AUTOMATING

# AUDIT AND COMPLIANCE

## WITH SKYBOX SECURITY

Business Brief

### Save Time and Resource by up to 80 Percent

Financial services, health, federal agencies and other regulated organizations face significant challenges complying with standards such as HIPAA, SOX, DISA, FISMA, PCI–DSS, ISO 27001 and EU GDPR. PCI requirements, for example, span every aspect of IT infrastructure and application and data security.

Financial and legal penalties for non–compliance are steep, and the resources and time required to meet and maintain compliance can be overwhelming for many organizations.

The Skybox® Security Suite automates compliance management, helping to implement organizational processes across your entire infrastructure for continuous compliance monitoring and maintenance.

With Skybox, you are able to eliminate errors and violations and ensure an effective compliance strategy with minimal IT resource requirements.

"In the financial sector, maintaining compliance is mandatory. There are many regulations that we have to follow, and Skybox enables us to deliver on–demand reports to our auditors that prove that we're compliant. The solution also allows auditors to validate results against our baselines, and baseline comparisons are critical to proving that our networks are secure."

*— Director of IT Security, High–Tech Commercial Bank*

SKYBOX® SECURITY | FORESIGHT® CYBER

## Compliance Auditing Challenges

### Regional and Industry Regulations

These include PCI–DSS, HIPAA, EU GDPR and NERC, among others, which are often complex and continually evolving. Multinational organizations may have to comply with multiple regional regulations that differ and may even conflict.

### Internal Organizational Policies

Most organizations have to comply with internal security policies in addition to external regulatory requirements. Compliance management must extend across both, avoiding conflicts and wasted resources.

### IT Complexity and New Technologies

Many organizations have applications and data residing on–premises and in private, public or multi–cloud networks. Visibility across all these environments can be a challenge for organizations struggling to understand just their physical networks. Cloud networks and security often work differently from on–prem equivalents, and holistic visibility is complicated by the variety of management tools, each covering a small slice of the overall infrastructure. Rarely do these tools work together.

### Resources and Skills Gaps

Managing and maintaining compliance across environments and regions can take up time and resources desperately needed for the strategic security initiatives, new technology implementation and digital transformation that today's businesses demand. Compliance and security expertise is in short supply, leaving many organizations struggling to tackle compliance effectively across their infrastructure while, at the same time, managing the resilience of their infrastructure.

### Shifting Threat Landscape

Organizations must manage compliance in the context of a continuously changing threat landscape. This requires identifying and tackling the new threats most likely to affect their IT environment and compliance posture.

## SKYBOX® SECURITY SUITE

- Unify management of internal and external policies
- Automate workflows and processes to maintain compliance
- Reduce violations gaps in compliance
- Quickly Identify and reduce risks due to vulnerabilities across on–prem, cloud and OT networks
- Reduced network change risks
- Automate audits and reporting

## Solving the Challenges

The Skybox Security Suite automates processes that maintain compliance, helping organizations to fill in resource gaps and comply with internal and external policies across physical and multi–cloud environments. Skybox helps tackle challenges such as:

**Understanding Internal and External Compliance Policies**

Skybox comes with out–of–the–box policy templates for external regulations, standards and best practices such as PCI–DSS, NERC, NIST, STIG and CIS Benchmarks. In addition, Skybox also allows customers to configure custom internal policies so that these can also be managed.

As well as network configuration policy audits, Skybox helps meet compliance obligations in the areas of network perimeter visibility, access and vulnerability management.

**Achieving A Holistic View**

Skybox automatically pulls together and normalizes information from more than 120 networking and security technologies. This creates a detailed, holistic model of your entire attack surface, spanning on-prem, multi–cloud and operational technology (OT) environments.

Skybox's powerful analytics deliver the context and foundation necessary for automating and maintaining compliance as you make changes to accommodate new users, technologies and business functions. With Skybox, you achieve a queryable infrastructure that will help you to understand exactly where and how a change (or threat) might affect your compliance posture before it is implemented.

**Streamlining Compliance Processes**

Skybox automates essential compliance functions, such as firewall and network device optimisation and compliance checks across internal and external policies. Audit and compliance reporting tasks are automated and run on a scheduled basis with reports being sent to relevant staff with executive visibility being provided via dashboards or export of data to relevant platforms.

Automated workflows and fast analytics streamline processes that can have an impact on compliance, such as change and vulnerability management, so that compliance can be maintained on a day–to–day basis.

Violations and exceptions are also managed via workflow and violations management capability.

Skybox eliminates gaps and blind spots such as vulnerabilities on un-scannable network devices and zones, leveraging multiple sources to ensure the most complete and up–to–date view of vulnerability data possible, extending well beyond vulnerability scanners.

**Managing Vulnerabilities**

Vulnerability management is an essential component of any compliance strategy. Skybox threat–centric vulnerability management (TCVM) approach integrates vulnerability management with compliance automation by:

- Centralizing vulnerability discovery results across on–prem, multi–cloud and OT environments
- Prioritizing the vulnerabilities and threats relevant to your specific business and IT environment — and known to be active in the wild
- Simulating attacks on your specific network model to identify your real–world risk of exposure
- Recommending effective, less disruptive alternatives to typical remediation measures such as patching or updates, which can cause downtime

**Reducing Change Risk**

Skybox analyzes proposed infrastructure, firewall and access changes to ensure they have no negative impact on compliance or introduce new vulnerability exposures. The analytics compare actual changes to proposed changes to ensure they were made correctly and with the relevant approvals.

**Eliminating Violations**

Skybox reviews firewall, cloud and infrastructure configurations and alerts IT to any internal or external policy violations.

"We engaged with Skybox to address several audit and compliance concerns. The support we received was exemplary, allowing for a quick, effective deployment.

Skybox provides us with a 360–degree view of our network, giving us an instant view of our compliance levels against major information security standards, together with a risk–based prioritisation of our cross–corporation vulnerabilities. Skybox has simplified our network device change management processes to such an extent that we are moving entirely to a Skybox– centric system — this helps us to maintain a stable, secure network, and retain all of the configuration information everywhere in that network."

— Director of IS Operations, Clinical and Lab Services Corporation

## WHERE TO START

To find out more about how Skybox's automation will improve your compliance and auditing processes, **visit our website.**

For further reading, download the whitepaper, ***Automated Security Management: Increasing Efficiency and Reducing Risk With Visibility, Context and Automation.***

## Key Business Benefits

- **Enable continuous compliance status visibility via reporting and dashboards** aligned to both external regulatory requirements and internal policies
- **Reduced risk of violations,** avoiding the high costs associated with regulatory fines and lawsuits
- **Easier, less costly compliance audits and reporting** thanks to automated compliance analysis, tracking and reporting
- **Resource savings of up to 80 percent**, allowing organizations to focus IT resources on strategic initiatives that benefit the business
- **Mature, compliance-aware processes** allowing compliance to be managed as part of day-to-day operations
- **Enhanced business agility** with less time required for provisioning new services and access while remaining compliant
- **Flexibility** to meet future, as yet unknown, compliance and regulatory requirements

## Contact US

Foresight Cyber Ltd
Universal House, Suite 3
56-58 Clarence Street
Kingston upon Thames
KT1 1NP
United Kingdom
+442071839858
info@foresightcyber.com
www.foresightcyber.com

## About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

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