attack surface of an enterprise is mapping all of the systems, devices and network segments in the organization, and the paths between them where data can flow. The elements mapped in this topology should include:

- Servers, including Web servers, application servers and database servers
- Endpoints, such as desktop systems, laptops and mobile devices
- Networks, network segments and private and public clouds
- Networking devices, such as routers, switches and load balancers
- Security devices, both physical and virtual, such as firewalls, intrusion prevention systems (IPSs) and VPN concentrators

INDICATORS OF EXPOSURE (IOEs)

The second step in understanding the attack surface of an enterprise is discovering and documenting all of the Indicators of Exposure (IOEs) on the network.

IOEs are indicators that show a system, device or network is exposed to attack. This is in contrast to Indicators of Compromise (IOCs), which are forensic artifacts that indicate that a cyberattack may have already happened.

Types of IOEs include:

- Software vulnerabilities, such as weaknesses in applications, browsers, plug-ins, operating systems, database management systems and software powering network and security devices
- Misconfigurations and missing security controls in systems and software, which allow hackers to access confidential data and to navigate to systems with vulnerable software
- Overly permissive rules, such as any/any rules on firewalls that allow any service from any source to reach any destination
- Violations of security policies and compliance rules, such as network configurations that allow unauthorized users to access credit card numbers or confidential customer information

Tens or hundreds of thousands of IOEs can be found on typical corporate networks. New exposures are created every day, from defects in purchased and internally-developed software, unpatched servers and endpoints, vulnerabilities in network and security devices, and mistakes made by overworked administrators. Most exposures are never exploited, but all of them represent potential attack vectors.

Visualizing the attack surface of an enterprise requires pulling together a wide variety of IOEs, "mapping" them to the organization's topology of systems, devices and network segments, and providing a visual representation that allows managers and IT security professionals to draw actionable conclusions from the data.

1. http://whatis.techtarget.com/definition/attack-surface

INDICATORS OF EXPOSURE (IOEs)	INDICATORS OF COMPROMISE (IOCs)
Indicate exposure to attack	Indicate that an attack is underway or a compromise has already taken place
Include software vulnerabilities, misconfigurations, missing security controls, overly permissive rules and policy violations	Include malware files detected on endpoints and servers, communications from IP addresses controlled by hackers or spammers and evidence of anomalous network traffic or unusual data access requests
Data collected from vulnerability scanners, scanless vulnerability detectors, network and security device logs and threat intelligence sources	Data collected from network and security device logs, network scanning tools, endpoint and host antimalware products and threat intelligence sources
Can be categorized, analyzed and prioritized by vulnerability management systems (like Skybox® Vulnerability Control) and security rules analyzers (like Skybox® Firewall Assurance and Skybox® Network Assurance)	Usually categorized, analyzed and prioritized by security information and event management (SIEM) solutions and incident response tools
Can be visualized with attack surface visualization tools (like Skybox® Horizon)	Can be visualized by incident analysis tools

Obstacles to Understanding an Attack Surface

It might seem that organizations could protect themselves from cyberattacks by following a few best practices: employing vulnerability scanners to ferret out weaknesses, promptly patching all of their systems and applications and implementing a robust set of security controls.[2] However, there are several reasons why these measures are rarely effective by themselves.

MASSIVE VOLUMES OF SECURITY DATA

Most enterprises have thousands or tens of thousands of vulnerabilities on their networks at any one time. They also have thousands of policy rules embedded in firewalls, IPSs and other security systems. Hundreds of new vulnerabilities and rules are introduced every month as organizations deploy and modify applications; add and remove servers and devices; reconfigure networks; and deploy virtualization, cloud computing and other new technologies.

It is impossible for security and network analysts to capture and correlate the massive quantities of security data produced by these changes. Extracting the intelligence needed to monitor IOEs, responding quickly to new threats or setting priorities for remediation are also major challenges.

