algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

Policy Change Automation

Curing the Network Security Management Headache

EBOOK

Table of Contents

Cure the network management headache

In today's IT environment, the only constant is change. **Business needs change.** As your business changes, so must your security policies.

The Problem

Change comes with challenges, leading to major headaches for IT operations and security teams. This develops into huge business problems:

- Manual workflows and change management processes are time-consuming and hinder business agility.
- Improper management changes lead to serious business risks – as benign as blocking legitimate traffic all the way to network outages.

The Solution

Automation and **actionable intelligence** can enhance security and business agility – without the headaches and misconfigurations caused by manual, ad-hoc processes. In this document, you will learn the secrets of how to elevate your firewall change management from manual labor-intensive work to a fully automated zero-touch change management process.

Why's it hard to change network policies?

Placing a sticky note on your firewall administrator's desk or sending an email that gets lost in the clutter and expecting the change request to be performed pronto does not constitute a formal policy. Yet, shockingly, this is common.

You need a formal change request process. Such a process dictates defined and documented steps about how to handle a change request, by whom, how it is addressed, defines a SLA, and more.

Firewall change management requires detailed and concise steps that everyone understands and follows. Exceptions must be approved and documented so stakeholders can understand the risk.

Your security policy management solution should seamlessly integrate with the tools you are already using to accelerate its adoption in your organization.

AlgoSec enables business agility by integrating with ITSM systems like ServiceNow, BMC Helix ITSM (formerly Remedy), Clarity SM (formerly CA Service Management) and HP Service Management.

Communication Breakdown

Network security and IT operations staff work in separate silos. Their goals, and even their languages, are different. Working in silos is a clear path to trouble. It is a major contributor to out-of-band changes which result in outages and security breaches. In many large companies, routine IT operational and administrative tasks may be handled by a team other than the one that handles security and risk. Although both teams have the same goal, decisions made by one team lead to problems for the other.

Network complexity is a security killer

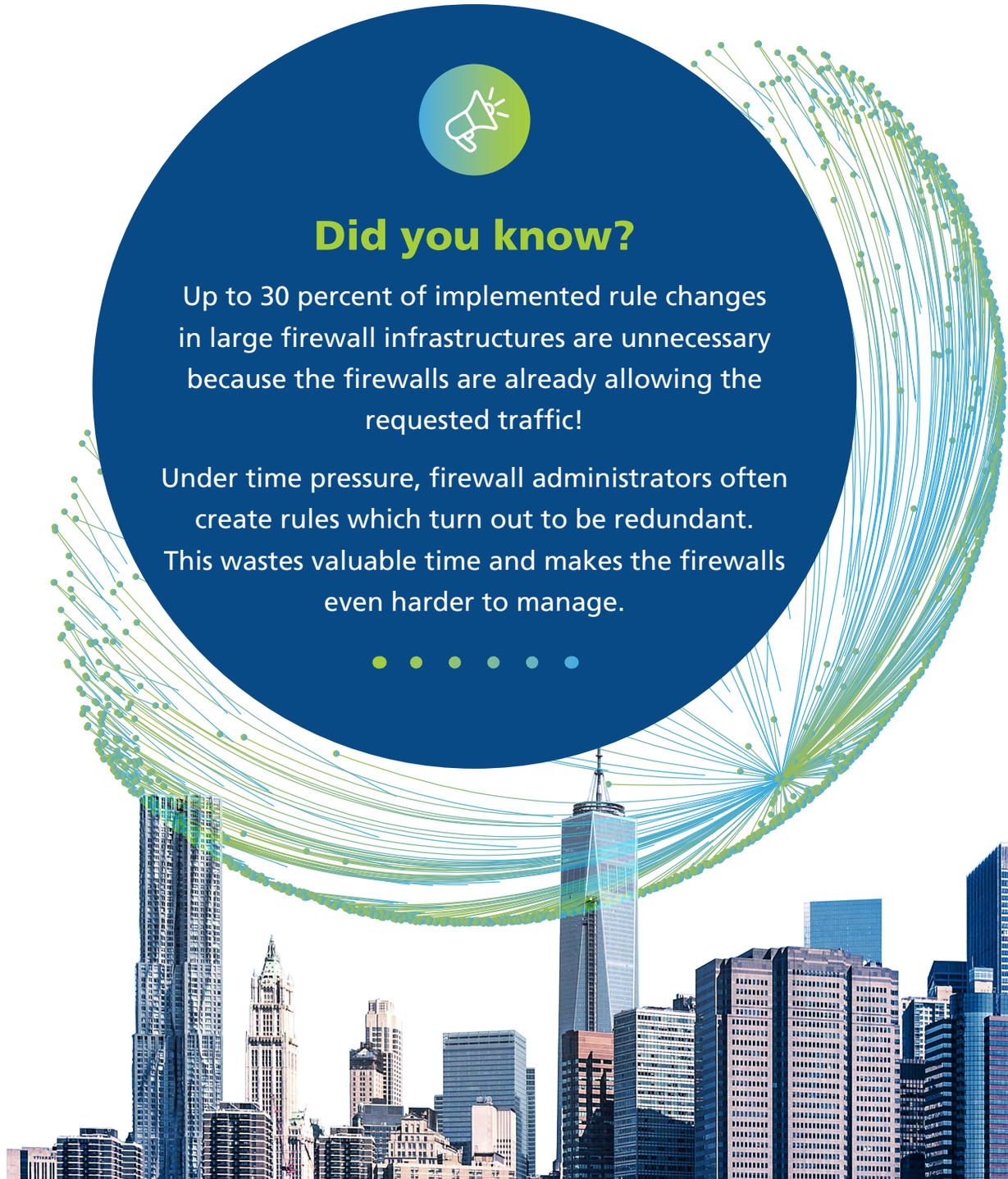
Today's networks exist across complex environments – on-premise data centers, multiple multi-vendor public and private clouds, spanning geographic borders. It's difficult to keep track of your entire network estate.

