E-BOOK

SKYBOX SECURITY

Smart Automation

For Security Policy Management

The problem

Most security breaches today are not the result of zero-day attacks but the exploitation of security issues such as misconfigured firewalls, weak security controls, and ineffective vulnerability management strategies.

The problem lies in the security management gap — the deficit between what you need to do and the resources you have to do it.

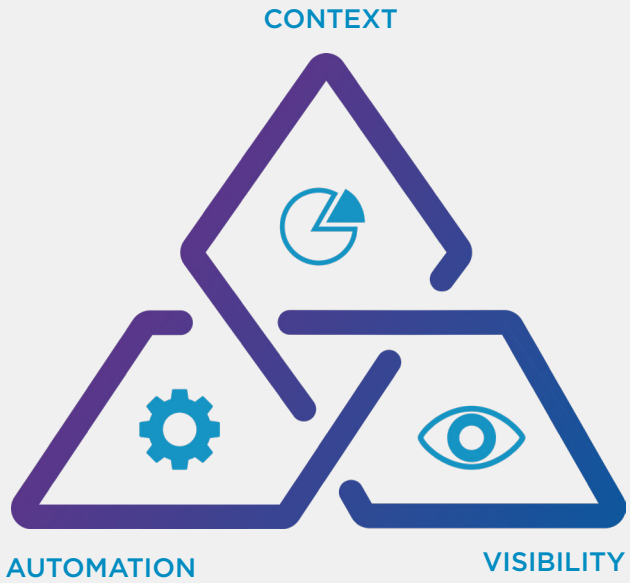
RESPONSIBILITIES	GAP	REALITY
Control a growing attack surface encompassing hybrid network infrastructure and assets.		Lack of visibility of what it is you're trying to protect and from what.
Make sense of data from disparate technologies, multi-vendor solutions, and disconnected processes and teams.	**Attack vectors** **Compliance violations** **Errors** **Data breaches**	Siloed data on a massive scale without actionable intelligence or context.
Execute security processes accurately and at pace with the business needs and evolving threat landscape.		Manual processes that can no longer keep up with the challenge.
Power major business initiatives such as cloud enablement and digital transformation.		A scarcity of security expertise.

The solution: Smart automation

Many organizations have turned to automation to meet the demands of an increasingly complex attack surface and the constant demand for regulatory compliance. However, automated solutions vary greatly in quality and return on investment. Without the proper visibility and context, automation can have neutral or even negative impacts on security and compliance posture.

However, with visibility and context, automation can reduce errors, slash risk, and improve process efficiency by up to 80 percent.*

Those benefits can be found in what's called smart automation.



THE TRIAD OF SECURITY MANAGEMENT

Automation, visibility, and context are the indivisible triad of security management. Any strategy or solution offering one component without the others will not deliver the expected benefits.

+ **Visibility** across the entire attack surface, including its security controls, assets, vulnerabilities, threats, and network topology spanning:
  + On-premises and shared data center networks
  + Public and private cloud infrastructures
  + Operational technology (OT) environment
+ **Context** of the attack surface gleaned from sophisticated analytics that turn data into actionable intelligence.
+ **Automation** to streamline and orchestrate processes that manage vulnerabilities, threats, security policies, firewalls, and their changes.

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

Incorporating smart automation into your SPM program

Smart automation has applications in a variety of security policy management (SPM) processes, as well as linking these processes through efficient, streamlined workflows:

- **Data collection, normalization and modeling**
- **Security posture assessment and analysis**
- **Recommendations and alerts**
- **Process orchestration**
- **Continuous oversight**

1. Data collection

Fundamental to the success of a security policy management program is good data. Information from the vast and varied components of the attack surface must be collected automatically on a regular basis from multiple technologies and vendor products, including:

- **Network devices** such as routers, switches, application delivery controllers, and the vendor tools that manage them.
- **Security controls** such as firewalls and cloud security tags, intrusion prevention systems (IPSs) and virtual private networks (VPNs).
- **Public and private cloud services** such as Amazon Web Services, Microsoft Azure, Cisco ACI, and VMware NSX, as well as their provided management tools.
- **Asset repositories** including endpoint security systems (EDRs), patch management systems, configuration management databases (CMDBs), and homegrown databases.
- **Vulnerability occurrence data** from vulnerability scanners, web and app scanners, asset configuration weaknesses, and custom vulnerabilities.
- **Business metadata**, including details of the assets, applications, asset owners, and users that can be used to drive smart automation policies.

