SKYBOX® SECURITY

WHY SKYBOX SECURITY
SHOULD BE AT THE HEART OF YOUR

CYBERSECURITY STRATEGY

How, why and where Skybox should form the bedrock of your cybersecurity defences

Whitepaper

Skybox should form the bedrock of your cyber defences.

A Trusted, Military–Grade Security Solution

Since 2002, Skybox has provided trusted solutions to Global 5000 organisations including over 750 major enterprises and governments in 50 countries. Currently, more than one million network devices and ten million network assets are being modelled with Skybox — with the largest installations modelling over 1.5 million assets.

Initially, Skybox focused on security applications in Financial Services (for audit and compliance) and Government & Defence (for situational awareness) — with eight NATO members and almost all the world's largest banks having major deployments. Today Skybox **integrates with over 120 networking and security technologies,** and is used extensively across markets as diverse as Service Providers, Energy & Utilities, Technology, Healthcare and Consumer. Within these markets Skybox adds value wherever security is a strategic concern — from small enterprises to the largest, most complex organisations.

So why are security professionals investing in Skybox, what kinds of challenges are they looking to address, how is Skybox helping them and how could your organisation benefit? This short whitepaper will help you answer all these questions and more, and so explain why Skybox should form the bedrock of your cybersecurity defences.

You Can't Secure What You Can't See

One of the major challenges facing any large organisation is the sheer scale and complexity of its infrastructure. Often this is based on heterogeneous network and IT infrastructure with a myriad of different platforms and software packages, most of which do not communicate with each other. This fragmented situation is made even more complex when parts of the infrastructure are outsourced, virtualised or migrated to the cloud. The result: the organisation simply cannot see what it is trying to defend, making planning an effective defence strategy almost impossible.

In their attempts to deal with this, many organisations have become highly reactive, and have over–invested in security information and event management (SIEM) and other alerting and monitoring tools. These tools are now generating so much data that their security teams don't know where to focus. Typically, their security processes will also have become highly dysfunctional, making organisations less and less able to respond to the rapidly evolving threat landscape. They therefore face a range of interlinked problems including:

- No visibility of their infrastructure and environment
- Disjointed security tools, processes and organisational silos
- A highly reactive approach, undermined by a lack of resource and context
- The proliferation of security 'big security data'
- Difficulties in securing strategic business programs
- Inability to counteract the evolving threat landscape

So how does Skybox enable you to address these complex challenges?

Complete Visibility of Your Infrastructure and Attack Surface

To enable security teams to see exactly what they're trying to defend, Skybox begins by building a model of the organisation's entire infrastructure. Skybox technology uses collection tasks that connect to all relevant components within the infrastructure, and create a model of the environment that can then be used to inform decision making. These components include:

- **Security controls** such as firewall management platforms, intrusion protection systems (IPS) and virtual private networks (VPN), including detailed understanding of their configurations, policies, etc.
- **Network topology** components such as routers, load balancers and switches, including configurations and routing tables. This provides a detailed understanding of the network, such as exactly what access is possible from one part of the infrastructure to another, and all ingress and egress points into the environment.
- **Assets** such as servers, workstations and networks, including how these assets are grouped and their relative importance to the organisation.
- **Vulnerabilities** including their location and criticality. This involves connecting to scanners and patch repositories to provide a daily updated view of all vulnerabilities within the infrastructure, such as insecure internet connections; outsourcers, business partners or suppliers whose security has been compromised; exposed malware, etc.
- **Threat intelligence** including daily updated threat origin and exploit data, including details of the latest vulnerabilities, the availability of exploit kits, and an understanding of which vulnerabilities are actively being exploited in the wild.

Once all this data has been collected and analysed, it is used to generate a visualisation that sits on top of the Skybox model and provides a high–level view of the organisation's attack surface and where all weaknesses are located. These could, for example, include risky firewall rules, exposed vulnerabilities, large concentrations of vulnerabilities for which exploit kits are available, unsecured networking access into the environment.

