algosec

Secure application connectivity.
Anywhere.

Six levels of intelligent automation

The change management Journey to automated security

An AlgoSec Whitepaper

Table of contents

Introduction 2

The reality of automation 2

Demystifying automation in network change management 3

AlgoSec and the case for intelligent automation 4

What real world success looks like 5

Exploring the opportunities ahead 6

About AlgoSec 7

Introduction

Advances in automation continue to accelerate, promising to greatly increase network efficiency and scalability, enabling employees to pursue more strategic endeavors. Gartner predicts by 2026, 30% of enterprises will automate more than half of their network activities. In mid-2023 it was just 10%. At the same time, organizations are shifting to hybrid environments with both cloud and on-premise, networks, local and remote workers, and a mixture of different vendor solutions to manage.

In this dynamic environment, managing and securing enterprise application connectivity is an increasingly complex endeavor. To mitigate risk, some organizations are prioritizing application-centric security with an eye toward solutions that reduce complexity, improve interoperability, and enhance real-time visibility across hybrid environments. One critical component is a robust change management approach that minimizes network disruption and maintains a robust security posture.

While manual change management is still common in many organizations, it can cause inconsistent network changes and integration problems that introduce security risks. Automating the change management process provides IT teams with greater visibility into the configuration of every network device and enables them to ensure there are no security gaps in the network. Yet some organizations are reluctant to implement an automated change management process because they don't fully understand what the process entails. Additionally, application developers are leveraging cloud technology to shorten the time to develop and deploy; this is outpacing the traditional tempo of change requests from even a few years ago.

The reality of automation

Automating any process is overwhelming, but especially one that is vulnerable to cyberattacks such as network change management. It's important to understand that automation is not a quick flip of a switch, but a deliberate and controlled process. For context, it helps to look at self-driving cars. According to the Society of Automotive Engineers, we're far from fully autonomous cars as industry experts navigate the complexities of implementation. Goldman Sachs estimates that just 10% of global new car sales could be partially automated by 2030, which still returns self-driving cars to human control as necessary.

If today's companies were self-driving cars, many of their network automation systems would also be in the early stages. While they may be eager to advance to higher levels, they're often intimidated by the complexities of the implementation process and the pace by which it's accomplished. This puts unnecessary pressure on the organization by:

- Providing the C-suite with unrealistic goals and a false understanding of what success looks like
- Putting impossible expectations and timelines on IT teams, leading to frustration and disappointment
- Misrepresenting the existing capabilities and future potential of automation with employees and clients

Instead, organizations should take a step back to fully understand what automation can do now, where it's heading in the future, and what makes sense for the company.

Demystifying automation in network change management

When planning to implement or update automation in any business process, it helps to first unpack existing barriers. As an example, network change management is a business function that could greatly benefit from automation, but is slow to advance due to some entrenched concerns. Because tech teams are accustomed to manually planning, testing, and approving changes to their network infrastructure, they often fear losing control and visibility, which ultimately jeopardizes network continuity and safety.

But tech teams may shift their viewpoint if they fully understand how automation can help in daily operations. Here are some examples:

- **Optimizing complex systems:** For organizations to function and compete in the modern digital landscape, they need data to securely move through every branch of the business. Enterprise-wide automated change management seamlessly manages the process between a network alert and the action needed, while automatically addressing security issues that currently require constant manual attention.
- **Securing the flow of data:** Automation enhances business agility and security while reducing misconfigurations caused by manual, ad-hoc change management processes. It also proactively identifies security policies across the network that will block access; provides risk analysis; and reveals where there are compliance vulnerabilities.
- **Integrating hybrid networks:** Gartner predicts that 90% of organizations will adopt a hybrid cloud approach by 2027. With cloud and on-premise networks, plus multiple vendors, it's increasingly difficult to manage enterprise-wide change management using manual processes. Automation builds architectures that reduce complexity, improve interoperability, and enhance real-time visibility across hybrid environments.
- **Elevating the employee experience:** Manual interventions are repetitive, time-consuming, costly, and susceptible to errors. These factors add pressure and risk to tech teams that can impact job satisfaction and retention. Automation can reduce many of these common tasks and free up employees to focus on higher value, strategic activities that are more rewarding.

LEARN MORE ABOUT THE LEVELS OF INTELLIGENT AUTOMATON

Ultimately, automation provides reliable, continuous, and secure connectivity that benefits the organization, its customers, and its employees.

AlgoSec and the case for intelligent automation

Intelligent automation combines AI with other advanced technologies to automate and streamline complex, repetitive tasks. It 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.

AlgoSec's approach to change management leverages intelligent automation and is characterized by six distinct levels, where each level is defined by how much human interaction is required. As organizations gain experience and confidence, they continue on their journey from manual change management to a fully automated security management solutions.