Security expert Bruce Schneider once stated that "Complexity is the worst enemy of security." The sheer complexity of any given network can lead to a lot of mistakes. Simplifying and automating the firewall environment and management processes is necessary.

Did you know?

Up to 30 percent of implemented rule changes in large firewall infrastructures are unnecessary because the firewalls are already allowing the requested traffic!

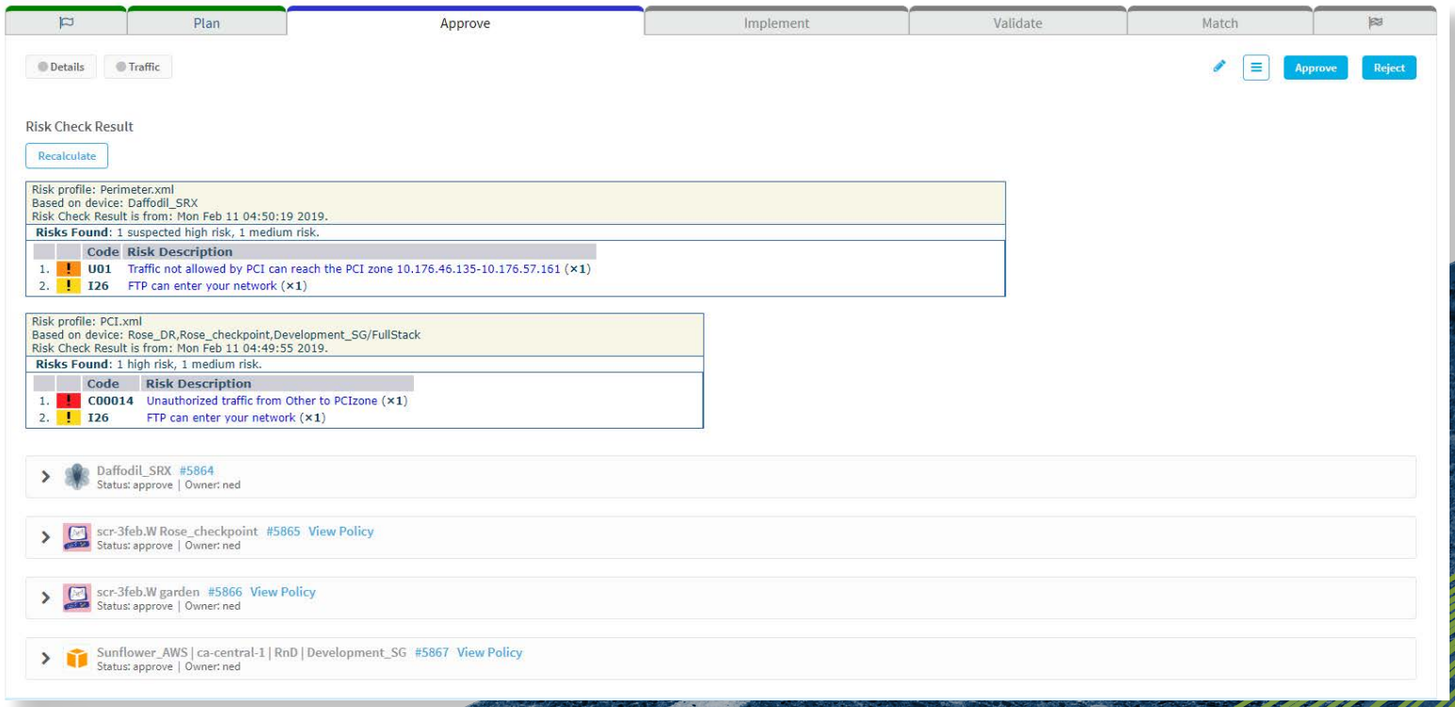
Under time pressure, firewall administrators often create rules which turn out to be redundant. This wastes valuable time and makes the firewalls even harder to manage.



