SKYBOX SECURITY

# Improving Cybersecurity Management, Workflows and Processes

## The business benefits of the Skybox Security Suite

# SKYBOX® SECURITY SUITE

## Cyber Risk Management


# Total Visibility.

# Focused Protection.™

# Integrated Security Management

## One Platform. Many Solutions.

### Cybersecurity is More Challenging Than Ever

Network assets now live in the cloud, application workloads can be moved around the world and business services are expanding to create myriad holes in network defenses. In addition, adversaries are constantly evolving and stepping up their ability to commit cyberattacks.

### Reduce the Attack Surface

In today's complicated business technology ecosystem, it's no longer sufficient to simply gather security data. You need to quickly identify exploitable attack vectors so you can neutralize risks before an attack occurs and quickly contain attacks when they do. That means gaining complete visibility of your attack surface — all the ways in which your organization is vulnerable to cyberthreats — so you can reduce and control it.

### Think Strategically and Holistically

Now is the time to evolve your security management from a passive "check-the-box" approach, relying on disconnected products and processes, to a powerful, data-driven program. A new approach combines comprehensive network visibility, security analytics and understanding of the potential business impact of a successful attack to focus security action where it matters most for your organization.

- Measurably reduce risk
- Improve your security posture across physical, virtual and cloud environments
- Increase cost savings and reduce resource burden
- Improve operational processes
- Enhance communication and collaboration

Skybox® Security provides unprecedented attack surface visibility and advanced analytics, giving you actionable intelligence to respond quickly to threats, proactively improve security and better inform strategy and investments.

The Skybox® Security Suite includes five modules on a common security analytics platform designed to meet complex challenges in vulnerability and threat management and security policy management. Through platform integration with more than 130 networking and security technologies, the Suite unifies data from an organization's existing solutions, breaking down the silos between products, processes and teams. Using network modeling, attack simulation and analytics, Skybox is able to build the most comprehensive picture of an organization's attack surface and indicators of exposure (IOEs) across physical, virtual and cloud networks, and even OT environments.

# Attack Surface Visibility

## Understand, Reduce and Protect Your Attack Surface

### Visibility Is Key

Your IT security teams are faced with many disruptive trends, from next-generation and virtualized network architectures to rapidly mutating threats at every possible point of entry. These forces increase the complexity of your primary objective: to secure and defend the network from attacks and data breaches.

The problem is, you can't protect what you can't see. A platform that visualizes all the layers that make up your organization's attack surface is the foundation your security team needs to effectively manage and reduce it. In addition, the ability to model your network gives you more insight into how your security measures are working together — or leaving you exposed to attack.

### Indicators of Exposure

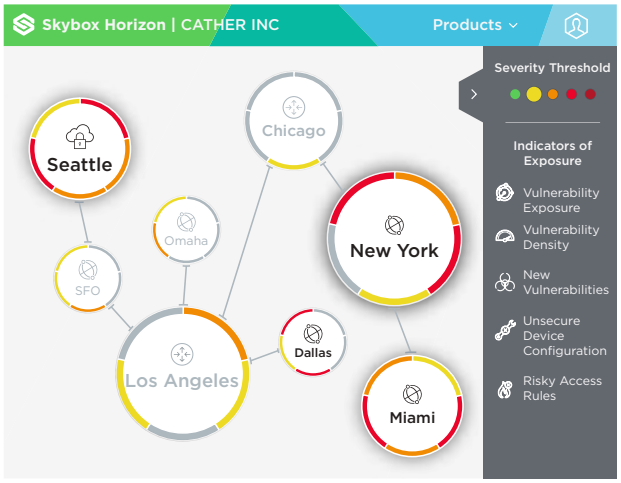
Indicators of exposure (IOEs) offer deep yet actionable insight to the attack surface. IOEs bring traditionally disparate areas of risk under a common language, making it easy for an organization to holistically understand their security status. Each IOE consolidates multiple security factors to gain a more accurate, contextual metric. Focusing on IOEs — such as vulnerability density, risky access rules and new exposures — improves network defenses, ensures consistent workflows and minimizes risks that changes to configurations and access policies could cause.

