SKYBOX SECURITY

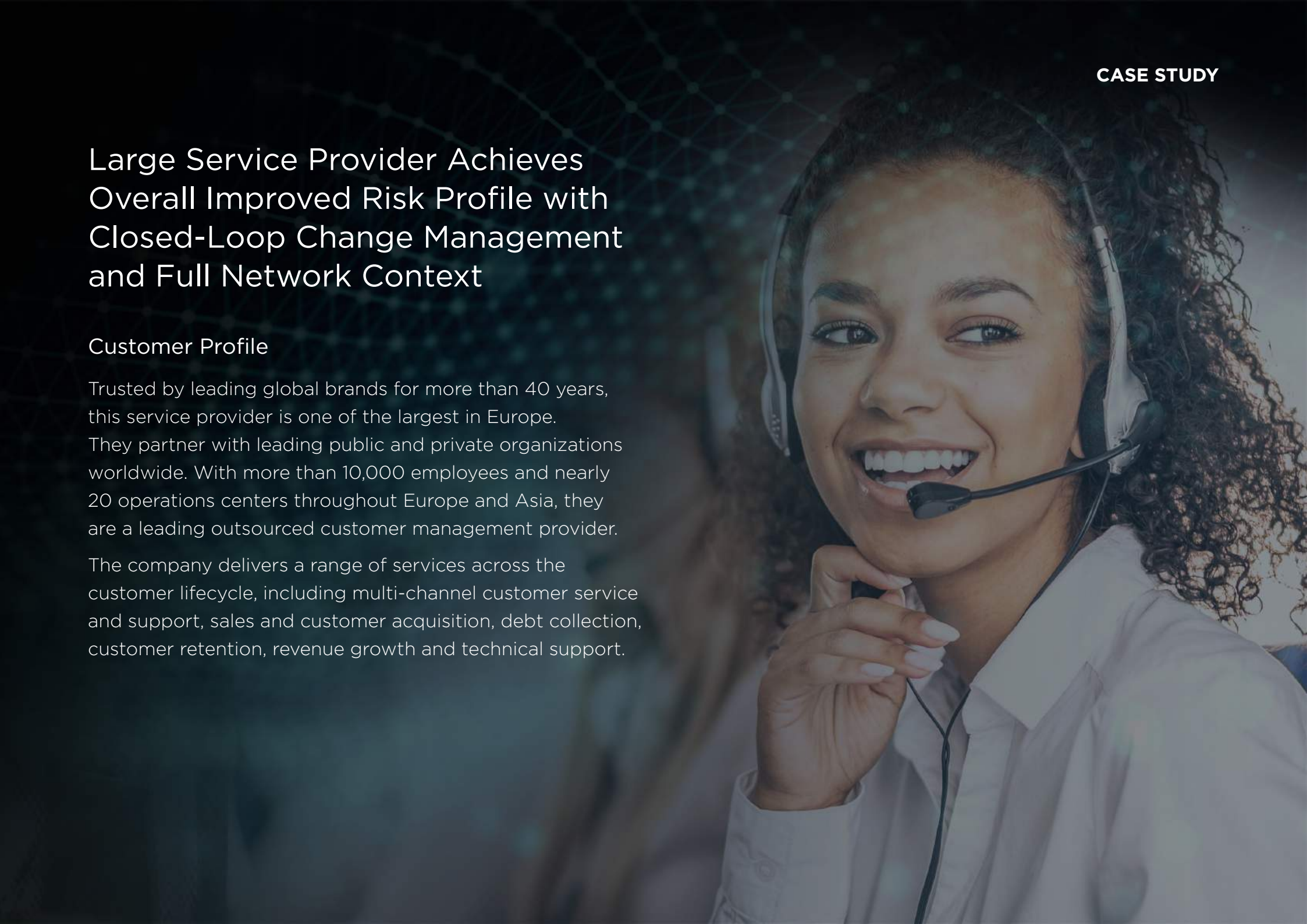
CASE STUDY

STRONGER SECURITY

Through Context-aware Change Management

CASE STUDY

Large Service Provider Achieves Overall Improved Risk Profile with Closed-Loop Change Management and Full Network Context



Customer Profile

Trusted by leading global brands for more than 40 years, this service provider is one of the largest in Europe. They partner with leading public and private organizations worldwide. With more than 10,000 employees and nearly 20 operations centers throughout Europe and Asia, they are a leading outsourced customer management provider.