This view can be aligned in many different ways — by geography, data centre, platform, business service, legal entity — and uses colour coding to represent the different weaknesses and their criticality. Skybox therefore provides your security teams with a single view across your entire infrastructure, so they know where the risks and exposures are, can prioritise those that need to be dealt with and have the information to fix them proactively. Where appropriate, this view can also extend across virtualised, cloud and outsourced environments to provide a level of access and exposure analysis that would otherwise be impossible to create.

Improving and Maturing Your Operational Processes

As well as enabling your security teams to see and act on potential risks and vulnerabilities, Skybox helps to mature multiple existing operational processes by embedding powerful continuous monitoring and analytics capabilities across the entire cycle of predict, prevent, detect and respond.

1

Predict

Skybox exposure analysis, vulnerability assessment, threat intelligence and proactive defence planning help assess vulnerabilities and exposures, simulate attacks and improve baseline systems.

2

Prevent

Skybox network auditing, change management, firewall/IPS management and patch management help harden and isolate systems, divert attackers and proactively reduce the risk of attack.

3

Detect

Skybox improves incident detection and security information and event management (SIEM) tuning, to better detect, confirm, prioritise and contain incidents.

4

Respond

Skybox helps investigation and forensics; design, model, remediate and make changes; and avoid repeat incidents.

Embed powerful continuous monitoring and analytics capabilities

Examples of the kinds of operational processes that you can improve using the objective central reference model provided by Skybox include:

- Automating firewall and network device auditing, and ensuring, for example, that your security teams know which IPS signatures need to be turned on to prevent serious attacks.
- Managing infrastructure changes to reduce cost, maintain compliance and ensure the changes being made aren't impacting the integrity of your environment.
- Improving vulnerability management by bringing consistency and objectivity to the high volumes of data being produced by vulnerability scanners, and enabling your security teams to properly assess risk, prioritise remediation, understand the options available and track remediation via workflow and service level agreements (SLAs).
- Providing context for the correlation rules used by detection tools such as SIEM by describing where exposed assets and exploitable attack paths are located, and enabling SIEM to be tuned to generate a much smaller number of high–severity alerts that are genuinely risky for your organisation.
- Improving incident response by helping you plan response and containment; giving home advantage to your security teams by enabling them to make informed decisions about how to block exfiltration of data and contain malware outbreaks; and providing forensic analysis of breaches that may have occurred in the past.

In addition, Skybox integrates with and complements over 120 technologies across firewall, network security, infrastructure, vulnerability management, SIEM, endpoint security, patch management and cloud environments. Historically, many of these tools have been purchased primarily for compliance purposes and have been very difficult to deploy and tune. But by transforming data into contextual intelligence and understanding of your organisation's attack surface, Skybox helps **drive value** from these investments, and also makes **future planned investments** much easier to embed operationally.

Supporting Your Strategic Initiatives

As well as giving you complete visibility of your infrastructure and attack surface, and helping you improve and mature your operational processes over time, Skybox gives you a solid platform on which to plan, execute and securely enable a wide range of strategic initiatives.

Cloud Enablement and Digital Transformation

Cloud enablement presents many risks and challenges, for which Skybox is being used to create an architectural blueprint for the adoption of cloud or virtualisation capabilities. This is because Skybox:

- Provides unparalleled visibility into the cloud.
- Allows organisations to bridge and extend their existing processes into the cloud, rather than having to introduce new technologies, new processes, and new ways of managing security, risk and compliance in the cloud environment.
- Helps them plan the migration of infrastructure and applications into the cloud, and do this in a secure way.
- Enables security teams to understand the risks of virtualisation and cloud migration on a day–to–day basis, so they can plug any gaps as they appear.

Security Transformation

The first step of any security program should involve a detailed understanding of the attack surface, for which Skybox enables a common sense approach with fast risk reduction. Skybox is being deployed at the start of many security transformation programs because it enables organisations to:

- Understand what they're trying to defend.
- Quickly fix the high risks within their environment, and report this risk reduction to key stakeholders.
- Mature their existing processes in areas such as change management, patch management and compliance.
- Create a solid foundation for more advanced use cases such as SIEM, a security operations centre (SOC), outsourcing to a managed security service provider (MSSP), etc.