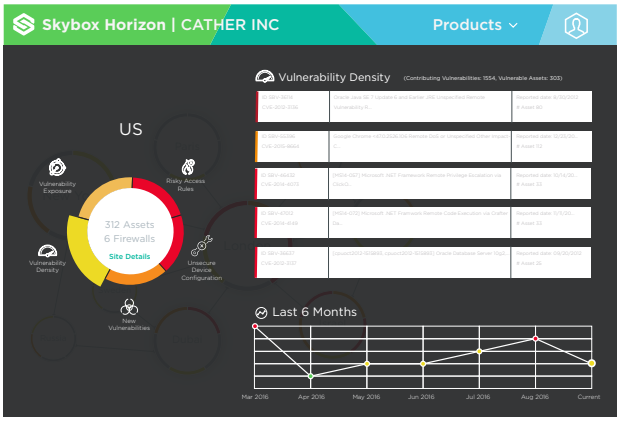
### Evaluate in Context

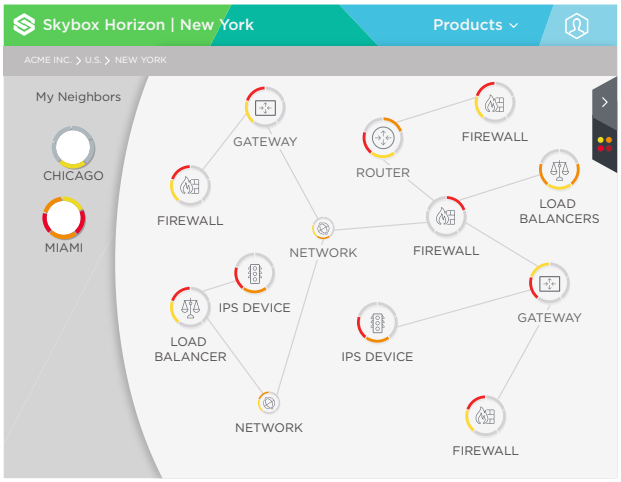
Simply knowing the criticality of vulnerabilities and threats is insufficient for understanding the true security posture of your organization. For example, a vulnerability with a "medium" CVE score could actually be a critical risk to your organization if it exposes an asset running a crucial business application. Understanding how vulnerabilities and threats relate to your entire IT infrastructure and business is fundamental to managing and reducing the attack surface. And, contextual intelligence enables you to prioritize security management tasks to better protect your most critical assets.

Focusing on indicators of exposure (IOEs) puts security issues in more accurate context, helping strengthen network defenses and enabling workflows that quickly mitigate critical risks.

# BUSINESS BENEFITS




## REDUCE BUSINESS RISK

- Achieve and maintain compliance with industry and regulatory best practices
- Ensure your network is hardened against threats and vulnerabilities
- Reduce audit costs, scope and time needed to prepare and execute them
- Integrate security across both IT and operational technology (OT) devices

## AT-A-GLANCE VIEW OF SECURITY POSTURE

- Quickly visualize your attack surface and perimeter
- Drill down on IOEs like risky access rules or new vulnerabilities
- Understand how and where you are most exposed in order to focus remediation efforts
- See how IOEs are trending over time to gauge the effectiveness of security strategy

## IMPROVE COMMUNICATION AND COLLABORATION

- Provide high-level views to executives, the board and security management teams
- Justify the need for security budgets to executives and the board
- Empower network, security and vulnerability teams to work closely with a common language and platform
- Provide staff with security analytics to efficiently focus remediation efforts

# Vulnerability Management

## Prioritize Vulnerability and Threat Response

### Mature Vulnerability Management

Large organizations have thousands of vulnerabilities on their network — some months or even years old. And chances are, the latest threats that have been announced are taking advantage of known vulnerabilities your team has yet to fix.

With most organizations unable to detect, assess, prioritize and remediate vulnerabilities fast enough, vulnerability management becomes an impossible game of catch-up.

