SKYBOX SECURITY

Establish a Zero Trust framework with network visibility and context

Gain continuous understanding of your hybrid cloud networks and the entire attack surface to build and maintain zero trust frameworks

Challenges

Today's threat landscape combined with the rapid adoption of remote work and accelerating migration to the cloud has made adopting a Zero Trust strategy more urgent. Of the organizations adopting Zero Trust, 72% reported that the pandemic has sped up their adoption efforts[1].

Despite the urgency, establishing a Zero Trust environment is a challenging undertaking. Most organizations do not have adequate visibility into their networks to architect Zero Trust environments. Lack of visibility makes it difficult to properly establish "inherently untrusted" policies without disrupting business workflows. Once established, it is difficult to maintain zero trust policies due to changing networks and applications.

Driving factors for Zero Trust adoption

- **Rapid adoption of remote access technologies**
- **Expansion into new environments**
  - \+ Cloud applications and workloads
  - \+ Hybrid and multi-cloud environments
- **Increasing threat vectors**
- **Inability to handle increasing alerts**

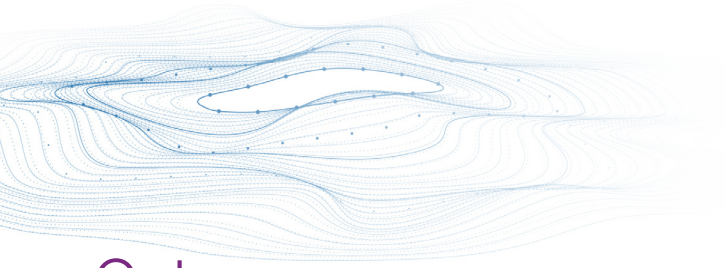
106%
Increase year-over-year in new ransomware samples in 2020[2]

56%
Of large companies receive 1000+ alerts daily[3]

[1] Zero Trust Cybersecurity: Never Trust, Always Verify, Deloitte, July 2020
[2] Vulnerability and Threat Trends Report, Skybox Security, February 2021
[3] State of SecOps and Automation Report, Sumo Logic, July 2020

What's needed

To establish and maintain a Zero Trust framework, you need a continuous understanding of your hybrid networks and the attack surface across all environments. You need to model and analyze your network, cloud, and security configurations together. This context helps you make informed decisions about what critical assets to protect with Zero Trust, how to properly design the network environments, and what specific policies need to be applied. Once the Zero Trust architecture is established, continuous and adaptive modeling of the hybrid networks is necessary to effectively maintain the Zero Trust posture.



Outcomes

+ Reduce risk by reducing exposure to potential cyberattacks
+ Improve business resilience with continuously validated Zero Trust environments
+ Maximize the efficiency of valuable human resources using automation

Contact an expert

Schedule a demo ···>

Why Skybox?

Determine where to focus your Zero Trust efforts

+ Aggregate and consolidate data sets that reflect the current configurations of your hybrid infrastructure, all your security controls, and endpoints
+ Identify the critical assets, applications, data repositories and infrastructure that will comprise your Zero Trust zone

Model your hybrid network

+ Model your network connectivity, combined with your network and security configurations, to understand what you are working with
+ Visualize and assess your security efficacy and develop your Zero Trust strategy

Architect for Zero Trust

+ Develop and optimize segmentation strategies
+ Configure and optimize your network and security technologies

Establish and validate Zero Trust policies

+ Validate policies using your network model
+ Automatically assess policies for exposure risk and compliance

Monitor and maintain

+ Leverage your network model to continually monitor your hybrid networks
+ Validate changes before they go live to ensure compliance
+ Automate change management processes and align with your Zero Trust strategies

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.