FINANCIAL INSTITUTIONS:

Best Practices for Network Security and Compliance

AN ALGOSEC WHITEPAPER

Introduction

In order to maintain a competitive advantage, information security teams at financial institutions must be able to support business transformation initiatives and deploy new applications or updated functionality to market quickly and securely.

Most IT departments use automation tools to assist them with many aspects of their work – including managing software changes or provisioning storage. Automation allows them to support the fast pace required, ensure quality and maintain compliance with industry regulations. However, when it comes to security, oftentimes the InfoSec team still makes the necessary network security changes using manual processes. This is mostly due to the perceived complexity of the segmented network infrastructure; the large number of firewalls and network security devices (from multiple vendors) that are typically deployed across a financial institute's network, as well as the extensive compliance requirements that financial institutions are subjected to.

As a result, the InfoSec team is often perceived as a bottleneck to progress - holding back the release of a new competitive application or feature to market.

This white paper will discuss the challenges facing InfoSec teams today. It will then explain how a network security management solution delivers critical automation that will help transform the InfoSec team from a business inhibitor to a business enabler.

Network security challenges for financial institutions

Financial institutions face two key network security related challenges in their mission to serve their customers: regulatory compliance and a continual demand for changes in order to compete in the market.

The number of regulations that financial institutions are required to uphold has significantly increased over the years. They include GLBA, GDPR, BASEL II, SOX, Dodd-Frank, PCI-DSS and many others. While these regulations aim to provide best practices that will help both the financial institutions and their customers, they require considerable effort to maintain, particularly with regards to network security.

The second challenge that impacts network security in financial services, is the constant demand for changes.

In recent years, the demand for innovation coupled with competition from agile and disruptive fintech companies is putting considerable pressure on financial institutions. As a result, financial institutions are constantly seeking ways to improve the way they interact with their customers while becoming more efficient. This means that there is now an ever-present need for change in a typically conservative industry which has previously been slow and reluctant to embrace change!

Managing network security changes efficiently and effectively across today's complex network environments requires automation. Yet, while IT organizations have embraced automation to handle many of its tasks, the InfoSec team has not. In the following section, we will discuss ways to utilize automation to manage security changes and manage the ever-increasing demands of industry regulations.

Automated network security policy management

To tackle these challenges, the InfoSec team needs automation to effectively manage the demands of regulatory compliance as well as keep up with the volume of network security policy changes.

Managing compliance with industry regulations

As part of compliance requirements most regulations require full visibility into the security posture, regular audits, and documentation of any changes.

Visibility of the security posture: The first step to achieving visibility is to identify all the applications that support customer transactions and manage customer information. Then they should be classified based on the relevant regulations, such as PCI for applications that manage cardholder information. There are tools that can handle this process automatically, including the discovery process, which saves considerable time.

Moreover, automation tools can help with documenting the entire environment, including the network security device configurations and security policies – which is a key part of regulatory compliance. In addition to supporting compliance requirements, this visibility and transparency will expose any gaps and risks in your network security, and thus help in making your network secure.

Streamlined audits: Whether internal or external, audits eat up considerable resources. The InfoSec team currently needs to spend significant time and effort generating reports that document their security posture and prove compliance with every regulation – time that could be better spent focusing on securing the network or responding to business requests. Automation can handle all these processes, and generate self-documenting, audit-ready reports out of the box.

Documenting compliance: Most network security management solutions will review all changes during design and deployment to ensure that they comply with the industry regulations. As part of this process they will document and provide a full audit trail of the change, thereby automating the requirement for change documentation.

Managing the constant barrage of change requests

An automation solution is a paramount to tackling the frequent change requests that are typically required in the financial industry. An automation solution will enable the InfoSec team to focus on the impact and risk of the change as well as ensure that all changes are necessary (typically around 30% of change requests are unnecessary).

An automation solution must:

1. Ensure that the network security policy change request will not breach the compliance posture
2. Automatically map the network route for any planned changes and identify the firewall, routers and switches along that route that need to be changed
3. Assess all the risks of a security change. These include regulatory compliance risks as well as internal risks
4. Understand the details of each firewall rule change request and determine whether a change is really needed, whether a change to an existing rule will be sufficient or if there is a need to create a new rule as part of the change request. This process will reduce the overall number of rules and help optimize the security ruleset
5. Can automatically deploy changes directly onto firewalls

Summary

Financial institutions are constantly seeking to better serve their customers and maintain a competitive edge through new technology innovations. Yet often these organizations fall behind on delivering these new innovations into production. Their network and security operations team are hampered by manual and error-prone security change management processes coupled with the ever-increasing demands of industry regulations, which impact time-to-market.

Automated network security management solutions help streamline the auditing process, ensure continuous compliance as well as significantly simplify and speed up the process of managing network security changes.

About AlgoSec

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With AlgoSec, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch - across their cloud, SDN and on-premise networks. Over 1,800 enterprises, including 20 of the Fortune 50, have utilized AlgoSec's solutions to make their organizations more agile, more secure and more compliant - all the time. Since its inception, AlgoSec has provided the industry's only money-back guarantee.