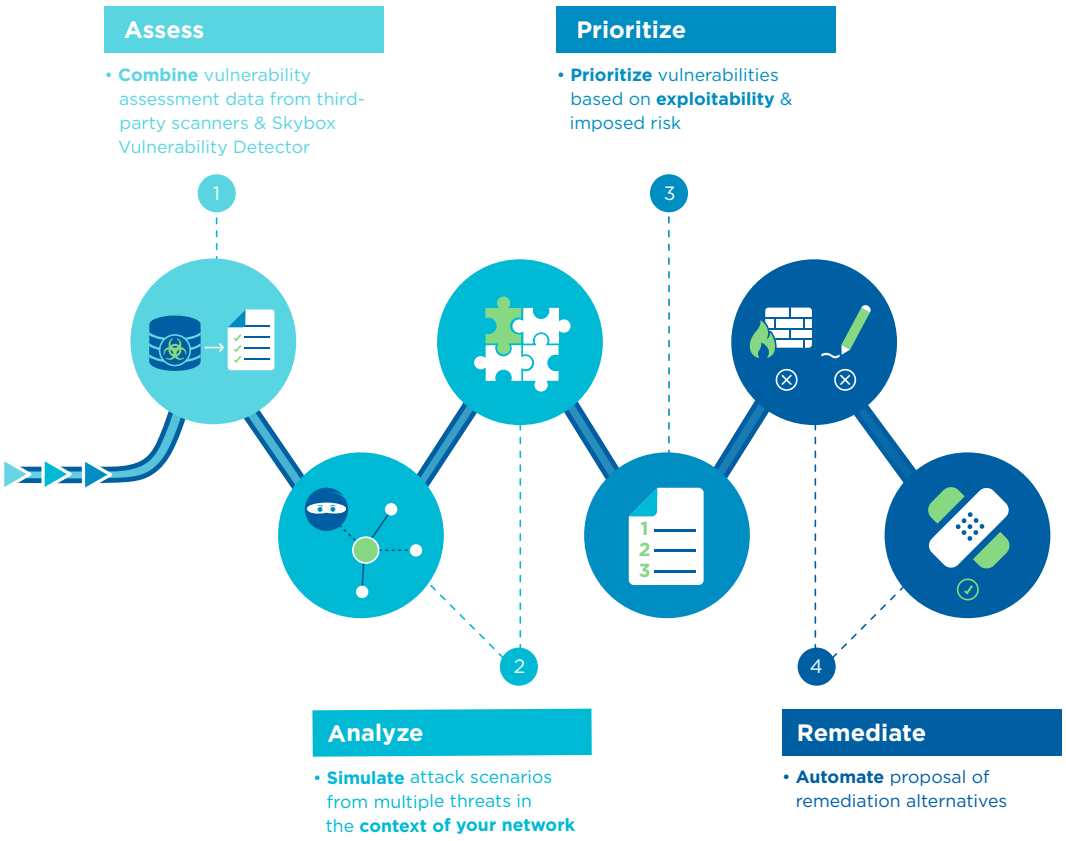
To focus on what counts, your team needs visibility across all exploitable attack vectors. And they need solutions that help them quickly and intelligently respond to the most critical threats.

### Unify Data for a Complete View

Effective vulnerability management starts with comprehensive vulnerability assessment. A mature program will correlate data from multiple scanners and intelligence sources, and use scanless vulnerability assessment technology to reach "unscannable" network devices and systems. Scanless assessment also provides an accurate view of the latest vulnerability risk without waiting for the next scan cycle.

### Enable Context-Aware Prioritization

Prioritizing vulnerabilities is difficult and can be inaccurate if your security team doesn't have a complete understanding of the entire network and what systems are exposed. For example, security controls



such as firewalls and IPS signatures that effectively block a possible exploit can turn high-risk vulnerabilities into a low-risk business priority.

By analyzing vulnerabilities in the context of the network and business, security teams are better able to prioritize what is low and high risk, so they can focus remediation efforts where they are needed most.

## Respond to New Threats Faster

With continuously updated vulnerability data, automated prioritization and full visibility of the attack surface, security teams have the tools they need to gauge business impact and launch a coordinated response in hours, not weeks.

Skybox automates data correlation, integrates vulnerability and threat intelligence feeds and generates prioritized recommendations to trim response and remediation time by as much as 90 percent.

# BUSINESS BENEFITS

### MAXIMIZE EFFICIENCY AND EFFECTIVENESS

- Eliminate manual risk analysis and correlation to focus on remediation
- Create automated, consistent processes for discovery, prioritization and remediation
- Automate vulnerability updates and discoveries without the need for intrusive, active scanning
- Reduce patch management costs by 80 percent or more by eliminating unnecessary patching
- Cut assessment costs by 90 percent by prioritizing risk and response based on potential business impact
- Reduce false positives to near-zero levels

### UPDATE DATA DAILY AND REDUCE RISK EXPOSURE

- Get accurate data more quickly, without the need for an authenticated scan
- Analyze and prioritize vulnerabilities faster to reduce critical risk exposure to less than 24 hours
- Increase ROI of existing investments and improve the effectiveness of IPS by increasing and fine-tuning its utilization
- Proactively reduce the chance of cyberattacks or data breaches which cost an average $3.8 million* per incident

### INCREASE COLLABORATION

- Understand risk levels by organizational or geographical business units
- Maintain a common language and risk-level definition for your entire organization
- Align network, security and vulnerability management teams by showing the interdependencies of vulnerabilities
- Reduce costs of compliance reporting for PCI DSS, FISMA, SOX and other industry regulations