Mind the security gap

Introducing new things open up security gaps. New hires, software patches, upgrades, server migrations, and network updates increase your exposure to risk. Who can keep track of it all?

What about unexpected, quick fixes that enable access to certain resources or capabilities? A fix is made in a rush (after all, who wants a C-level exec breathing down their neck because he wants to access resources RIGHT NOW?) without sufficient consideration of whether that change is allowed under current security policies.



Speed becomes mistaken as agility and takes precedence over security.

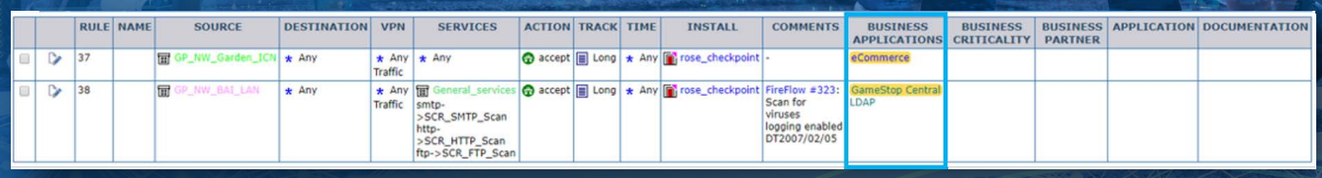
You need to be able to make changes fast and accurately. Agility and security together.

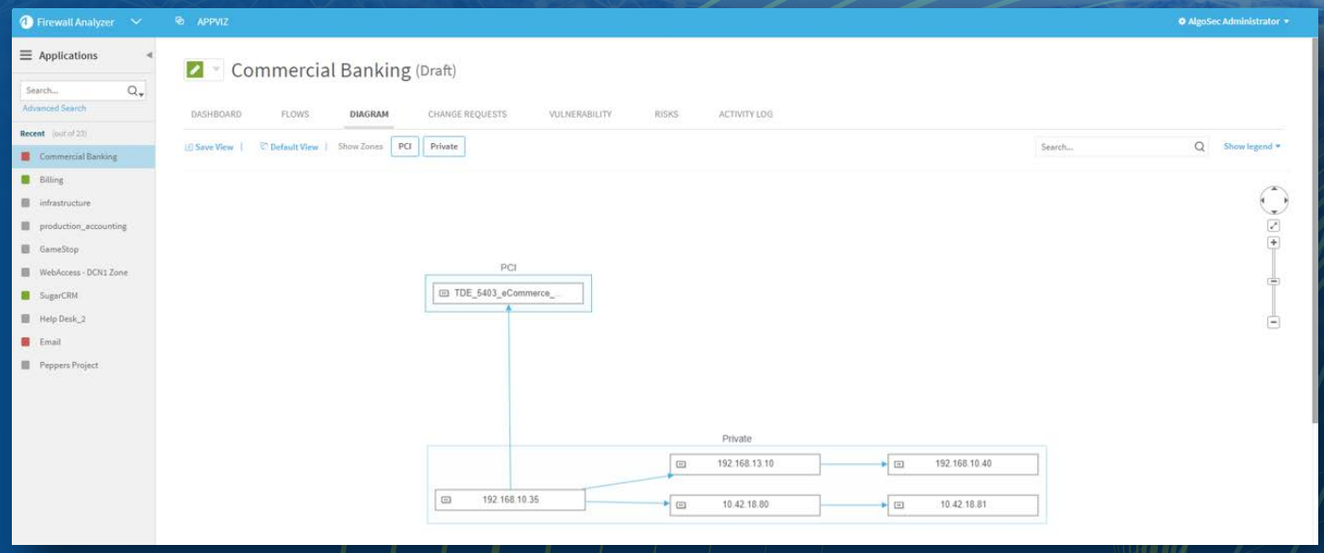
How can you get both agility and security? Network automation.

