SKYBOX SECURITY

SKYBOX FOR CLOUD
Extending and unifying security management in hybrid networks

WHITEPAPER
Digital transformation is accelerating across industries, and most organizations are migrating applications and workloads into the cloud at a rapid pace. Meanwhile, IT and security teams are now faced with increased management and operational challenges that are adding to overall business risk. Hybrid and multi-cloud deployments are opening up new cybersecurity challenges where inconsistent levels of visibility, misconfigurations and deployment of uncertified policies are all becoming more prevalent.

Cloud migrations are driving a myriad of pain points — thus driving security operations teams to adopt new approaches and more effective management tools.

**CLOUD SECURITY CHALLENGES**

**Security and Control**

Ubiquitous access to cloud technology provides an unchecked ability for shadow IT personnel to “spin up” arbitrary or rogue cloud assets. This typically occurs outside the control of corporate IT and security operations, and it happens without complying to necessary security policies. Security risks and exposure are typically underestimated in the rush to virtualize workloads and where cloud security considerations are often bypassed. These circumstances make it difficult to understand how policies are being enforced, what risks are present and, simply, what’s even deployed in the cloud.

**Siloes**

Siloes present another issue. Besides departmental siloes within the corporate structure such as finance, marketing and sales, siloes are also prone to exist between traditional IT and security operations. With deployments of multiple security point solutions and different workloads across competing cloud platforms such as AWS, Azure and Google Cloud, siloes have developed between teams managing the applications and teams managing various different tools.

**Complexity**

IT departments are overwhelmed with complexities trying to manage the ever-increasing mix of technologies and multi-vendor corporate assets being deployed across hybrid and multi-cloud networks. These disparate technologies can be hard to synchronize and secure from a single control point. Managing deployments across multi-cloud environments can get very complicated very quickly. Maintaining a consistent security posture between dynamic virtual environments and existing physical infrastructure is increasingly more difficult.

**Insufficient Visibility**

The diversity of cloud architectures makes visibility across deployments extremely difficult. Gaining visibility inside cloud networks is crucial for security teams to fully understand and manage security risks across physical IT and multi-cloud environments, and to ensure that compliance and consistent policies are applied.

**Poor Vulnerability Management**

Identifying and managing vulnerabilities is a challenge for security teams, especially when certain cloud environments don’t allow external scanning. However, vulnerabilities within these environments still contribute to overall risk levels. It is essential for security teams to be able to address exploitable vulnerabilities within cloud environments so that they can prevent exploits from undermining integrity of cloud services.

**Policy Management and Compliance**

Misconfigurations and violations are the greatest risk when deploying applications and services in the cloud. The devops teams often underestimate security requirements within different cloud environments, and organizations end up assuming more and more risk as virtual assets are added.

Security configuration settings, techniques and tools also vary significantly across different cloud networks. This scenario makes it very challenging to incorporate policy changes and certify accuracy, consistency, and continuous compliance.
SKYBOX SOLUTION

Skybox enables enterprises to transform their security operations with critical security management capabilities that will enable you to:

• Maintain consistent levels of visibility and control as your organization adopts new technologies and expands across hybrid and multi-cloud domains

• Confidently and securely expand your networks and adoption of new technologies to ensure your business can maximize profitability

• Continually and efficiently optimize the effectiveness of your security operations, resources and technologies to maximize your overall return on cybersecurity investments

Our unique platform starts by creating a network model, pulling in data from network devices, security controls, compliance policies, vulnerability scan data and threat intelligence. Skybox aggregates millions of datapoints from these sources, analyzes them from multiple perspectives and provides clear and actionable insights for your organization. With this foundation, the platform enables:

• Automation of security processes and workflows to keep up with the faster pace of changes in virtual and cloud networks

• Consolidation of data silos from diverse network environments for better security visibility, context, prioritization and control

• Unification and simplification of processes to manage vulnerabilities, threats and security policies across your entire organization — in a single dashboard view

• Extension of security and compliance assessments across physical, virtual and multi-cloud environments

Visibility With Context and Dynamic Modeling

Security depends on attaining complete visibility with a continuous reduction of your attack surface. Being able to aggregate relevant and comprehensive data to go along with the application of prescriptive analytics is key so you can effectively and efficiently apply a strong and consistent security posture while addressing security risks and vulnerabilities. Cloud migrations have made this more challenging than ever.