Here's a brief look at each level of automation as it moves towards reducing manual interactions, helping users get more comfortable with automation along the way:

LEVEL 1

Manual Control

At the initial stage, security operators are primarily responsible for planning and executing network-related tasks. AlgoSec provides essential visibility tools that offer insights into network structures, security policies, and potential risks.

LEVEL 2

Assisted control

Security operators are introduced to a security management solution that includes a structured workflow to facilitate efficient task execution. While the workflow can be audited, operators continue to manually carry out various activities within the provided framework.

LEVEL 3

Partial automation

This is the transition towards intelligent automation where security operators receive assistance from AlgoSec's policy management but own responsibility for change validation and approval.

LEVEL 4

Conditional automation

In this stage, the security operator's workload decreases and rule changes are being implemented automatically on the different devices. Risk is automatically identified and the operator's focus shifts toward validating and authorizing the recommended modifications.

LEVEL 5

High automation

By creating a customized risk profile, the security management solution automatically handles low-risk changes, freeing up security operators to focus on critical tasks. Integration with external solutions is recommended for a more tailored and sophisticated approach to automation.

LEVEL 6

Very high automation

At the highest level, AlgoSec's policy management solution processes the majority of change requests submitted. While security operators still play a role in specialized cases, this level of automation allows the solution to operate seamlessly, ensuring a highly efficient and reliable network environment.

Throughout the process, AlgoSec centers each organization's unique operational capabilities and philosophical perspectives, including customizing the automation process to create a tailored approach and timeline. The goal is to help organizations fully understand the individual levels and their value prior to continuing on the automation journey.

What real world success looks like

Results matter. The C-suite wants to see ROI and proof that the security management solution is differentiating the organization in the marketplace. The tech team wants to feel confident that it will not only be secure and reliable, but free them up to pursue strategic goals that advance the company and their careers. The rest of the organization wants to know they can trust the system to run smoothly without interrupting their day-to-day workload.

Here are three case studies that illustrate how the six levels of intelligent automation helped transform different business processes.

Streamline Firewall Management

LEVEL 2: Assisted control → LEVEL 4: Conditional automation

A global IT services provider operating in more than 20 countries was managing firewalls from various vendors. Manual processes for rule cleanup, risk evaluation, and audit preparation were slowing down operations and introducing risk.

At Level 2, its rule base cleanup was entirely manual and risky with assessments depended on individual expertise. Additionally, ISO 27001 compliance reporting was time-consuming for the team. By transitioning to Level 4 with intelligent automation, the organization automated rule analysis, policy tuning, and change validation to reduce manual overhead and risk.

Results achieved:

- Cut planning and implementation time by 50%
- Saved five hours per change request
- Improved performance and visibility across firewall estate
- Streamlined compliance with automated audit-ready reports

Gain a holistic view of a hybrid network

LEVEL 3: Partial automation → LEVEL 5: High automation

A leading financial services provider operating hundreds of firewalls and thousands of virtual machines in a hybrid multi-cloud environment needed to improve its change management process while maintaining visibility and compliance.

The Level 3 partial automation lacked full visibility across the hybrid network and manual processes were still needed for validation and risk checks. Additionally, application connectivity was not mapped or understood end-to-end. Level 5 delivered an application-aware automation platform to unify visibility and policy changes.

Results achieved:

- End-to-end visibility across cloud and on-prem networks
- Automated application discovery and change simulation
- Reduced time and errors in policy provisioning
- Improved compliance posture across all environments

Automate security at scale

LEVEL 4: Conditional automation → LEVEL 6: Very high automation

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.

Results achieved:

- Reduced change processing time from 3 months to 2 weeks
- Streamlined onboarding and provisioning across departments
- Improved scalability and policy consistency across 1,000+ devices
- Enhanced responsiveness to agency needs while reducing risk

Exploring the opportunities ahead

In our complex and competitive world, organizations are constantly being tasked to deliver more and do it faster. Intelligent automation is critical for ongoing success in this environment. But organizations need to stay informed about emerging technology, manage expectations around their capabilities, embrace smart change, and navigate employee resistance with empathy and facts.

For many companies, the automation road will ultimately lead to Zero Trust network security, which we'll explore in a future e-book. The goal is to help businesses move toward robust, policy-driven automation that ensures continuous protection for business-critical applications while enhancing overall operational efficiency.

How AlgoSec's Six Levels of Change Management can benefit your organization

Speak with one of our experts

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

© AlgoSec Inc. All rights reserved. AlgoSec and the AlgoSec logo are registered trademarks of AlgoSec Inc.
All other trademarks used herein are the property of their respective owners.