*IBM Cost of Data Breach: http://www-03.ibm.com/security/data-breach/

# Secure Change Management

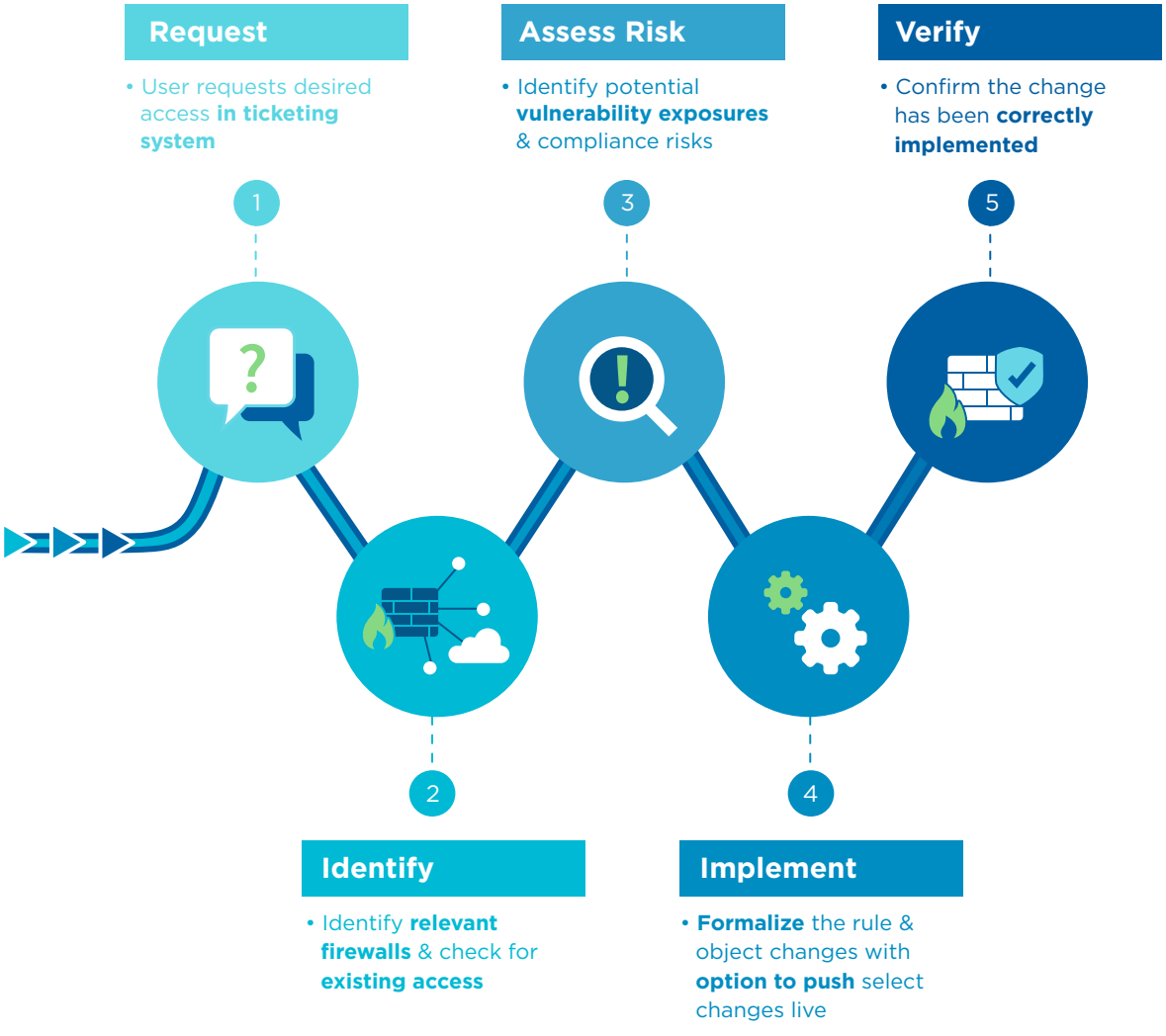
## Ensure Continuous Compliance and Reduce Risks During Network Changes

### Automated Change Management

Your enterprise network changes every day. Users are added, access paths are opened and closed and rules are modified. Every change needs to be recorded, tracked and recertified. This constant flux and the high degree of detail make security management, as well as achieving and maintaining compliance, a huge challenge.

An automated change management workflow, customizable to your organization's needs ensures continuous compliance, increases efficiency and reduces risks associated with manual process errors that could introduce an exploitable security gap.

Skybox brings total network visibility, compliance management and risk analysis to your change management process. With Skybox network modeling,



simulations and analytics, you can assess the risk of proposed changes before they are implemented.

After changes are assessed, the closed-loop workflow also tracks every change from ticket to implementation, verifying that all changes are authorized and made as intended.

Use network modeling and analytics to assess the risk of proposed changes. Track every change from ticket to implementation, verifying that all changes are made as intended.