Once the data is collected, similar data between like products is automatically normalized and merged. This step will yield a centralized repository.

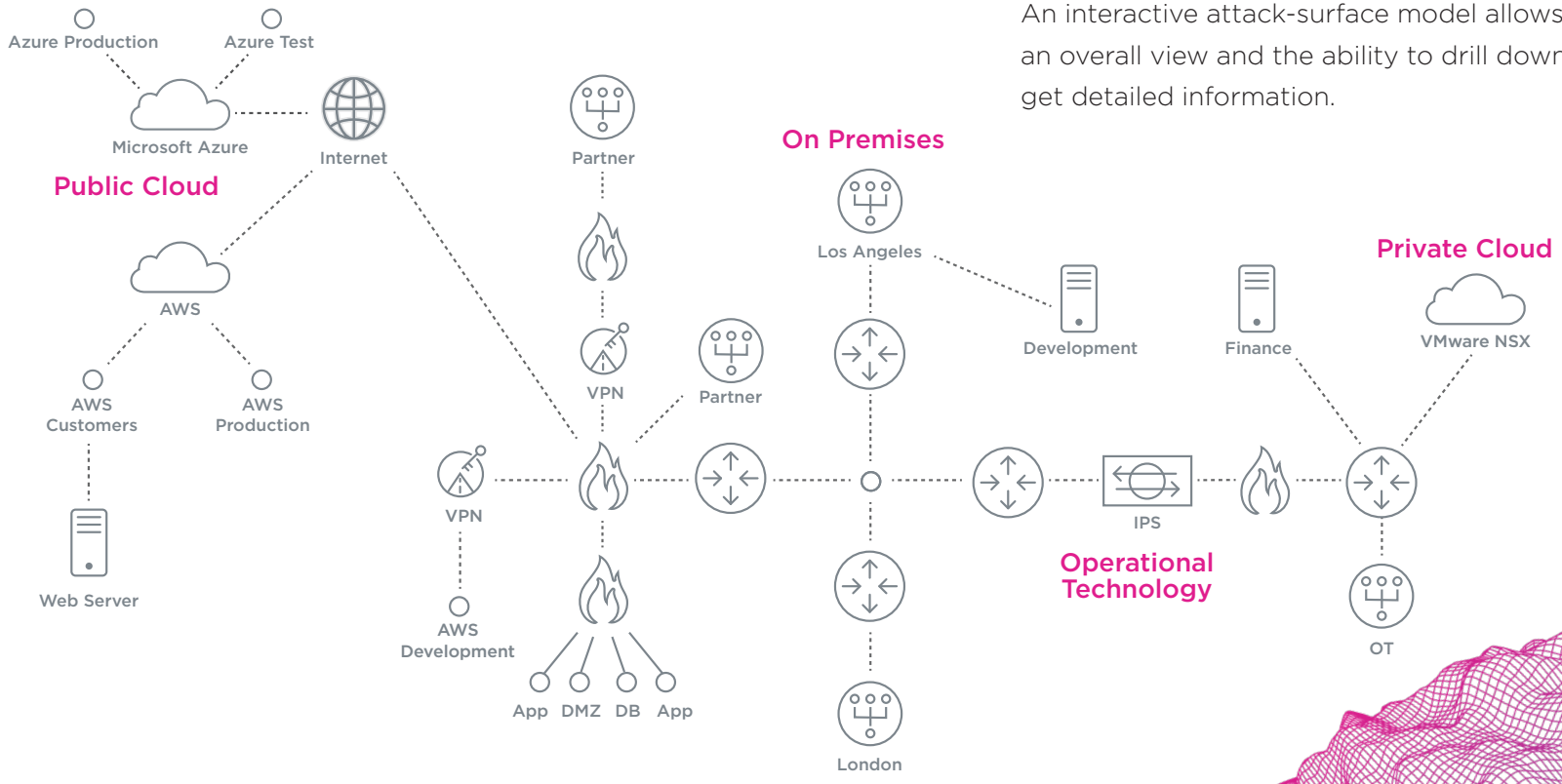
Model-driven visibility

Data collection, integration, and analysis should be used to build a visual, interactive dynamic security model that reflects the current state of the infrastructure and its risk. This model empowers CISOs and their teams with ongoing situational awareness and insight for many security management use cases.