There are solutions that automate firewall management tasks and record them so that they are part of the change management plan. Network automation helps bridge the gap between change management processes and reality. A sophisticated firewall and topology-aware system that identifies redundant change requests increases productivity.

IT and security teams are responsible for making sure that systems function properly. But, they approach business continuity from different perspectives. The security department's goal is to protect the business and its data, while the IT operations team focuses on keeping systems up and running. The business has to keep running AND it has to be secure.

Alignment is easier said than done. To achieve alignment, organizations must reexamine IT and security processes. Let's have a look at some examples of what happens when there is no alignment.





Good changes gone bad

Example 1

A classic lack of communication between IT operations and security groups put XYZ Corporation at risk. An IT department administrator, trying to be helpful, took the initiative to set up (with no security involvement or documentation) a file share for a user who needed to upload files in a hurry.

By making this off-the-cuff change, the IT admin quickly addressed the client's request. However, the account lingered unsecured. The security team noticed larger spikes of inbound traffic to the server from this account. Hackers abound. The site had been compromised and was being exploited.

Example 2

A core provider of e-commerce services suffered a horrible fate due to a simple, but poorly managed, firewall change. One day, all e-commerce transactions in and out of its network ceased. The entire business was taken offline for several hours. The costs were astronomical.

What happened?

An out-of-band (and untested) change to a core firewall broke the communication between the e-commerce application and the internet. Business activity ground to a halt.

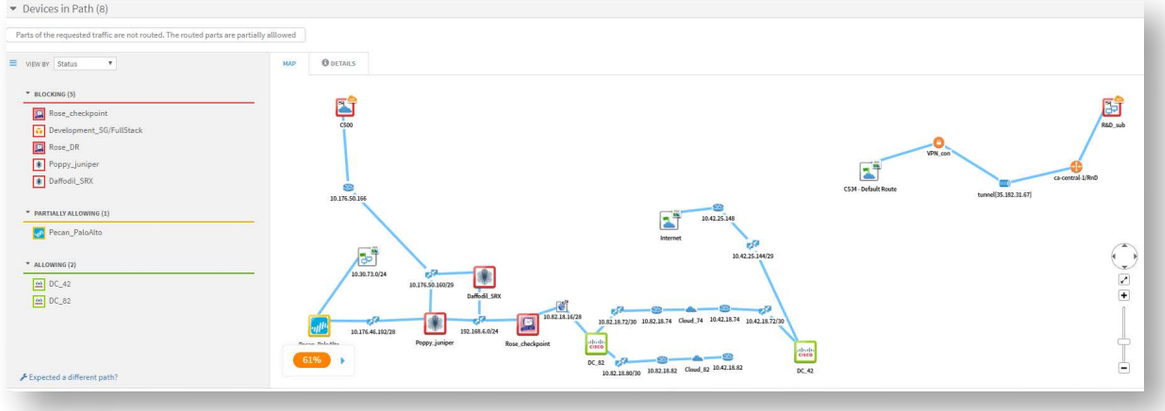
Because of this incident, executive management got involved and the responsible IT staff members were reprimanded. Hundreds of thousands of dollars later, the root cause of the outage was uncovered: IT staff chose not to test their firewall changes, bypassing their "burdensome" ITIL-based change management procedures. They were oblivious to the consequences.