**ROI provided by customer deployment analysis. Cost savings based on first year of a 150-firewall deployment compared to manual change management costs. Results may vary.*

# BUSINESS BENEFITS

### INCREASE COST SAVINGS

- Save more than $400,000* through automated, intelligent workflows
- Ensure continuous compliance with internal policies and industry and government regulations such as FISMA, SOX and PCI DSS
- Prevent costly errors that can lead to data breaches, downtime and rework
- Avoid time spent on unnecessary changes and identifying firewalls relevant to proposed changes

### REDUCE BUSINESS RISK

- Simulate new access paths on your network model before implementing changes to reduce risk of exposure and downtime
- Identify compliance issues and vulnerability exposures before any changes are made
- Verify that changes are made correctly, preventing unintended access
- Roll out new technology faster with fewer errors through pre–change assessments and automated implementation

### IMPROVE PROCESSES AND WORKFLOWS

- Reduce firewall management time by more than 80 percent
- Reduce the volume of unnecessary changes
- Automate rule recertification to ensure clean, optimized firewalls, minimizing the lifespan of risky rules
- Increase business agility by reducing time to provision new services and access
- Streamline documentation for compliance audits

### IMPROVE COLLABORATION AND COMMUNICATION

- Demonstrate compliance on demand, eliminating tedious, manual processes
- Enable informed decisions and gauge expectations through reporting on how risk is reduced and managed over time
- Reconcile change requests with a streamlined workflow

# Firewall Analysis and Management

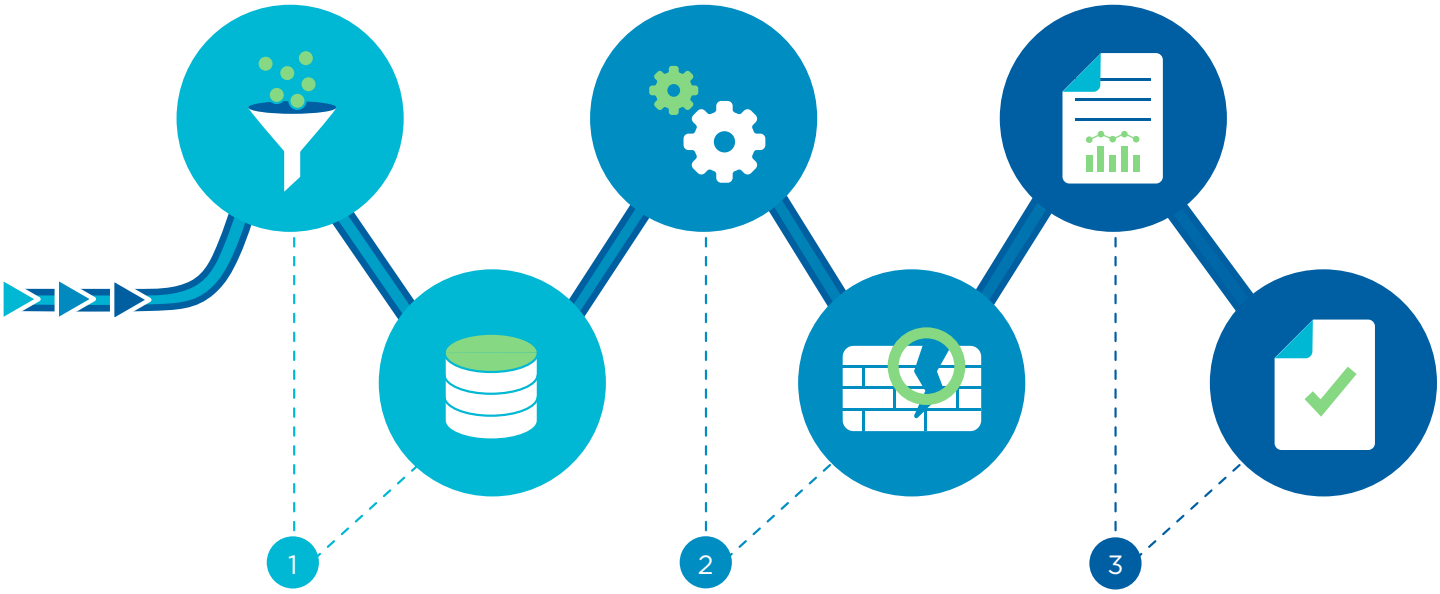
## Validate Firewall Rules and Access Policies With Automated Analytics

### Streamline Firewall Management

Security teams have one priority: to defend the network from attackers. Firewalls have traditionally been the first line of defense, but managing the firewall estate is incredibly complex, time consuming and tedious. Security policies need to be checked and firewalls optimized to ensure access to data and business services is secure. And with the addition of compliance maintenance, audits and incident response tasks, network security teams are constantly overwhelmed.

