algosec

Secure application connectivity.
Anywhere.

Building trust in automation

Is automation advanced enough for cybersecurity experts?

An AlgoSec Whitepaper

Table of contents

Introduction

Managing large, modern networks has become increasingly complex in multi-cloud, multi-vendor environments. More connections mean more vulnerabilities which translates into increased risk of data breaches from cyber criminals, foreign powers, and inside actors. In addition, rapid business growth calls for new applications, new connections, new integrations and users, which requires constant change management that has a direct impact on security policies.

Adding to the challenge is that networks, security, and cloud resources are often working in silos, creating roadblocks that make policy change implementation and application connectivity even more difficult. Many leaders hesitate to implement automated change management because of concerns around visibility and oversight. But when multiple network security controls in an organization don't communicate with each other, it increases risk – 64% of companies face significant issues across various domains due to network deficiencies including poor detection, tracking, and remediation of security issues

It's time for cybersecurity experts to recognize that today's intelligent automation solutions have the ability to elevate change management from a manual labor-intensive process to one that securely responds with speed and precision.

Intelligent Automation provides a single source of visibility into security and compliance issues across a hybrid network environment in order to ensure ongoing adherence to internet security standards, as well as industry and internal regulations.

Secure application connectivity with automation

Most companies today have undergone a complete digital transformation – modernizing their networks and moving to a hybrid cloud in order to better support their application delivery pipeline. But this transformation comes with multiple challenges. As more applications are spread out across cloud and on-premise networks, there's decreased visibility which obscures existing applications and their connectivity requirements.

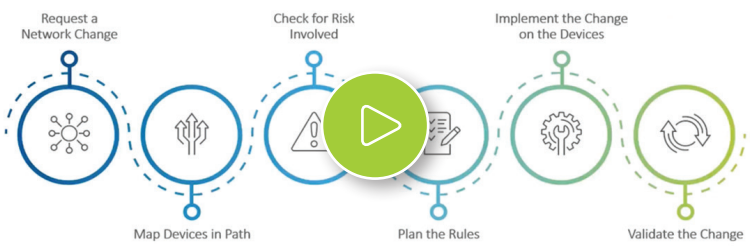
Another significant challenge is slow application changes that often take between three days and a week or longer, with one of the biggest bottlenecks being security policies. Many organizations have an informal change request process that relies on ticketing systems that can't handle complex requests. They also typically have network security teams and operations that work in silos. In this environment, communication is degraded leading to out-of-process firewall changes that result in system outages, exposure to data breaches, and costly audit failures.

To successfully automate network security policy changes without breaking core network connectivity, it's critical to have a strong foundation in place. This means you need to move away from an informal, siloed process and commit to standardizing how the organization manages network security policies.

Here's a roadmap to help you create a more formalized framework for automating the change process.

- **Request a network change:** The first step is to be clear about who is requesting the change. Typically, it's generated by either the application owner or a member of the DevOps team. These experts are constantly working on their applications – testing new features, building new networks, and trying out brand new applications which leads to a lot of change requests.
- **Map devices:** Many companies find this stage very difficult because identifying all of the security devices impacted, including firewalls, SDNs, and cloud security groups, is complicated when done manually. And sometimes it doesn't even need to be done – around 22% of requests are for things that already exist. In the remaining requests, some of the connectivity is allowed and some is blocked. Intelligent automation enables all of this to occur in seconds, providing the team with quick insights into what actions need to happen next, if any.
- **Check for risk:** Most companies have identified their network risk and created defined zones where connectivity is permitted. Intelligent automation recognizes where these zones exist and allows approved security changes to proceed without manual intervention. This frees up time for the team to focus solely on changes that present a risk.
- **Plan the rules:** Networks have multiple vendors and contracts that require tailored decision making. Many of them already have rules in place and creating a new rule can wreak havoc on firewalls and security policies. But, mistakes are all too common and sometimes there's not enough time to look for an existing rule, such as during outages. Automation scans the rule base to determine if a new rule needs to be created or if an existing one can be amended. This helps avoid duplications while also enforcing naming conventions and other best practices.
- **Implement the change:** There are two primary options when you want to implement changes on different firewalls, SDNs, or with cloud security groups. The first is where the change request is communicated to the device through REST API. The other is when the request is done directly to the device. With intelligent automation, all changes are pushed automatically, either through APIs or directly to the device.
- **Validate the change:** Automation ensures that all changes are implemented as requested and flags those that raise concerns. For instance, if the change is too wide, it exposes risk but if it's too narrow it may not satisfy the necessary requirements.

Check out our webinar:
Secure Application Connectivity with Automation

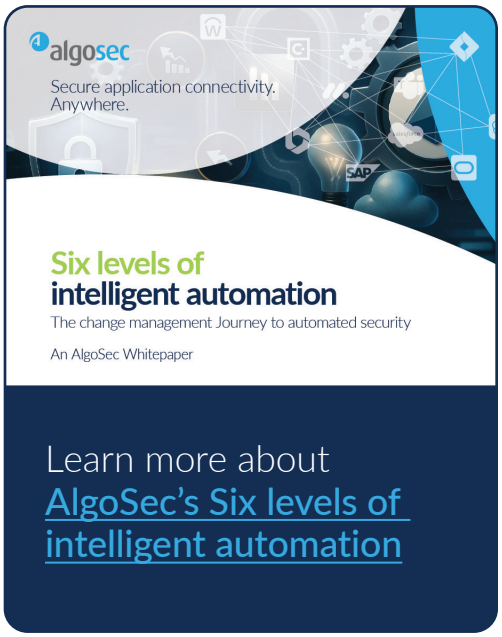


Another crucial component where automation is beneficial is keeping an audit trail of all changes, including all manual approvals. Not only will this enhanced level of documentation serve your compliance and audit requirements, but it can also help with troubleshooting and undoing changes if necessary.