Avoiding a firewall fire drill

Automation is the key to gaining control. It helps staff disengage from firefighting. It bridges agility with security to drive business-driven productivity.

The right automation solution automates manual, error-prone workflows. It allows changes to be made accurately, with clear visibility across complex network topologies, while focusing on keeping the business running effectively.

Automation helps teams track down potential traffic or connectivity issues and highlights risky areas. It can automatically pinpoint devices that require changes and show how to create and implement the changes.



To ensure the proper balance of business continuity and security, look for a firewall policy management solution that:

- Provide visibility of network traffic flows and network devices across complex, hybrid and multi-cloud network topologies
- Intelligently design firewall rules to eliminate redundant rules and reduce clutter and complexity.
- Eliminate mistakes and rework. Improve accountability for change requests.
- Proactively assess the impact of network changes to ensure security and continuous compliance.
- Identifies risky security policy rules and offers suggestions to de-risk your network environment
- Automatically pushes changes to devices

10 Steps to automate and standardize the firewall change-management process

Once a request is made, a change-request process should include these steps:

01 Clarify the change request and determine the dependencies. Obtain all relevant information (i.e., who is requesting the change and why).

02 Validate that the change is necessary. Many requests are unnecessary and already covered by existing rules.

03 Get proper authorization for the change. Make sure you understand the dependencies and the impact on business applications, and other devices and systems. This usually involves multiple stakeholders from different teams.

04 Perform a risk assessment. Before approving the change, thoroughly test it and analyze the results so as not to block desired traffic or compliance violations. Does the proposed change create a new risk in the security policy?

05 Plan the change. Assign resources, create and test your back-out plans, and schedule the change. This is also a good time to ensure that everything is properly documented for troubleshooting or recertification purposes.

06 Execute the change. Backup existing configurations, prepare target device(s) and notify appropriate workgroups of any planned outage and perform the actual change.

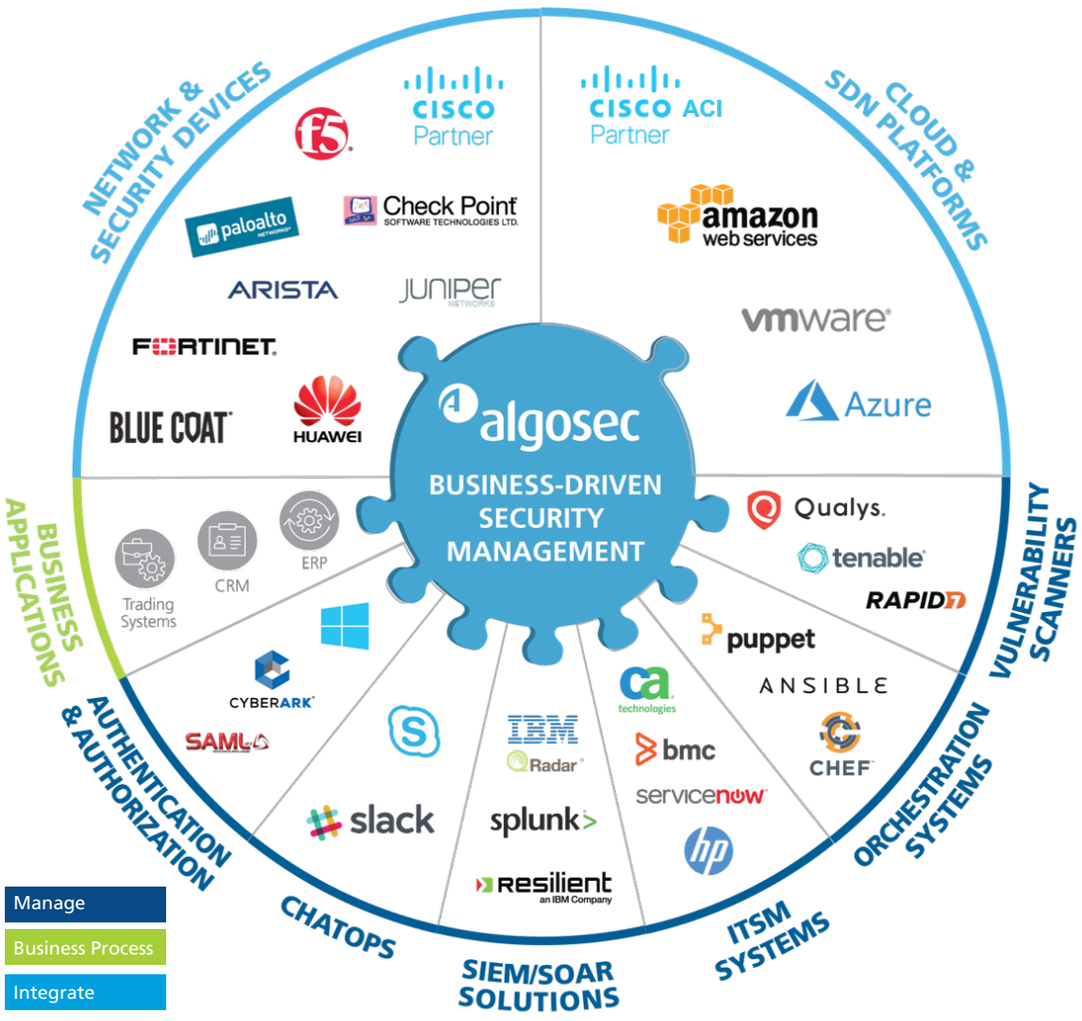
07 Verify correct execution to avoid outages. Test the change, including affected systems and network traffic patterns.