Skybox streamlines these processes by creating efficiencies in firewall management workflows, as well as automating firewall optimization and compliance tasks. With audit and analysis capabilities, security teams are able to uncover risky access rules and identify allowed and blocked paths throughout your network quickly and accurately.

- Understand and validate firewall rules and access controls; automatically implement access rule changes
- Perform daily network audits to increase security
- Provide audit documentation while ensuring continuous compliance




**Collect & Normalize**

- **Automatically** collect data, log files & security policies
- Normalize for **fast** & **consistent** evaluation

**Analyze**

- **Correlate** config & policy data with best practices
- **Identify** & **prioritize** security & compliance gaps

**Report & Act**

- Unique reports generated for **each stakeholder**
- Enable teams to **optimize** rules & **identify** misconfigurations

# BUSINESS BENEFITS

Skybox creates efficiencies in firewall management workflows by cleaning up messy rulesets and automating firewall optimization and compliance tasks across hybrid IT environments.

### OPTIMIZE COMPLIANCE TASKS

- Get out-of-the-box reporting on industry standards and regulations, including FISMA, PCI DSS, SOX and more
- Narrow the scope of network audits so they cover the smallest network footprint
- View remediation plans to achieve compliance and implement change workflows to maintain compliance

### INCREASE COST SAVINGS

- Save nearly $500,000* when replacing biweekly manual firewall audits with automated analysis
- Reduce compliance costs by up to 90 percent* by replacing manual data collection, analysis and reporting activity with an on-demand, automated process
- Improve network and firewall performance, reducing the need for equipment or capacity upgrades

### TROUBLESHOOT ACCESS ISSUES

- Understand access paths with complete network visibility
- Minimize the time required to find blocked paths
- Analyze the access between various networks and zones

### CLEAN UP AND MANAGE YOUR FIREWALLS

- Evaluate firewall rules for redundancy and shadowing to clean up messy rulesets
- Identify security policy violations
- Automatically implement access rule changes for firewalls
- Manage and visualize physical, virtual and cloud-based firewalls from a single platform

**ROI provided by customer deployment analysis. Cost savings based on first year of a 150-firewall deployment. Results may vary.*

# Context-Aware Network Intelligence

## Save Time and Focus Resources With Security Analytics

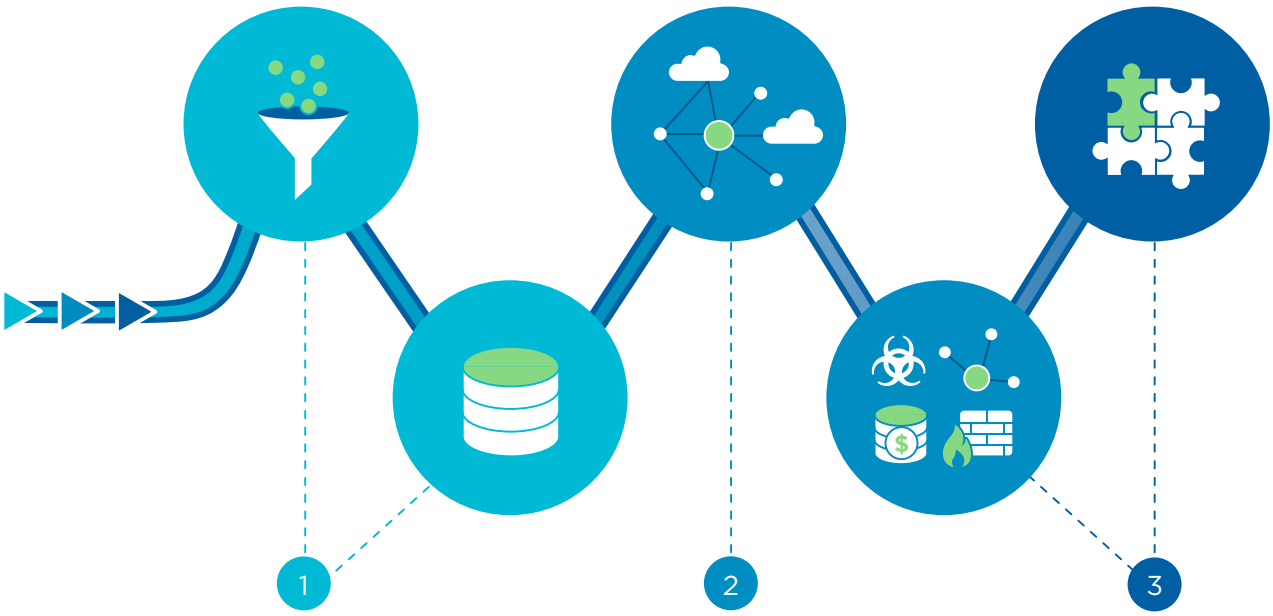
### Fully Secure Your Network With Visualization and Contextual Intelligence

Every network is different. Security policies, procedures, configurations and vulnerabilities all contribute to a constantly evolving, difficult-to-manage network security posture.