SECURITY SILOS

Most IT organizations work in silos. Security, network, applications and system operations teams are responsible for different parts of the IT infrastructure and different classes of

2. For a list of recommended controls, see the Center for Internet Security (CIS) Controls for Effective Cyber Defense, summarized at https://www.sans.org/critical-security-controls/guidelines. The controls include inventories of authorized and unauthorized devices and software; secure configurations for hardware and software on mobile devices, laptops, workstations and servers; continuous vulnerability assessment and remediation; and limitation and control of network ports, protocols and services.

vulnerabilities. These teams use their own point solutions, which generate disconnected pools of security data. They have little visibility into (or interest in) areas that overlap or are outside the scope of their responsibility. For example, the desktop operations staff might respond to a threat by spending hundreds of hours patching a vulnerability on desktop and laptop systems, when the same protection could have been provided far more efficiently by having the network security group change a couple of IPS rules at the network edge.

In the same way, teams in different geographical regions and business units often have no visibility into resources and information flows that cross geographic and organizational boundaries.

COMPLEX NETWORK TOPOLOGY AND CONFIGURATIONS

Often the most serious exposures are the result of combinations of vulnerabilities and misconfigurations of network security devices such as firewalls. These combinations expose organizations to attacks that cannot be detected by traditional security solutions. For example, a piece of malware may be able to find its way into the network through a connection to a third party, even though the connection is protected with security technologies such as a VPN. There is no easy way to anticipate these paths into the heart of the enterprise.

NO SYSTEMATIC APPROACH TO SHRINKING THE ATTACK SURFACE

Most IT organizations lack the tools to collect and correlate massive volumes of vulnerability and policy rule information from across the enterprise, or to visualize the attack surface as a whole. That means it is almost impossible for them to do a good job identifying the greatest risks, setting priorities for remediation and allocating resources to the most vulnerable areas. Nor can they track progress toward improving the overall security posture of the organization.

CONSEQUENCES

The inability to visualize and manage the attack surface of the entire enterprise has several negative consequences, including:

- Greater risk of data breaches: IT organizations can't identify all of the vulnerabilities, misconfigurations and overly permissive security rules on their networks, or correctly prioritize the ones they do find
- Slow reaction to new threats: It can take security and IT operations weeks to determine the potential impact of new threats and find and patch all of the associated vulnerabilities
- Difficulty justifying security investments: IT managers lack the data about vulnerabilities and risks that would allow them to demonstrate a business case for additional staff and upgrading technology
- High audit costs: It can take weeks or months to gather information about the entire network topology, get accurate vulnerability data and certify firewall and security device rules and configurations
- Inability to systematically manage remediation: It is impossible to compare data about vulnerabilities and policy violations across groups, or to track progress toward security and compliance goals

What is an Attack Surface Visualization Solution?

Fortunately, these challenges can be addressed by a new type of tool. By combining security analytics and data visualization technologies, an attack surface visualization solution can:

- Incorporate massive volumes of data about IOEs detected on networks and systems, including vulnerabilities, misconfigurations and security and compliance policy violations
- Create a map showing the topology of all the networks and systems and the paths between them
- Display at a glance concentrations and hot spots of IOEs
- Allow users to drill down and observe the concentration of IOEs in specific geographic regions, business units and collections of network and security devices

Skybox Horizon is an example of a leading attack surface visualization solution. In the rest of this whitepaper we will use terminology and screenshots from Skybox Horizon to illustrate the capabilities of this type of tool.