Algosec safely automates every step of the change process

Fears around cyberattacks or non-compliance can be paralyzing and lead to sticking with the status quo of manual change management. Many security teams also have concerns about the pace at which they'll need to progress from manual to zero touch automation, and the potential to instantly lose visibility, control, and oversight.

AlgoSec helps its clients embrace a more sensible shift to intelligent automation – one that gradually reduces manual interventions through a phased process. Its Six Levels of Intelligent Automation is a customized process that allows organizations to move along the path to full automation at their own pace. At the same time, it provides comprehensive visibility into security and compliance issues across a hybrid network and helps ensure adherence to internet security standards, as well as industry and internal regulation.



As networks become increasingly more complex and advanced, manual interventions will become untenable. Automated change management will be an absolute necessity for businesses to maintain agility and security moving forward. It decreases human error, provides accurate documentation, saves time and money, and frees up IT and security teams to focus on critical innovation.

Enhance security with an automated change management process

Without automation, security is inefficient at best and dangerous at worst. Proactively reacting to constant alerts is difficult and manual changes are inefficient and error-prone which can result in risky misconfigurations.

By using intelligent automation for the change management process, AlgoSec enhances network security by:

- Providing immediate notification if a change violates a compliance guidance
- Assessing the risk level of each proposed policy change
- Decreasing rule redundancies to streamline firewall management
- Verifying if a change is allowable under current security policies
- Improving collaboration between IT and security teams
- Increasing the productivity of the IT and security staff

In a hacking event, intelligent automation supports security by:

- Making instant changes in response to events
- Providing comprehensive visibility into apps impacted
- Initiating isolation of exposed applications and resources

Real-world success stories

When it comes to security and compliance, it's imperative to get it right. A structured change management process that centers around intelligent automation is critical for enhancing business agility, accelerating incident response times, and reducing the risk of compliance violations and security misconfigurations. All aspects of the business benefit, including network security and operation, benefit when application connectivity is rapid and secure.

Here are three case studies that showcase how intelligent automation delivered results.

Adhering to strict regulatory requirements

A leading European financial institution struggled to meet strict regulatory requirements when using a manual firewall policy review that was time consuming and error prone. It was especially difficult to identify risky or overly permissive rules across the complex hybrid environment, environment and compliance audits were taking a significant amount of resources and time.

Solution: Automate the risk analysis process

Results:

- Identified thousands of high-risk rules
- Reduced overly permissive rules by over 40% in three months
- Cut compliance preparation time by 70%
- Improved overall security posture with faster remediation cycles

Undergoing a rapid digital transformation

A multinational retailer was undergoing a rapid digital transformation with frequent application updates and a need to meet PCI-DSS compliance. Frequent network changes introduced risk and delayed application deployment. At the same time, manual processes led to misconfigurations and compliance gaps and change requests were slow and lacked proper risk evaluation.

Solution: Automate risk checks and change processes with AppViz

Results:

- Reduced time to deploy secure application changes from weeks to hours
- Maintained continuous PCI-DSS compliance
- Proactively detected and blocked risky access paths before they were implemented

Managing a Multi-Vendor Firewall

Background: A large government agency supporting 20+ departments faced inefficiencies managing over 1,100 firewalls. Change request delays hindered operations across critical sectors like education, public safety, and transportation. By fully automating low-risk changes with embedded business context, the agency accelerated service delivery while maintaining control and audit details.

Solution: Automated change processes using AlgoSec FireFlow

Results:

- Reduced manual efforts by 80% through intelligent automation
- Quickly identified non-compliant rules and remediated them
- Streamlined audit readiness with automated reports and continuous policy monitoring

Exploring the opportunities ahead

Applications are at the core of all networks. They're crucial for fueling organizational growth and creating a competitive advantage. But because they're interconnected across multiple clouds and on-premises systems, they carry a high security and compliance risk. And the challenge is only going to grow as more applications are added, networks become increasingly complex, and security threats grow.

To remain agile and secure, companies need to implement intelligent automation as they move along the path toward Zero-Touch, or full automation, of their network change management. Ultimately, this will help them implement their Zero Trust security goals, which require all requests to be authenticated, authorized, and encrypted—regardless of where they come from.

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 10 times faster by automating application connectivity and security policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2200 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads. AlgoSec Horizon platform utilizes advanced AI capabilities, enabling users to automatically discover and identify their business applications across multi-clouds, and remediate risks more effectively. It serves as a single source for visibility into security and compliance issues across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Additionally, organizations can leverage intelligent change automation to streamline security change processes, thus improving security and agility. Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.

algosec