Traditional network security management relies on disparate data generated by point solutions. These data silos miss the bigger picture of an enterprise's true state of security. Often, the weaknesses that could lead to attack are based on hidden connections that point solutions can't see or don't understand.

Skybox provides a better picture of an enterprise's true state of security, merging and analyzing comprehensive security data to generate contextual intelligence about your security posture. By viewing your network and security controls holistically across both IT and OT networks, your team has actionable insights to reduce your attack surface and enhance vulnerability and threat management and security policy management programs.

Skybox provides unique modeling and visualization capabilities that reflect the structure of your organization, whether by geographic sites, business units or other logical configurations. The model understands the links and interdependencies between these entities, as well as where vulnerabilities are located on your network, giving you the most comprehensive intelligence on attack vectors threatening your organization.




**Collect & Normalize**

- **Automatically collect** data from all layer three network devices
- Normalize data for **fast** & **consistent** evaluation

**Create Model**

- Create a **holistic, visual model** of your network devices
- Unify **hybrid IT environments** & vulnerability & threat data **in one view**

**Analyze in Context**

- Use the model to troubleshoot device configurations, **analyze access paths** end-to-end & assess compliance **with complete context**

# BUSINESS BENEFITS

### REDUCE RESOURCE BURDEN

- Spend less time correlating data and finding problems and more time resolving them by using analytics–driven intelligence
- Automate processes that are tedious and provide little value, allowing your teams to focus on remediating critical vulnerabilities and security gaps

### MEASURE AND REDUCE RISK

- Visualize the locations, business units or devices most vulnerable to attacks
- Report on your security posture to identify areas in need of improvement or successes to be replicated
- See trends in your security efforts to track progress toward regulatory compliance or best practices
- Triage threat intelligence for weaknesses within the network infrastructure based on likely aggressor tactics

### IMPROVE COLLABORATION

- Provide teams with direction and focus to remediate the most critical vulnerabilities and security gaps
- Use a common language across platforms and pinpoint solutions to normalize information and extract actionable intelligence
- See a complete map of your attack surface and the interconnections of your network
- Utilize comprehensive visibility and modeling for major network infrastructure change planning

Skybox provides a better picture of an enterprise's true state of security, merging and analyzing comprehensive security data to generate contextual intelligence about your security posture.

# Attack Simulation + Virtual Pen Testing

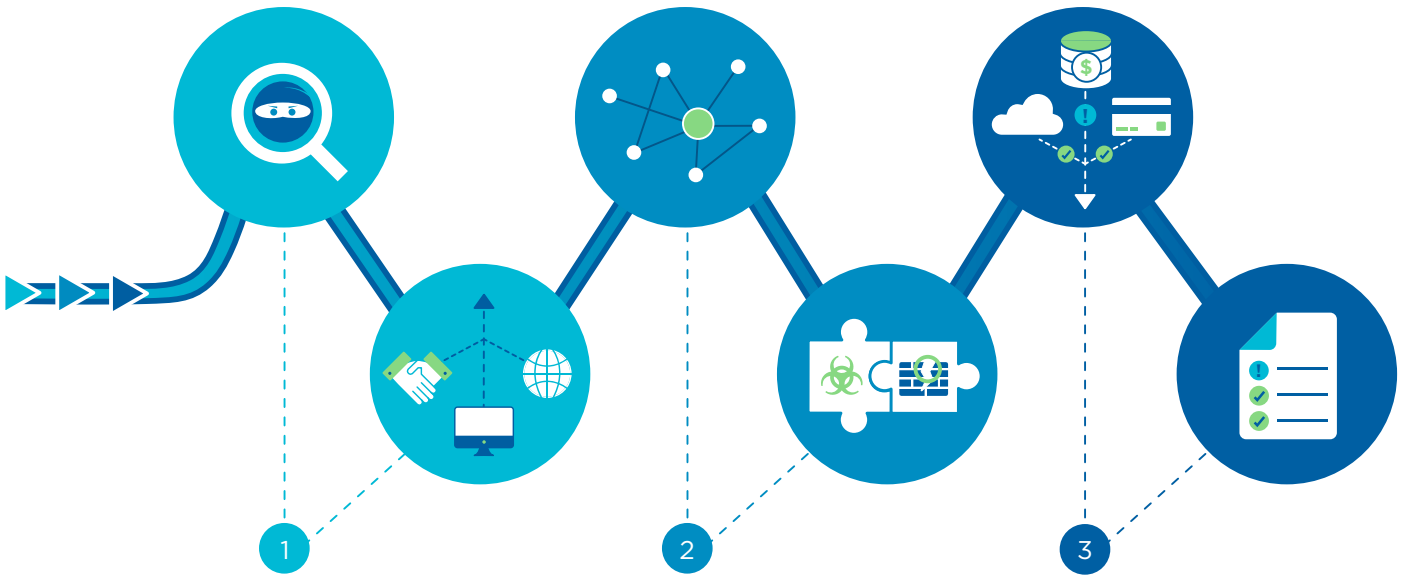
## Find Weaknesses Daily and Automatically