A truly effective attack-surface model provides an overall view of the attack surface and the ability to drill down to reveal:

+ Hybrid, on-premises, multi-cloud, and OT network topologies
+ Detailed configuration information on all network devices and assets
+ Any possible path between any two points in the network
+ How security controls restrict or allow access to different parts of the network
+ Potential attack paths and where they put the organization at risk

An interactive attack-surface model allows both an overall view and the ability to drill down to get detailed information.



2. Exposure assessment and analysis

Using smart automation is incredibly valuable when it comes to correlating disparate data sets to yield actionable intelligence quickly.

Automated assessment and analysis

+ Clean up and optimize firewalls by correlating system and firewall logs with access control lists to reveal firewalls rarely or never used, and redundant, overlapping, or conflicting rules.
+ Spot policy violations through the comparison of raw device configuration files with industry standards and custom policies.

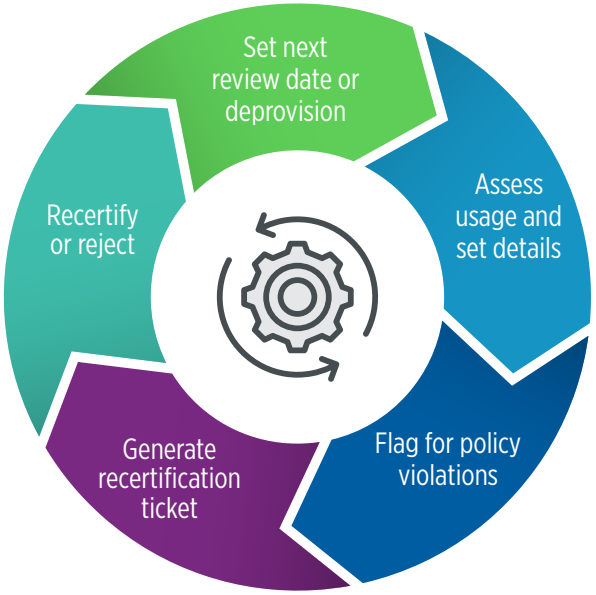
Modeling and simulation

+ Simulate access end-to-end between any two points in a network and between networks, including multi-cloud and OT environments, to identify zone-to-zone access compliance violations, troubleshoot connectivity issues, and spot misconfigurations.
+ Proactively assess rule changes on firewalls before they go live, identifying rule or access policy violations as well as vulnerability exposures the proposed change would create.

3. Recommendations and alerts

Once data has been contextualized through assessment and analysis, smart automation can be used to create specific recommendations and alerts to quickly address security and compliance issues and streamline processes.

Firewall rule reviews alert security teams to rules that have been unused for a pre-determined amount of time or that violate policy. Smart automation can trigger ticket reviews and initiate workflows to determine whether such rules should be recertified or de-provisioned.



RECERTIFICATION

Automated rule recertification workflows help manage the entire life cycle of firewall rules. Once rules are created, their usage is assessed to determine necessity, and metadata is applied to define the rule owner, the next certification date, etc. Tickets are automatically generated for rules that violate policy, are not used in a certain amount of time, or have reached their recertification date, which kicks off subsequent automated workflows.

4. Process orchestration

Orchestration must be backed up by visibility, context and some human interaction to prevent inadvertent security or performance issues. **Firewall change process** orchestration powered by smart automation reduces the time to carry out changes by up to 80 percent * and avoids wasting time on rollbacks due to human error.

Automating change provisioning carries a higher risk than other steps in these workflows, as it's when automation can directly impact network security. Without the right contextual intelligence, automated provisioning has the possibility to compound errors quickly over a large environment, which could lead to rollbacks and rework.

The accuracy and quality of the previous phases in the firewall change workflow are paramount to ensure any change meets policy requirements and doesn't open up risky access paths. This contextual intelligence is derived from insights into the hybrid network topology, security controls, assets, and vulnerabilities that impact the risk a change could introduce.