Understanding an Attack Surface

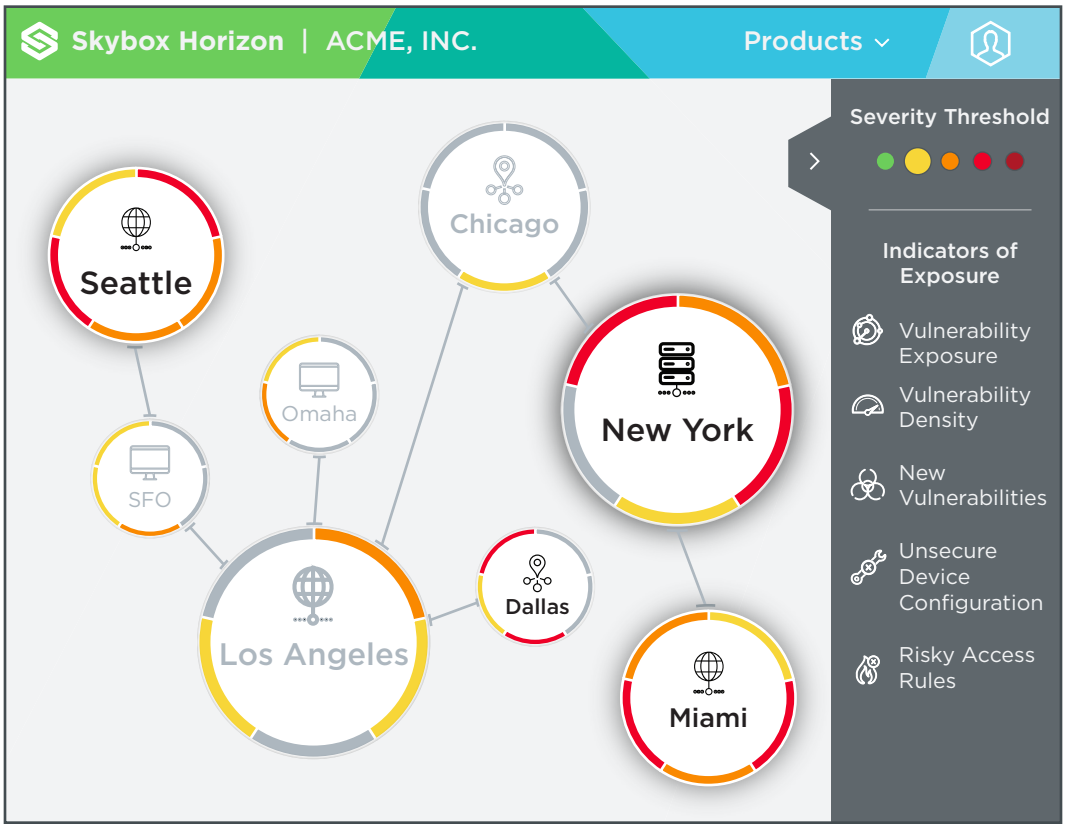

FIGURE 1: A map showing major components of an attack surface and the paths between them. The map provides an at-a-glance view of IOE severity at each node.

Figure 1 is an example of a high-level map of an attack surface – in this case, the attack surface of the American subsidiary of a multinational enterprise.

The map shows nodes, which in this example are the geographical locations of the subsidiary's offices. Lines depict the paths along which information flows between the nodes. The relative size of each node indicates the number of systems and devices included at that location.

Each node is surrounded by a ring of segments, each of which represents a category of IOE. The categories can include security and compliance rule violations as well as new vulnerabilities and exposed vulnerabilities (see explanation on page 10). They can also include indicators of change, such as new vulnerabilities.

The map also shows levels of severity. The severity of each ring segment is represented by its color, with dark red indicating IOEs of critical severity, light red indicating high severity and orange indicating moderate severity. When a node has multiple categories of IOEs with critical severity, then the name of that node is highlighted in boldface.

INSIGHTS FROM A SIMPLE PICTURE

Insights available at a glance from Figure 1 include:

- Attention should be focused first on New York
- In New York, attention should be focused first on the two categories of IOE with critical severity (the two categories can be identified by clicking on the New York node, as shown in Figure 3 below)
- Seattle, Miami and Dallas require the next level of attention
- Los Angeles, Chicago, Omaha and San Francisco represent lower-risk locations

The map also helps avoid mistakes that would be made if information were available only from data silos. For example, the map helps viewers draw important conclusions like:

- Although Los Angeles is a larger location than Seattle, Miami or Dallas, it has fewer critical IOEs; don't allocate resources simply by the size of the location
- Some categories of IOEs pose much greater risks to the enterprise than others; focus on the high-risk categories rather than applying equal resources to all of them
- Different types of IOEs are more severe in different locations; don't assume the type that is most severe in the largest location (New York) poses the greatest risk in every location

It should be noted that although this high-level map may appear very simple on the surface, it could only be created using advanced data integration, visualization and security modeling technologies. The solution had to integrate data from dozens of security and networking products, map the topology of the enterprise, categorize tens of thousands of IOEs, rank the severity of those IOEs and display the data in a format understandable to both technical and business-oriented viewers.

A DETAILED MAP

High-level maps of the atack surface can convey much useful information, but they are only the beginning of what an attack surface visualization solution can provide. Figure 2 illustrates a map that drills down into the network and security devices within the New York node of Figure 1.