With Skybox, enterprises can gain unprecedented levels of visualization and characterization of deployments and assets across hybrid, multi-cloud and OT networks. The platform leverages multi-source aggregation of data from multiple technologies and sources; this information is built into a comprehensive and dynamic model of your network. An automatically updated model is crucial for maintaining visibility, control and compliance as your organization expands and deploys new technologies and services across hybrid and multi-cloud domains.

With more than 140 technology integrations, the Skybox platform collects and aggregates detailed data from different networking, cloud and security technologies from across all the major cloud...
service providers, such as Amazon Web Services, Microsoft Azure and Google Cloud. Skybox incorporates a broad range of an organization’s data sources (e.g., from endpoints, firewalls, routers, virtual machines, containers, access control lists, VPN connections, group and virtual machine security tags, vulnerabilities, patch management and CMDBs) as well as threat intelligence.

The continuously collected, modeled data provides the foundation for unified and continuous analysis of entire IT infrastructures and security postures; and it assures that assets — physical or virtual — can be accurately monitored, secured and decommissioned when not in use.

In addition to data gathered from the vast number of network and security technologies, the Skybox visualization model pulls in data from all the major scanning technologies and gathers the following data points from cloud environments:

- Gateways (virtual private cloud connections; internet gateway; customer gateway)
- Firewalls
- Routers (route tables)
- Access control lists
- Network address translation (NAT)
- Elastic load balancing (ELB)
- Subnets
- Security groups
- Assets (virtual machines)
- Containers
- Vulnerabilities
- Data from dozens of threat sources including the dark web

Customized Views and Workflows

Skybox’s customized views, dashboards and filters let you focus on what matters most to you, highlighting risky access rules, vulnerability exposures and compliance risk. Skybox for Cloud ensures that network and security visibility is extended beyond your physical network and across your multi-cloud environments.

Our comprehensive network modeling and advanced security analytics provides invaluable insight into cloud environments and unifies security policy management throughout your hybrid network. Within a single view, the model can uniquely identify vulnerabilities and risk of a breach. It can also be used to underpin processes that require a thorough understanding of your entire IT infrastructure.

The Skybox network map provides a complete visual representation of your hybrid infrastructure — public and private clouds, geographic locations, OT networks and physical assets. Skybox also provides visibility down to the container level to ensure security of cloud services.

Skybox displays network and application connectivity across on-premises and multi-cloud environments with end-to-end access analysis and detailed path information — from any source to destination. This enables organizations to monitor

FIG 1: Skybox dashboard can help to focus on cloud assets and cloud infrastructure. Skybox provides many fully customizable widgets that can be configured to meet the needs of security operations. Every dashboard can also be saved and exported as a report.
and troubleshoot connectivity issues throughout the network.

- Shows connectivity across and within physical, virtual and multi-cloud networks
- Gathers information on the access route, including details on security groups accessed
- Performs ad hoc queries showing connectivity for applications between any source and destination, including detailed path analysis on the devices, rules, etc. along the path

Risk-Based Vulnerability Management

While cloud migrations continue to provide enormous business value to organizations, the flexibility, rapid replication and scalability of cloud assets is also exponentially increasing the proliferation of vulnerabilities. Auto scaling, cloud image duplication and deployment of containers all have potential to increase risk exposure for enterprises if vulnerability management capabilities are lacking.

Scanless vulnerability discovery combined with traditional scanning overcomes challenges of identifying vulnerabilities in virtual and multi-cloud environments. Skybox helps to fill in scanner blind spots with on-demand scanless assessment. We pull data from many sources — major scanners (Qualys, Tenable and Rapid7), container management tools such as Twistlock, cloud API/infrastructure, and cloud-native security services such as Zscaler. This data becomes centralized and organized within Skybox, eliminating the need to

FIG 3: Vulnerability Control has completely customizable dashboards that can be configured to meet the needs of any organization. The dashboards can be organized as a workflow, allowing analysts to systematically remediate each exposure or exploit; the left side of this screen shows exposures and the right-side show exploits.

