TAG

TRANSITIONING FROM SKYBOX TO REDSEAL: GUIDANCE FOR FORMER SKYBOX CUSTOMERS

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG

REDSEAL

TRANSITIONING FROM SKYBOX TO REDSEAL: GUIDANCE FOR FORMER SKYBOX CUSTOMERS

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG[1]

Skybox Security, once a recognized provider in the vulnerability and exposure management space, recently ceased operations.[2] The closure of Skybox leaves its enterprise customer base—many of whom depended on the company for network visibility, risk analysis, and policy assurance—facing the critical task of migrating to new solutions. It also created a potential seam in their existing cyber defense.

This report explores the potential for customers to transition from Skybox to RedSeal, a vendor with complementary capabilities and a solid technical foundation for hybrid network modeling and exposure management. The analysis is intended for enterprise security practitioners who are already familiar with the Skybox platform and who are now facing short timelines to maintain risk posture, operational continuity, and compliance alignment.

[1] *Founded in 2016, New York-based TAG Infosphere provides research and advisory in cybersecurity and AI for enterprise, government, lawmakers, researchers, and vendors. This report is part of a series of in-depth analyses of major cybersecurity vendors for general cybersecurity practitioners as well as TAG Research as a Service (RaaS) customers (see https://www.tag-infosphere.com/).*

[2] *See* ***https://www.skyboxsecurity.com/company/press-releases/*** *for the official statement from the former company regarding its decision to cease operations for financial reasons.*

HYBRID NETWORK MODELING AND VISIBILITY

As readers will know, Skybox was widely used by enterprise and government security teams for its ability to create models of enterprise networks, including for both premise-based and hybrid multi-cloud environments. Its goal was to provide a logical view of connectivity and enforceable segmentation policies. RedSeal offers similar, and arguably more refined, capabilities for modeling complex hybrid infrastructures.

RedSeal's platform constructs a real-time, comprehensive model of the network by ingesting configurations from routers, firewalls, cloud route tables, and security groups across AWS, Azure, and other clouds. This modeling is not just visual but analytical, allowing security teams to query and analyze access paths at scale. In comparison to Skybox, RedSeal's modeling is deeply optimized for operational use in large-scale, dynamic environments.

ATTACK PATH ANALYSIS AND EXPOSURE PRIORITIZATION

Despite the company's eventual financial challenges, Skybox enjoyed a customer base that valued the platform's ability to identify attack paths from vulnerable endpoints to crown-jewel assets. While effective, Skybox's reliance on scheduled scans and its lack of native real-time integrations limited how dynamic its attack simulations could be. This was not the root cause of the decision to cease operations, but it seems a relevant observation.

RedSeal improves on this through a real-time attack path analysis engine that simulates lateral movement and privilege escalation possibilities across the entire network topology. Using live configurations and vulnerability feeds, RedSeal calculates exposure risk in context, helping prioritize remediation not just based on CVSS score but on actual exploitable paths. This is a significant upgrade for teams looking to triage risk effectively.

VULNERABILITY MANAGEMENT INTEGRATION

Readers will also know that Skybox offered a means for performing central correlation and visualization for vulnerability scan results. It normalized data from third-party scanners and provided graphical overlays of vulnerability data on top of the network model. RedSeal offers similar functionality with greater automation and contextual analysis, both of which have emerged as high priority requirements.

RedSeal integrates with Tenable, Rapid7, and Qualys, among others, and overlays vulnerability data onto the modeled environment. What sets RedSeal apart, in our estimation, is its ability to trace each vulnerability to its exposure potential—meaning whether an attacker could reach it and whether it resides on a business-critical path. This type of contextual awareness greatly improves prioritization efforts and reduces false positives.