Audit and Compliance

Compliance and meeting regulatory requirements is a minimum expectation for any organisation. Skybox helps embed compliance management within normal day–to–day operations by:

- Automating, evolving and streamlining critical processes, including maintaining compliance as part of the process.
- Automating and aligning audit processes, compliance and policy management across the network, including tracking exceptions and fixing any potential violations.

Digital Resilience

Digital resilience can be greatly improved by managing cyber hygiene. Skybox helps to manage and mature the basic processes that maintain cyber hygiene and resilience on a day–to–day basis. This delivers significant improvements over traditional approaches, such as annual or bi–annual audits followed by intense periods of activity to fix the problems identified, but which are based on data that is often out of date.

Securing Operational Technology

Securing supervisory control and data acquisition (SCADA) and operational technology (OT) infrastructure presents many unique challenges. Skybox enables a proactive, non-intrusive means of managing risks within SCADA and OT environments, by modelling the risks that exist between a traditional IT environment and OT, and using this model to extend and join the processes being used within both environments.

Mergers, Acquisitions and Divestments

M&A and divestments present significant security and operational risks. Skybox enables the technology aspects of M&A to be concluded more quickly, and helps to de-risk their operational aspects by:

- Ensuring risks associated with the merger or acquisition target are properly understood.
- Identifying where those risks are and enabling them to be mitigated.
- Helping to plan how the two organisations' networking infrastructures will be combined.
- Saving considerable time compared to traditional manual processes, which will themselves typically be based on audit data that is quickly out of date.
- Enabling the organisation to realise significant business and commercial value more quickly than would otherwise be possible.

Similarly, for divestments, Skybox helps organisations understand and plan how network infrastructure can be segregated quickly and appropriately.

De-Risking Outsourced Environments

Within heavily outsourced environments, accountability is never fully outsourced, and so complete visibility of all assets is essential. Skybox is being used to police outsourced environments by giving total visibility of the complete attack surface; a single view across all infrastructure where multiple outsourcers are involved; and ensuring mature processes are in place between the organisation and outsourcers. This includes bringing consistency and maturity to processes such as security operations and managing changes and vulnerabilities, and 'baking' Skybox into contractual arrangements with outsourcers.

Automation and Orchestration

Skybox can help overcome resource shortages, improve process efficiency and reduce risk with analytics–driven automation that leverages complete visibility of your environment and the contextual intelligence of the attack surface. Skybox automates and orchestrates a variety of security management processes including:

- Data collection, normalization and modelling to give you merged, centralized data respositories and on-demand visibility to your attack surface.
- Security posture assessment to clean and optimize firewalls, spot policy violations, misconfigurations, etc.
- Vulnerability assessment and analysis to scanlessly discover vulnerabilities, simulate attacks and accurately prioritise remediation.
- SIEM data contextualization and incident resonse planning.
- Change management workflows to ensure firewall rule changes don't introduce new risk and existing rules are continuously monitored.

Key Benefits for Your Organisation

Whichever of these use cases you need to deliver, Skybox will help you optimise results by:

- Creating a central model of your organisation's entire infrastructure that can be used to join and de–risk processes across disparate technologies, regardless of how these are managed (e.g., in–house, outsourced, cloud).
- Embedding analytics within your existing processes, automating and reducing organisational overhead, while at the same time improving your security posture and resilience.
- Automating many important processes such as auditing, change management, vulnerability management and security operations.
- Providing context to security monitoring tools and within incident response processes, thereby allowing a reduction in resources.
- Enabling strategic initiatives such as cloud adoption, digital transformation, mergers and acquisitions, divestments, outsourcing, automation and compliance.