08 Audit and govern the change process. Review the executed change and any lessons learned. Having a non-operations-related group conduct the audit provides the necessary separation of duties and ensures a documented audit trail for every change.

09 Measure SLAs. Establish new performance metrics and obtain a baseline measurement.

10 Recertify policies. Part of your change management process should include a review and recertification of policies at a regular, defined interval (e.g., once a year). This step forces you to review why policies are in place, enabling you to improve documentation, and remove or tweak rules.

What to look for in a change-management solution



01 Your workflow system must be firewall- and network-aware. This allows the system to pull information from the firewalls and understand the current policies.

02 Your solution must support the firewalls, routers, security controls, load balancers, and other devices across your hybrid network.

03 Your solution must be topology-aware. It must understand how the network is laid out, comprehend how the devices fit and interact, and provide the necessary visibility of how traffic is flowing through the network

04 Your solution must integrate with the existing general change management systems. You don't want to undergo massive retraining of processes and systems simply because you have introduced a new solution.

05 Your solution must provide out-of-the-box change workflows to streamline change-management processes and be highly customizable. No two organizations' network and change processes are exactly the same.

Summary

While change management is complex stuff, the decision for your business is simple. You can continue to slowly chug along with manual change management processes or you can accelerate your processes with an automated network change management workflow solution that aligns stakeholders and helps your business run more smoothly.

Think of your change process as a key component of the engine of an expensive car (in this case, your organization). Would you drive your car at high speed if you didn't have tested, dependable brakes or a steering wheel? Hopefully, the answer is no! The brakes and steering wheel are analogous to change controls and processes. Rather than slowing you down, they actually make you go faster, securely!

Power steering and power brakes (in this case firewall-aware integration and automation) help you zoom to success.

> **Accelerate your business with security policy change automation**

AlgoSec enables the world's largest organizations to align business and security strategies, and manage their network security based on what matters most — the applications that power their businesses.

Through a single pane of glass, the AlgoSec Security Management Solution provides holistic, business-level visibility across the entire network security infrastructure, including business applications and their connectivity flows — in the cloud and across SDN and on-premise networks. With AlgoSec users can auto-discover and migrate application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate time-consuming security changes— all with zero-touch, and seamlessly orchestrated across any heterogeneous environment.

Over 1,800 leading organizations, including 20 of the Fortune 50, have relied on AlgoSec to drive business agility, security and compliance. **AlgoSec has provided the industry's only money-back guarantee since 2005.**

For more information, visit www.AlgoSec.com.

Did you know?

AlgoSec integrates with your existing business processes and multi-vendor security controls to keep your business safe and agile no matter where your network resides.