

CASE STUDY

NCR ACCELERATES TOWARDS ZERO-TRUST

Leading financial technology provider reduces risks and gains visibility over their application delivery pipeline.



CUSTOMER NAME

NCR Global

LINE OF BUSINESS

Digital banking,
enterprise POS systems

LOCATION

Georgia, USA

WEBSITE

ncr.com

NCR Corporation is a leading global point-of-sale (POS) provider for restaurants, retailers, and banks and a provider of multi-vendor ATM software. Headquartered in Atlanta, Georgia, NCR has over 36,000 employees in 160 countries, and solutions are distributed in 141 countries.

THE CHALLENGE

NCR needed to connect its DevOps pipeline with its network security. With over 4,500 policy changes made annually, it was difficult to securely manage their entire networking and security environment while being responsive to application owners but still achieve zero trust.

Strategically, they were aiming to automate and orchestrate security policy changes across their entire hybrid network, so they could securely accelerate application delivery.

THE SOLUTION

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

AlgoSec Firewall Analyzer enables organizations to discover, identify, and map business applications across their entire hybrid network. It analyzes complex network security policies across the network. It automates and simplifies security operations, including troubleshooting, auditing, and risk analysis.

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, the application visibility add-on for AlgoSec Firewall Analyzer, provides visibility for your network applications, enabling secure application delivery.

AlgoSec AppChange, the application automation add-on for AlgoSec FireFlow, allows for changes at the business application level, including during application migrations, server deployment, and decommissioning projects.

“AlgoSec helps us be vendor-agnostic and understand our full security posture to lead us down this journey to achieve zero-trust.”

Scott Theriault, Global Manager
Network Perimeter Security
NCR Corporation

AlgoSec is a strategic component of NCR's network security, managing its entire network security infrastructure.

The AlgoSec platform enables the NCR Corporation to manage application connectivity end-to-end across their network — including public cloud, Cisco ACI, and physical firewalls. “Most products don’t understand the end-to-end environment. AlgoSec does,” noted Scott Theriault, Global Manager, Network Perimeter Security.

Some of the ways that NCR Corporation benefits from AlgoSec include:

- **Launched migration** of their on-premises data centers into the Cisco ACI fabric.
- **Extended microsegmentation** to Cisco ACI environment.
- **Achieved complete visibility** of their global security posture from a single dashboard.
- **Automated risk analysis**, achieving visibility and insights into the risk that changes introduce.
- **Streamlined auditing process** with to automatic logging and audit-ready compliance reports.
- **Cleaned up and reduced firewall policies** with rule cleanup, object cleanup, and policy tuning.

“As we aspire to achieve zero-trust, when moving into the cloud, micro-segmentation and container security come into play. Therefore, we need tools like AlgoSec to assist us in the journey because most application owners don’t know what access is needed. This tool helps them learn what needs to be implemented to reduce the attack surface,” stated Theriault.