SKYBOX SECURITY

Automate security change management with network context

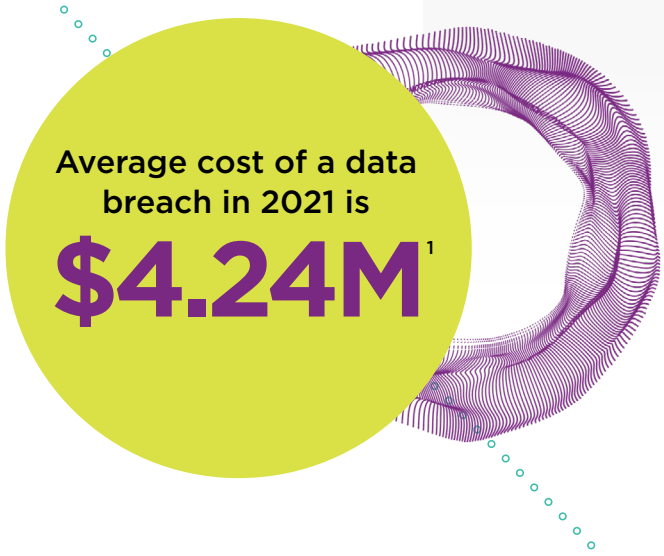
Gain understanding across your attack surface to assess rule and policy changes before making them, spot misconfigurations, and identify vulnerability exposures

Challenges

The sheer volume of security change management tasks to manage can be overwhelming for organizations of any size. Multiple vendors and disparate technologies make change management, rule recertification, and audit management difficult and resource intensive. But without sufficient validation, any proposed configuration changes can lead to exposed vulnerabilities and a potential security breach. Focus your limited resources on the highest priority tasks and reduce the chance of errors by ensuring proposed changes are compliant before they take effect.

Risk factors

- **Multiple vendors for network and security systems**
- **Complex IT, OT, and multi-cloud infrastructures**
- **Audit, compliance, and rule recertification requirements**
- **Limited resources and tight SLA requirements**
- **Too many priorities and not enough context for decision making**



[1] Cost of a Data Breach Report 2021, IBM and Ponemon Institute

What's needed

Automated, context-aware change management

Save time and money and increase your security efficacy by centralizing and automating your change management workflows.

Context where it matters most

Conduct path analysis and gain context from your hybrid network. Use this insight to model changes before implementation and avoid opening your network to bad actors.

More confidence in less time

Automate your workflows across multiple vendors and technologies. Gain efficiency while simultaneously limiting your exposure risk and ensuring compliance objectives are achieved.

Outcomes

+ Gain visibility and understanding across your attack surface
+ Model and validate changes before implementation
+ Identify potential vulnerability exposures and prevent potential exploits
+ Meet compliance requirements and avoid hidden costs
+ Automate rule recertification processes
+ Integrate with existing ITSM ticketing systems

Why Skybox?

Skybox Change Manager automates change management workflows so organizations can optimize their resources, technologies, and processes to achieve more comprehensive risk assessments, reduced errors, and faster response times.

Identify and trace

Aggregate all business, policy, and configuration requirements. Ensure accurate path identification in NAT-rich environments. See options for full access routes and details of changes at each step.

Assess and manage risk

Discover if proposed firewall rule changes could expose previously protected vulnerable assets, create security gaps, or violate policies. Integrate with existing ticketing systems to centralize and formalize change requests and comply with audit requirements. Assign metadata to create rules including rule owner, review date, and other details.

Detect and protect

Manage and automate workflows for firewall rule creation, change verification, rule recertification, and deprovisioning. Easily review rules for recertification or deprovisioning to keep firewalls clean, secure, and compliant. Validate rules and reduce rollbacks and unnecessary changes with proactive assessments.

Contact an expert

Schedule a demo ···>

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.