FIG 2: Skybox Vulnerability Control can provide a prioritized view of all the highest to lowest risks.
use multiple tools and means to collect, rationalize and normalize the data.

The Skybox vulnerability occurrence list is updated daily by a team of security analysts, and the threat feed is downloaded into the product daily using an automated task. This threat data is compiled from dozens of public and private security sources, plus insight to the dark web.

In vulnerability prioritization, Skybox takes into account which systems are mission critical and high risk, which vulnerabilities have known exploits in the wild, and which are exposed in the network. A single customizable dashboard displays all vulnerabilities occurrences in your entire environment and offers detailed drilldowns into vulnerabilities across the entire hybrid network. This context is then used to enable a mature and well-orchestrated vulnerability management process.

Skybox also provides a completely flexible risk scoring solution which can be configured based on the risk value of each asset as determined during the prioritization analysis.

**Unified Policy Management**

Skybox unifies security policy management — viewing, maintaining and controlling security policy — across hybrid and multi-cloud networks. Skybox normalizes security tags from private and public cloud networks and combines this information with data from physical networks. This synthesized data is provides in a customizable, single dashboard view of an organization’s overall compliance posture for internal standards, best practices and industry regulations.

Using the Skybox model and automated access analysis, Skybox for Cloud quickly assesses network and application connectivity, access rules, compliance and security policy information along any north-south or east-west path on the network. These include paths across physical IT, multi-cloud environments (down to container level) and OT networks, as well as within a single network such as a specific cloud environment. This analysis can then be embedded within the change process to speed up change with reduced risk of outages.

Skybox provides rule, access analysis and configuration policy management. Rule analysis is available for AWS and Zscaler and Azure Firewall. Skybox also provides comprehensive policy management, assessing enforcement against security baselines, external regulatory mandates and internal corporate policies.

**Skybox unifies, normalizes, improves and rationalizes policy management across your increasingly complex infrastructure.**
Compliance Policy Visibility

Skybox for Cloud provides a single dashboard view of your entire network compliance and security posture for internal standards, best practices and industry regulations such as PCI DSS, NERC CIP, SOX and EU GDPR. It enables the creation of consistent policies and compliance across physical and cloud environments and provides immediate visibility into new instances and assets spun up and down in cloud networks.

De-Risked Transitions

Skybox gives visibility of the risks and indicators of exposure being introduced to the environment during a transition to the cloud. High-risk vulnerabilities, misconfigured devices and exploitable attack paths are highlighted, allowing security teams to proactively mitigate risks while the business pushes ahead with the transition.

Consistent, Mature Security Processes

With Skybox, CISOs can immediately extend a wide range of operational security processes to cover new environments as they come online. Operational processes such as incident response, monitoring, proactive defense planning, change management and vulnerability management can all benefit from increased visibility and context to evolve maturity and extend coverage to cloud and virtual infrastructures.

FIG 3: Skybox Network Assurance can query to analyze access between a source and a destination within the network map. By simply selecting one asset as “source” and another as “destination,” the route between the two can be analyzed.

FIG 4: The results of the access analysis and details of the security controls along the path shows there is no access between the two selected assets.
SECURE DIGITAL TRANSFORMATION

Skybox provides benefits to your digital transformation initiatives and security operations by:

• Assisting with the planning and modeling of multi-cloud migrations and transitions to ensure successful deployments while minimizing business risk

• Centralizing management and visibility across hybrid and multi-cloud environments

• Optimizing security operations, resources and hybrid/multi-cloud technologies to continuously minimize an organization’s attack surface and maximize the overall return on their cybersecurity investments

ABOUT SKYBOX SECURITY

At Skybox Security, we provide you with cybersecurity management solutions to help your business innovate rapidly and with confidence. We get to the root of cybersecurity issues, giving you better visibility, context and automation across a variety of use cases. By integrating data, delivering new insights and unifying processes, you’re able to control security without restricting business agility. Skybox’s comprehensive solution unites different security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level. With obstacles and complexities removed, you can stay informed, work smarter and drive your business forward, faster.