Figure 2 maps the attack surface at the level of groups of devices. Viewers can tell at a glance the type of device at each node, the paths between them and the severity of each category of IOEs for each group of devices. They can draw immediate conclusions about what types of devices and what types of IOEs should be given top priority for remediation.

An attack surface visualization solution is not restricted to creating maps of geographic locations or groups of security and network devices. A map can show the topology and IOEs for business units, individual departments, data centers, cloud resources and groups of servers, as well as other entities relevant to the enterprise.

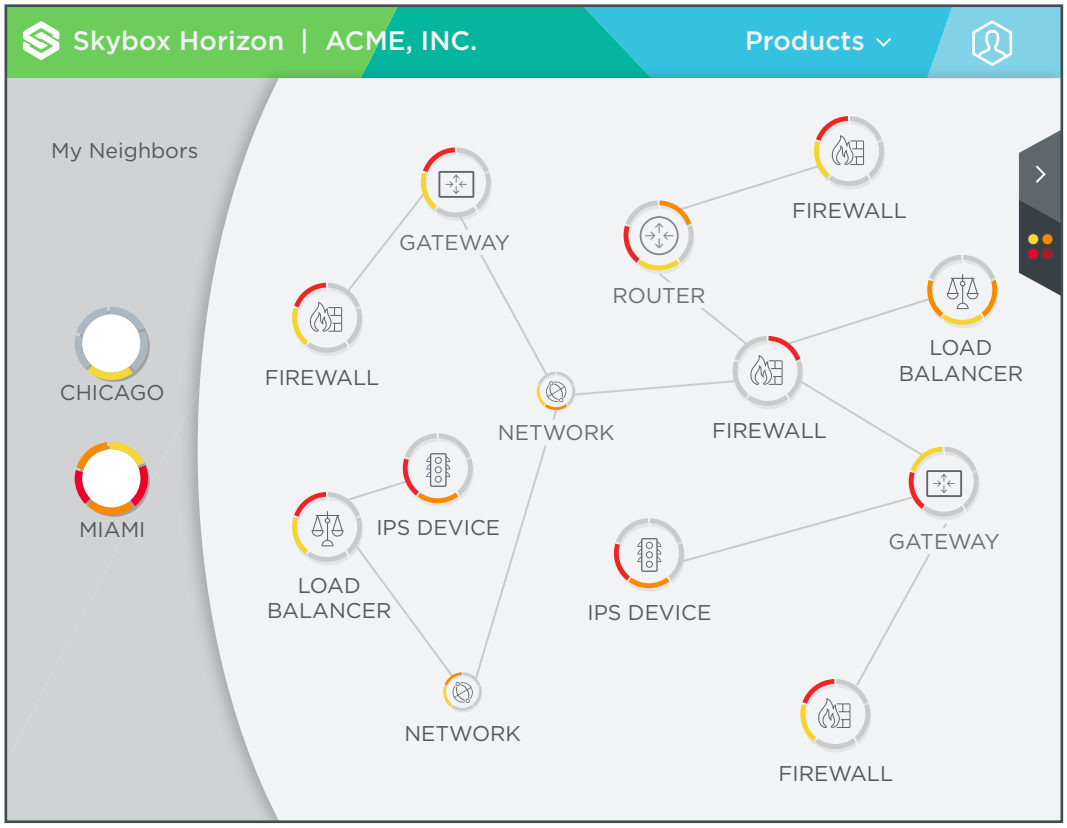

FIGURE 2: A map showing groups of network and security devices within a geographic location and the IOEs in each group.

COMMUNICATING PRIORITIES AND JUSTIFYING SECURITY INVESTMENTS

An attack surface visualization solution is not just a tool for security administrators to plan their activities. It provides a means to communicate security issues and priorities across groups and up the management chain.

For example, the map in Figure 2 might help network, security and IT operations teams develop a common understanding of what types of vulnerabilities pose the greatest risks to the organization. Such an understanding is very difficult to reach when each group brings to the table its own data and its own mental map of security.

The map in Figure 1 could be shared with regional managers to explain why remediation efforts should be focused on specific locations. The same map (with accompanying data) might help make the case to the CEO and CFO that new staff or upgraded security technology are needed to address the areas of greatest risk to the enterprise.