The company delivers a range of services across the customer lifecycle, including multi-channel customer service and support, sales and customer acquisition, debt collection, customer retention, revenue growth and technical support.

Challenges

Complex network environment featuring over 100 firewalls

Costly and slow manual change management processes

Inability to track changes and verify they were implemented as intended

Unacceptable overall network risk profile

Compliance issues with PCI and ISO 27001

Results

Improved change management and reduced firewall maintenance costs

Accelerated change implementation with confidence that changes made were as intended

Reduced the overall network risk profile

Ensured continuous compliance with PCI and ISO 27001

The Problem

The company had a large and complex network infrastructure with more than 100 firewalls. With the addition of new firewalls on a regular basis, the firewall management team faced a chronic headache: ensuring new firewalls were deployed correctly with the right rules and that the rules matched intent. Network teams also struggled to understand where they stood on compliance requirements, including PCI and ISO 27001.

The security teams needed to step in and determine how to quickly and accurately check for policy violations, potential vulnerabilities, risky new changes, and keeping systems optimized.

Scope And Selection Criteria

The company's organization was looking for a comprehensive solution to address five key challenges. With the high volume of firewalls, it was impossible to fully understand the network infrastructure. Next, the organization flagged firewall clean-up and optimization as a critical initiative. From there, the organization expanded the scope to address policy compliance and implement a robust and closed-loop change management process. Finally, the team sought capabilities to reduce the network's risk profile. The organization selected Skybox Security Suite as a fully integrated solution to address a multitude of concerns around network security and policy compliance.

> With Skybox, we've improved our process around change management and reduced our costs. Most importantly, we know that all of our firewalls are PCI and ISO 27001 compliant.

– Security Consultant

Solving the Problem

The company deployed the full Skybox® Security Suite—Network Assurance, Firewall Assurance, Change Manager and Vulnerability Control—all through a Skybox virtual appliance.

One of the first tasks was completely understanding the network infrastructure. Using Skybox® Firewall Assurance, they were able to achieve the necessary understanding of the full network and endpoint spectrum and intelligence. The network was quickly modeled, identifying and documenting all firewalls and rule sets.

Network Assurance laid the foundation of total network visibility, and with the addition of Firewall Assurance, the team could not only see all of their firewalls, but were also able to actively review all firewall rules in context with the network: with routing rules, access control rules, and with network/port translation rules.

The combination of Network Assurance and Firewall Assurance greatly improved their team's control of access policies and routes. Firewall Assurance automated network access paths, translated administrator concepts into well defined policies, and identified specifc tests that were needed to ensure that policies were properly implemented and enforced.

"Previously, we didn't have full knowledge across the estate," said their security consultant. "Now we have a more comprehensive understanding of all our firewalls, and we've begun analyzing all the rules on them."

Managing Changes

The company had been using a legacy change management process, which entailed using an Excel spreadsheet to submit and approve firewall changes. They had no way to confirm that changes were made correctly, and there was no closed-loop process to ensure that the implemented change matched the intent of the change request.

Now the network team monitors firewalls for changes which are reconciled against the change database to ensure that they were implemented correctly.

Change Manager turned a manual and disorganized change management process into a secure, manageable and automated workflow. Change Manager's closed-loop design transformed their processes into a secure, manageable and automated workflow, allowing for the validation they needed to ensure every change matched the original intent of the change request and didn't introduce risk.

Reducing Risk

To continually minimize risk across the network, the company was able to leverage Vulnerability Control to go beyond the scope of scanning and patching with combined analytics and attack surface context that enabled them to accurately identify exposures, prioritize risks, and focus remediation efforts to reduce the greatest amount of risk with the least amount of effort.

Guaranteeing Compliance

Once firewalls were cleaned up and optimized, the team needed to ensure that the network and its devices were in compliance with both internal security policies and external regulatory requirements. With Skybox, they were able to automate the analysis of network access paths and easily design and validate access policies. After their analysis and review, it was discovered that some policies were misconfigured and required remediation.

The end result: a customized, consolidated view of NIST and PCI regulatory requirements mapped across all connected devices to ensure continuous compliance. Skybox's search functionality was so robust, the team was able to find network devices they had never seen before with any other security tool.

Results

The company achieved dramatic improvement of their security processes with context-aware change management, which has reduced firewall management costs and strengthened overall security across their estate.

Change management is now faster, more accurate, and operations teams are much more effective and efficient at managing their firewalls while maintaining all of them compliant with PCI and ISO 27001.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with more than 140 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