If pre-change analysis ignores any one of these components, the change management security process could actually worsen security and compliance posture rather than improve it.

PATH ANALYSIS

An automated analysis of the network model identifies all firewalls relevant to the change request and determines whether the requested access already exists.

RISK ANALYSIS

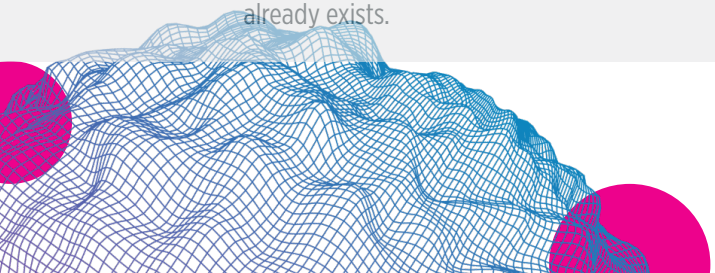
Automated model analysis also determines if requested changes would create new vulnerability exposures or violate rule or access policy.

PROVISIONING

Automated provisioning is available, implementing changes automatically for many leading firewalls.

RECONCILIATION

Automation verifies that the change made matches the original intent and provides third-party validation that the change was completed.



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

5. Oversight

Continuous oversight is vital to maintaining continuous compliance and systematically improving the security posture of dynamic networks facing an ever-changing threat landscape. Smart automation can help oversee these important tasks, including:

TRACKING AND AUDIT REPORTING

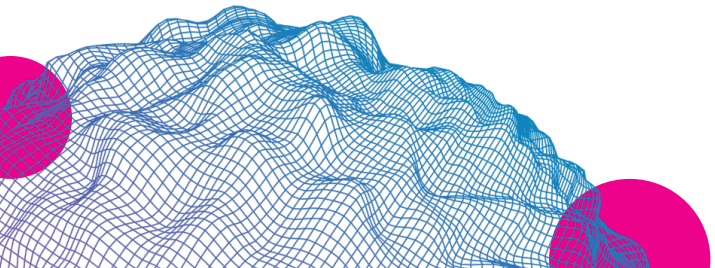
Demonstrate risk reduction effectiveness and adherence to security policy at all times. Automation can, for example, track every step of firewall change workflows and compile audit reports on demand.

MONITORING

Confirm zone-to-zone access compliance continuously and flag access and rule policy violations to stay abreast of attack vectors and identify compliance violations.

REPORTING

Gauge the overall impact of security actions and identify network locations and processes that need more resources or investment.



Business benefits

Smart automation powered by attack surface visibility and contextual intelligence can have a dramatic impact on your organization's overall risk and keep your infrastructure secure and compliant. By introducing smart automation, your organization can:

SIMPLIFY VULNERABILITY MANAGEMENT

of complex networks — on-premise, in the cloud, and in OT networks.

REDUCE COSTS

through operational efficiencies and the reduced risk of data breaches which require remediation, disrupt business revenue, and damage reputation.

MAXIMIZE HUMAN RESOURCES

by ensuring the team focuses on strategic tasks, while automation takes care of the routine and mundane.

ENSURE CONTINUOUS COMPLIANCE

with regulations such as PCI–DSS, NIST, and others, mitigating the risk of legal action and potentially steep fines for violations.

IMPROVE NETWORK SECURITY AND PERFORMANCE

reducing your risk of attack and the need for costly equipment or capacity upgrades.

About Skybox smart automation

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 Exposure Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.

The smart automation embedded in the Skybox Security Policy Management solution ensures organizations can:

Automate collection from enterprise networks and asset repositories to ensure a strong foundation for your security program.

Centrally manage security data from hybrid network environments, their security controls, assets, and vulnerabilities.

Visualize your attack surface with an always up-to-date network map and an offline model to analyze and troubleshoot issues.

Proactively identify issues most likely to be exploited in an attack and continuously monitor for policy violations.

Prioritize vulnerabilities and security weaknesses in context to target action where it's needed most.

Intelligently plan responses to systematically reduce your organization's risk of cyberattack and meet compliance requirements.

Want to learn more? Get a demo or talk to an expert:
skyboxsecurity.com/request-demo

SKYBOX SECURITY

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