Preventing Data Breaches

An attack surface visualization solution can also help IT organizations prevent data breaches by providing data about vulnerabilities, misconfigurations and rule violations at a location, or within a specific business unit, data center, group of devices or other node in the attack surface map.

Figure 3 shows the five most critical exposures in the New York location from Figure 1.

Exposed vulnerabilities represent a higher level of risk than mere vulnerabilities because they are far easier for attackers to locate and exploit.

Exposed vulnerabilities cannot be detected simply by scanning; they can only be identified by security solutions that can map network topologies and security controls and then correlate those maps with known vulnerabilities. This is one way that attack surface visualization solutions add value to conventional vulnerability scanning products.

The type of information shown in Figure 3 gives IT organizations a means to quickly identify and prioritize the most critical exposures and vulnerabilities at any level of the attack surface, from business units, to individual locations, to data centers, to specific groups of devices. It provides the same type of prioritization for firewall and other device rules that are overly permissive or out of compliance with corporate policies.

These capabilities enable enterprises to prevent data breaches by patching or otherwise remediating the systems and applications that are really most at risk, rather than dissipating effort on low-priority issues and nominally "critical" vulnerabilities that are not actually exposed to attackers.

What is an exposed vulnerability?

An exposed vulnerability is a vulnerability that can be exploited through an attack vector accessible to threat actors.

For example, a vulnerability on a SharePoint server accessible through an Internet-facing Web server is an exposed vulnerability. The same weakness would not be an exposed vulnerability if the SharePoint server were in an isolated internal network sub-segment.

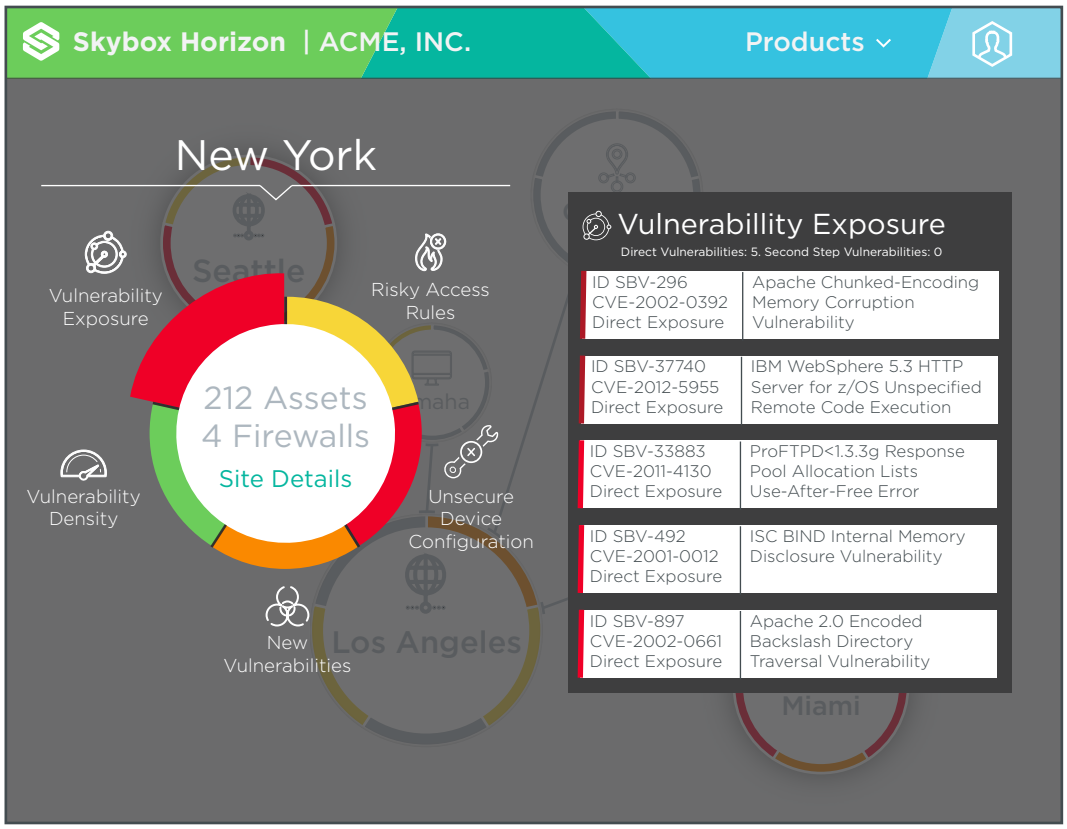

FIGURE 3: A list of top exposed vulnerabilities in the New York location.

