CASE STUDY

ORANGE CYBERDEFENSE FURNISHES APPLICATION DELIVERY AND NETWORK AUTOMATION

Application owners for global retail chain get faster response times with application visibility and automated deployment.

CUSTOMER NAME

Orange Cyberdefense

LINE OF BUSINESS

Digital security services provider

LOCATION

Multinational

WEBSITE

orangecyberdefense.com

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. They embed security into Orange Business Services solutions with more than 250 security researchers and analysts and 16 SOCs distributed around the world supporting customers in over 160 countries.

"We cut the time it takes to implement firewall rules by at least 50%."

Hans Broomé
Security Engineer
Orange Cyberdefense

THE CHALLENGE

Orange Cyberdefense is an on-site consultant for a large retail chain with hundreds of stores and hundreds of thousands of employees spread out across the world.

The client has over 2,500 multi-vendor firewalls and Layer 3 devices in their global data centers. They also run hundreds of mission-critical business services. Business services include supply chain management and ERP systems, global eCommerce operations, financial management systems, and much more. As a result, they had to cope with hundreds of change requests daily.

Some of the challenges included:

Lack of centralized management – Multiple vendors' firewalls are deployed, which were implemented by multiple third-party vendors. There was no validation that rules were consistently applied across multiple vendor's management consoles.

Commissioning and decommissioning devices – A mix of multi-vendor new and legacy devices run in the data center and maintaining consistency across multiple vendors and multiple versions of devices was difficult.

Lack of automation – Firewall communication and traffic flows were described in Excel sheets and needed to be manually updated whenever there was a change.

Slow execution of change requests – Implementing firewall changes took over a week.

Poorly implemented rules – The rules did not reflect what the requester asked for. They either allowed too much traffic in or were too narrow, not allowing the required traffic and thus needed to be re-implemented.

THE SOLUTION

The client searched for a solution that provided:

Faster implementation of firewall changes.

Comprehensive firewall support for a globally dispersed multi-vendor, hybrid estate.

Automation of security policy change management and documentation of security policy changes.

Visibility into their business applications and traffic flows.

They implemented the AlgoSec Security Policy Management Solution, made up of AlgoSec Firewall Analyzer, AlgoSec FireFlow, and AlgoSec AppViz and AppChange (formerly AlgoSec BusinessFlow).

AlgoSec Firewall Analyzer analyzes complex network security policies across on-premise, cloud, and hybrid networks. It automates and simplifies security operations, including troubleshooting, auditing and risk analysis. Using Firewall Analyzer, the client can optimize the configuration of firewalls, and network infrastructure to ensure security and compliance.

AlgoSec FireFlow enables security staff to automate the entire security policy change process from design and submission to proactive risk analysis, implementation, validation, and auditing. Its intelligent, automated workflows save time and improve security by eliminating manual errors and reducing risk.

AlgoSec AppViz and AppChange (formerly AlgoSec BusinessFlow) discover, identify, and map business applications, providing critical security information regarding the firewalls and firewall rules supporting each connectivity flow. With AlgoSec AppChange, changes can be made at the business application level, including application migrations, server deployment, and decommissioning projects.

THE RESULTS

Some of the ways the client benefits from using AlgoSec include:

Greater transparency by providing a single source of truth that took into consideration the entire network estate.

50% reduction in the time needed to implement firewall rules.

More communication between network security/IT staff and business application owners, who are now able to submit change requests in business language and easily describe their needs, thus reducing misconfigurations and potential breaches.

Better compliance reporting – with both an easy API integration and also audit-ready compliance reports.

Automated change management – network changes are now recorded while being made – not managed with Excel.

By using AlgoSec, application owners have more visibility into the network and are better able to trace what has changed within their business applications. "Documentation is several hundred percent better this way," said Hans Broomé, Network and Security Consultant at Orange Cyberdefense. "With many different versions of the services, by using AlgoSec the IT team is confident that they are making changes to the correct version."

There were even unexpected gains, such as improved security management procedures. Change requests became more accurate as they gained visibility into the network and made the change request process more systematic and transparent. Requesters, as well as stakeholders such as their managers, have full visibility of their change request's status and can verify that the request works as intended.

Orange Cyberdefense is also impressed with the dedicated attention they receive from AlgoSec. AlgoSec's support team is familiar with the global organization and provides dedicated attention tailored to their exact needs. They stay up to date with the AlgoSec solution's latest capabilities, and the technical team maximizes their use of it thanks to an extensive training library. "The best is yet to come," concluded Broomé.