### Non–Disruptive Attack Simulation

Worldwide, organizations are faced with an increasing number of new government and industry regulations for cybersecurity. And many of these regulations mandate the use of penetration testing to ensure compliance. An example of this is the Payment Card Industry Data Security Standard (PCI DSS), which require payment card processing companies to provide documentation and audit results of controls in place for data security, as well as the results of penetration testing.

To meet PCI DSS requirements, organizations have traditionally used a "red team exercise" to systematically conduct exploits and attack scenarios, documenting vulnerabilities, access paths and attack routes discovered along the way. This approach requires extensive resources, cost and time. In addition, it's not scalable because these exercises cannot be conducted across entire networks. And some business services would be disrupted by direct testing, leaving blind spots of risk.

Skybox provides a complementary, automated way to find attack vectors daily using non-disruptive attack simulation. This delivers the benefits and documentation of network penetration testing at a much greater scale and in a fraction of the time. Skybox simulates attack scenarios against a virtual model of your network to validate if the conditions are




**Origin**

- Simulate from **any threat origin**, including endpoints, internet or third-party systems

**Path**

- Simulate all potential attack paths & **exploitable attack vectors** along the way

**Assess & Report**

- Assess security posture of **most critical** assets
- Provide **up-to-date** weakness & vulnerability data & document results of testing

present for exploitation. This provides a comprehensive penetration test, with no impact on your live network.

- Locate potential exposures in new services or after network changes
- Pinpoint specific attack vectors that warrant scrutiny or additional testing
- Perform more frequent penetration tests to check your network for new exploits and vulnerabilities
- Understand where to proactively implement additional security measures

Simulate attack scenarios against a virtual model of your network to validate if the conditions are present for exploitation — it's a comprehensive penetration test with no impact on your live network.

# BUSINESS BENEFITS

### INCREASE COST SAVINGS

- Cut costs of penetration tests or red team exercises in half* and run tests daily
- Save the outsourcing cost for penetration testing
- Avoid potential outages or operational downtime associated with taking production systems offline for live penetration testing
- Reduce audit time and expense by finding potential exposures ahead of an audit

### REDUCE RISKS AND DOCUMENT COMPLIANCE

- Demonstrate regulatory compliance after every major system change or upgrade
- Scale penetration testing from occasional to daily, across any portion or all of your network, without increased expense or management time
- Proactively reduce the chance of a cyberattack or data breach which can cost an average of $3.8M**

### IMPROVE PROCESSES AND WORKFLOWS

- Provide your security teams up-to-date weakness and vulnerability data without network disruption
- Conduct audits and penetration tests anytime, validating there are no new weaknesses in your security infrastructure
- Test critical business services and networks that cannot risk the disruption of a traditional penetration test
- Use attack simulation results to fine-tune SIEM solutions, reducing false positives and manual efforts to configure correlation rules

*On an enterprise network, one-time penetration testing or red team exercises can cost more than $50,000.*

**IBM Cost of Data Breach: http://www-03.ibm.com/security/data-breach/*

## Silicon Valley Headquarters

2077 Gateway Place
Suite 200
San Jose, CA 95110
United States

www.skyboxsecurity.com
info@skyboxsecurity.com


## About Skybox Security

Skybox arms security leaders with a powerful set of integrated security solutions that give unprecedented visibility of the attack surface and key indicators of exposure (IOEs), such as new, exposed or concentrations of vulnerabilities, unsecure device configurations and risky access rules. By extracting actionable intelligence from data using modeling, simulation and analytics, Skybox gives leaders the insight needed to quickly make decisions about how to best address threat exposures that put their organization at risk, increasing operational efficiency by as much as 90 percent. Our award-winning solutions are used by the world's most security–conscious enterprises and government agencies for vulnerability management, threat intelligence management and security policy management, including Forbes Global 2000 enterprises.