Responding Faster to Emerging Threats and Ongoing Attacks

IT organizations often go into firefighting mode when a security intelligence source reveals an emerging threat against enterprises in their industry, or the press announces a zero-day attack based on a newly discovered vulnerability, or the incident response team detects IOCs pointing to an ongoing attack.

Unfortunately, after security and IT operations teams determine the vulnerabilities that can be exploited by the emerging threat, they can spend weeks locating and patching all of the systems affected by those vulnerabilities.

An attack surface visualization solution can enable those teams to identify all of the vulnerabilities across the enterprise in hours. It can also help differentiate between exposed vulnerabilities, which should be addressed first, and other vulnerabilities that are impossible for attackers to reach.

In some cases, an attack surface visualization solution can help security teams find less obvious but more effective means to remediate a threat. For example, if a piece of malware is exploiting a set of known vulnerabilities, it may be possible to protect against exploitation by changing rules on one firewall or adding an IPS signature, rather than patching software on every desktop system in a department.

In addition, if administrators find that a security policy has been misconfigured on one device, they can quickly find and fix all the other devices that have the same misconfiguration.

Controlling and Reducing the Attack Surface

An attack surface visualization solution can also help an enterprise better manage security activities and systematically reduce its attack surface.

We have already discussed how an attack surface visualization solution can help IT organizations better set priorities for remediation, justify needed investments and target security resources where they can have the most impact. But there are other valuable capabilities as well.

It may be possible to identify security and network teams within the organization that should be emulated. For example, data might show that administrators in location A have done the best job minimizing network security misconfigurations, and that the operations team in business unit X has been able to patch servers faster than other teams. The best practices of these leading teams can be shared with their peers. At the other end of the spectrum, comparative data can also point out teams that could be helped by additional training and support.

An attack surface visualization solution can streamline audit preparation by producing up-to-date maps of network topology and by dramatically reducing the work required to document vulnerabilities. It can validate that firewall and security device rules comply with regulations and corporate policies. It can also be used to document progress toward security and compliance goals.

More broadly, an attack surface visualization solution gives IT executives and managers an essential tool to systematically attack their attack surface. It enables them to extract actionable intelligence from hundreds of thousands of data points, uncover and rank attack vectors that would otherwise be invisible, prioritize remediation activities optimally across multiple business units, and track progress reducing all types of IOEs across all types of networks and systems.

Summary

In cybersecurity, attackers have an unfair advantage because they can succeed based on one weakness in defenses, while IT organizations need to monitor and secure the attack surface of the entire enterprise. Defenders are also handicapped by massive and ever-growing volumes of security data, by security information silos, and by an inability to correlate data in ways that would allow them to manage remediation and other security activities consistently across the enterprise.

A new type of tool for attack surface visualization can address these issues by creating maps showing the enterprise's network topology and concentrations of Indicators of Exposure (IOEs) located in specific geographic regions, business units, data centers and groups of network and security devices.

An attack surface visualization solution enables an IT organization to:

> Visualize the attack surface of the entire enterprise, in order to identify the areas of greatest risk, develop common understandings of risks and remediation priorities across technical and business groups and help justify security investments to the CEO and CFO

> Prevent data breaches by remediating the systems and applications most at risk

> Respond faster to emerging threats and ongoing attacks by quickly locating all of the vulnerabilities associated with those threats and attacks and identifying the fastest and easiest way to provide protection

> Control and reduce the attack surface, by targeting resources where they can have the most impact by identifying high-performing security and network teams and streamlining preparation for audits, as well as giving IT managers essential tools to uncover and rank attack vectors, prioritize remediation activities and track progress toward achieving security and compliance goals

For information on Skybox Horizon, the industry-leading attack surface visualization solution, schedule a live demo with Skybox Security.

About Skybox Security

Skybox arms security teams with a powerful set of security management solutions that extract insight from traditionally siloed data to give unprecedented visibility of the attack surface, including all Indicators of Exposure (IOEs). With Skybox, security leaders can quickly and accurately prioritize and address vulnerabilities and threat exposures.

SKYBOX™ SECURITY

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