COMPLIANCE ASSURANCE AND POLICY AUDITING

Skybox was also effective in supporting continuous compliance checks against major industry regulations such as PCI DSS, NIST, and ISO 27001. This compliance and regulatory support allowed for simulation of network changes by Skybox customers to ensure they would not violate security policies or compliance baselines. RedSeal matches and in many cases extends these important capabilities.

RedSeal specifically maintains a real-time compliance posture dashboard and supports both out-of-the-box and customizable policies. One valuable RedSeal capability is the platform's ability to simulate policy violations at the path level—allowing auditors and technical staff to understand not just if a rule is broken, but how it would manifest in practice. This visibility can be critical during audits or forensic reviews.

CHANGE MANAGEMENT SIMULATION

One particularly strong feature of Skybox was its firewall change manager tool, which provided a workflow to validate rule changes prior to deployment. This helps to explain the company's recommendation that users dependent on this feature consider shifting support for such capability to commercial vendor Tufin. That said. RedSeal supports a similar concept, though more focused on simulation and impact analysis.

With RedSeal, teams can simulate proposed configuration changes across the network and evaluate potential access path changes. While it does not offer a ticketing system, its integration with operational workflows via API allows teams to fold RedSeal simulations into broader change management pipelines. Users who have shifted to Tufin or other vendors for firewall changes would thus be wise to complement such support with RedSeal.

CLOUD SECURITY AND MULTI-PLATFORM SUPPORT

Skybox had made some initial strides toward supporting cloud visibility, but it was often limited by static configurations and slower development cycles. RedSeal has native support for major public cloud platforms and continuously updates cloud inventory and route maps. This dynamic mapping is especially beneficial in environments with frequent changes to security groups or routing configurations.

Furthermore, RedSeal's ability to bridge physical, virtual, and cloud environments into a single exposure model is key for organizations undergoing digital transformation. We have found that such converged focus is an increasingly common approach, especially for larger environments that might include critical physical support. This includes industrial control and operational technology-based infrastructures.

OPERATIONALIZATION AND MANAGED SERVICES

Finally, we should point out that some Skybox customers were known to cite the complexity of maintaining the platform.[3] RedSeal, in contrast, offers managed service options, including fully staffed deployments, ongoing operational support, and health-check assessments. These services lower the overhead of keeping the platform tuned and effective, which is crucial for lean security teams.

RedSeal also maintains a strong professional services presence and a modular architecture that aligns well with service-based adoption models. We have found that for some teams who have not developed in-house expertise in developing an accurate and useful network model, having the option to engage professional services-based assistance is viewed as a valuable management option.

CONCLUSION: A LOGICAL TRANSITION PATH

To conclude, we would share our view that RedSeal will provide former Skybox customers with a technically sound and operationally mature platform for exposure management. Its focus on real-time modeling, path analysis, contextual vulnerability mapping, and compliance assurance closely mirrors—and in many cases improves upon—the capabilities that made Skybox popular. We endorse transition of customers who resonate with these scenarios to RedSeal.

Given the urgency facing former Skybox users, RedSeal represents a practical, low-friction transition option, particularly for teams needing to preserve compliance, maintain risk posture, and avoid

---

[3] TAG provides a Research as a Service (RaaS) community in which feedback, reviews, insight, and guidance are offered not just to the TAG analysts, but also to other community members through unilaterally established connections. Through this work, we gain insights into feedback on tools such as Skybox.

disruption in their security operations. While no migration is without challenges, the architectural and functional parallels between Skybox and RedSeal offer a reassuring roadmap for continuity.

Organizations seeking to replace Skybox should initiate a RedSeal proof-of-value (PoV) engagement to map current Skybox use cases into RedSeal's corresponding functions. This technical alignment will help ensure a smooth and defensible migration strategy. Readers who are TAG Research as a Service (RaaS) customers can reach out to TAG for more assistance on this and related topics through their RaaS portal account. We look forward to hearing from you.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and rec-ommendations to enterprise teams, government agencies, and commercial vendors in cyberse-curity and artificial intelligence.