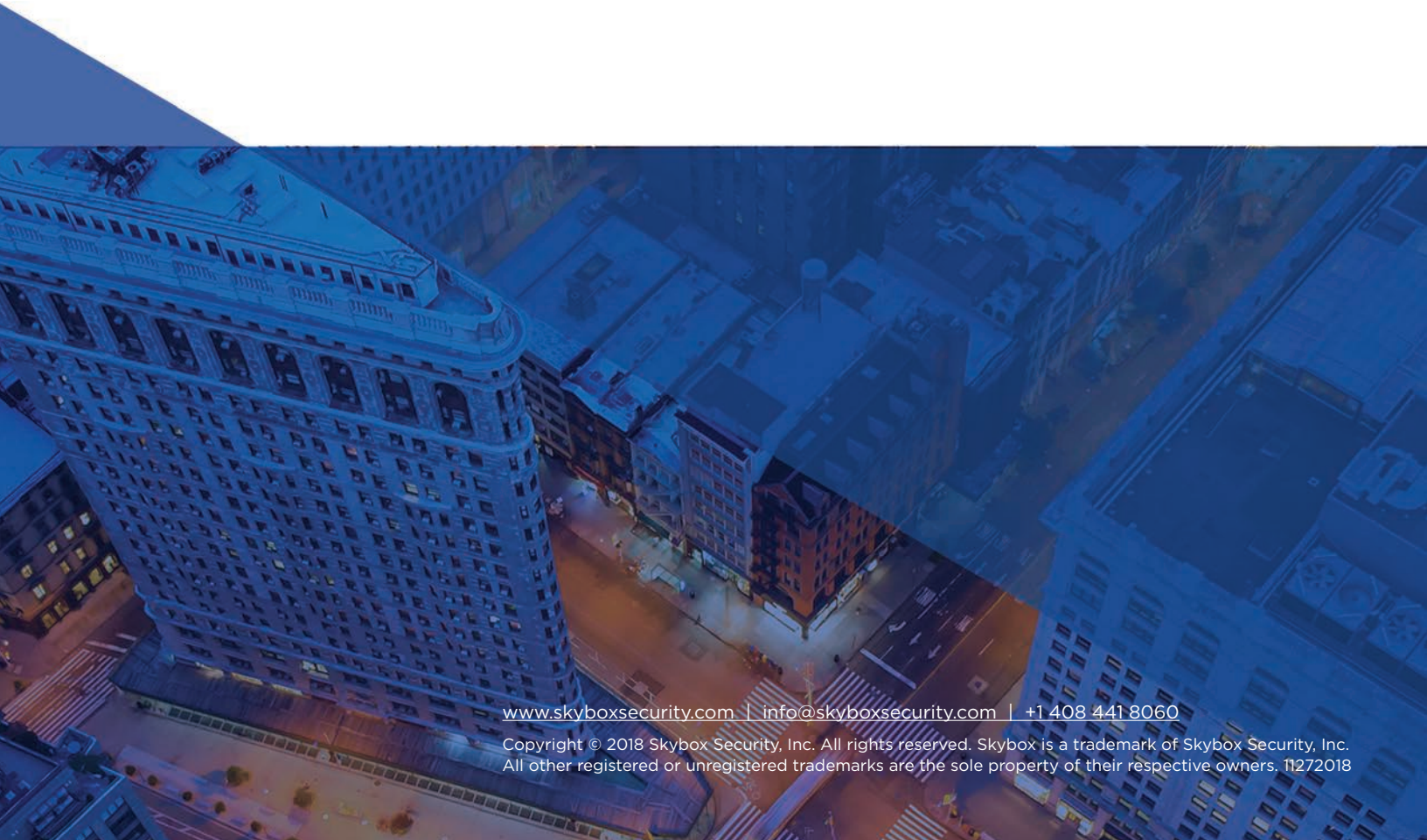
Embed analytics within your existing processes, automating and reducing organisational overhead

Where to Start?

Skybox arms security leaders with a powerful set of integrated security management solutions that give unprecedented visibility of the attack surface and key indicators of exposure (IOEs), such as exposed vulnerabilities or with active or available exploits, unsecure device configurations and risky access rules.

By extracting actionable intelligence from data using modelling, simulation and analytics, Skybox gives leaders the insight needed to quickly make decisions about how best to address threat exposures that put their organisation at risk, increasing operational efficiency by as much as 90 percent. Skybox's 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.

To find out more about how Skybox can form the bedrock for your cybersecurity strategy, please visit our **website**.



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

Copyright © 2018 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc.
All other registered or unregistered trademarks are the sole property of their respective owners. 11272018