KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | November 2017

AlgoSec Security Management Suite

AlgoSec Security Management Suite is a highly automated and business-focused integrated solution for managing network security policies and business application connectivity across a wide range of devices in heterogeneous environments.

by **Alexei Balaganski**
ab@kuppingercole.com
November 2017

Content

Related Research

Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network – 72163

Advisory Note: Plant Automation Security – 71560

Advisory Note: Sustainable Infrastructures through IT Compliance – 72025

Survey: State of Organizations – 74003

1 Introduction

AlgoSec is a privately held software development company headquartered in Ridgefield Park, New Jersey, USA. Founded in 2004 with the initial focus strictly on firewall management solutions, the company has long outgrown this legacy market and now provides a comprehensive suite of products for network security policy management across a broad range of security devices, both on-premises and in the cloud. With offices all over the world, the company has a strong global market presence, serving over 1500 customers worldwide, including large enterprises, managed service providers and consultants.

With the increasing pace of business in the age of Digital Transformation, achieving greater agility and efficiency of business processes is becoming one of the key challenges for IT. Companies are under constant pressure to support new digital transformation initiatives, to expand to the cloud and mobile platforms and to open their network perimeters to numerous new communication channels. Instead of a single perimeter we now have thousands of them, and thousands of security products to deploy and operate across a distributed heterogeneous IT landscape.

Unfortunately, the resulting dramatic increase in complexity of heterogeneous IT infrastructures combined with the growing sophistication of cyberthreats has made security a real bottleneck to business. Enterprises are simply unable to address the modern threat landscape and often fall victim to ransomware attacks, security breaches or malicious insiders. A massive skills gap is often cited as the reason for it: companies are forced to constantly deploy new cybersecurity products, many of which are still largely rely on manual operations by teams of experts who are in increasingly short supply.

However, the bigger problem for IT security nowadays has more to do with the fact that just like all other aspects of IT in a modern organization, it must align with business requirements. Without the important business context, a security infrastructure quickly becomes disconnected from the corporate assets it’s designed to protect, and is overwhelmed by thousands of irrelevant security alerts and false positives. At the same time, a security tool that does not provide meaningful analysis for business people would probably not get much support at the boardroom level. Finally, without a set of business-relevant performance indicators, justifying a budget increase for a much-needed improvement of a security infrastructure becomes even more problematic.

AlgoSec addresses these challenges with an integrated solution for business-driven security policy management for your corporate network infrastructure. With its unique business-oriented approach, the solution not only provides unified visibility across on-premises, software-defined and cloud networks for a wide range of network devices and security products, but incorporates business applications and connectivity flows between them into the big picture as well.

With intelligent automation controls, the solution supports complete lifecycle management for network security policies – from discovering application connectivity requirements, assessing potential risks, performing changes, monitoring, optimizing and finally decommissioning legacy rules. An integrated set of modules provides full coverage from low-level firewall rule management to high-level business risk assessment and continuous compliance.

2 Product Description

A fundamental purpose of a network security policy management solution is to provide full and constant visibility into all information flows across the corporate network infrastructure. It also needs to enable administrators design and manage rules for these flows that conform to corporate security and compliance regulations, as well as ensure that a change to a rule does not compromise a business application's availability, security or compliance. In a sense, this is what network administrators, security and application teams have been doing for decades, largely manually and usually completely separate from each other.

With its business-driven approach towards security management, AlgoSec provides a solution that's highly integrated, both between its individual modules and with a wide range of third party security products, highly automated to improve administrator's productivity and to eliminate human errors, and highly focused on business requirements like application connectivity, risk assessment and compliance management. The company's solution provides automation controls for the whole lifecycle of a security policy, from initial discovery of the underlying security infrastructure to application-centric connectivity management, to proactive risk assessment including vulnerability and cyberthreat management, to automated change management, and finally to recertification and decommissioning of redundant rules.

This closed loop process, where each step is automatically proactively analyzed, optimized, implemented and validated with a full audit trail, not only ensures that the risk of an outage due to an error is reduced practically to zero, but also provides continuous security and compliance monitoring and greatly simplifies various business tasks. Provisioning connectivity for new applications, migrating them between on-premises and the cloud or isolating a system as a part of incident response to a cyberattack can take minutes instead of days, since everything but an executive decision can be automated.

Architecturally, AlgoSec's product suite comprises three modules, which can roughly be differentiated by the level of abstraction they are dealing with: from the foundational network infrastructure management all the way up to business application connectivity. Both on-premises deployments as hardware or software appliances as well as cloud deployments as Amazon Machine Images are available. Multiple "slave" instances can be deployed for large-scale projects, high availability and disaster recovery scenarios are supported as well. Although the modules can be licensed independently, together they form an integrated solution with a common administration console and seamless switching between them.

AlgoSec Firewall Analyzer is the foundational module of the solution, providing automated network topology discovery, firewall ruleset analysis and optimization and centralized policy management across heterogeneous network environments. This product originates from the company's decade-long experience in firewall management, however over the years it has evolved to support a wide range of other security products.

Besides all leading brands of "traditional" and next-generation firewall, the Firewall Analyzer supports numerous routers, load balancers and web proxies as well as management controls of cloud (Amazon Web Services and Microsoft Azure) and SDN (VMware NSX, Cisco ACI) platforms. In addition, AlgoSec

Extension Framework allows customers to add support for new network devices without coding, just by creating new device configurations, which can be shared with the AlgoSec community for change monitoring, baseline compliance and routing analysis. Full policy analysis may require some coding, or can accommodate third party plug-ins independent from Algosec code

By creating a dynamic map of the existing network topology and by enabling centralized and vendor-independent security policy management across all devices, the product provides full visibility into traffic flows in the network, as well as the ability to analyze the potential impact of any change in a security policy. Thus, an administrator can easily visualize current issues, plan necessary changes, and assess potential risks.

For firewall administrators, the product provides a range of intelligent analysis, which can detect unused or duplicate firewall rules, overly permissive access and other risky rules. It also significantly simplifies designing and enforcing network segmentation for security and compliance purposes, as well as ensures that no policy change violates existing segmentation.

For more business-focused users, Firewall Manager provides predefined comprehensive audit-ready compliance reports for industry regulations like PCI DSS, HIPAA or NERC as well as the means for creating custom reports. An extensive built-in database of industry best practices allows the product to perform instant risk assessment of any existing policy or any change before it’s implemented.

AlgoSec FireFlow is the module that provides automation capabilities for security policy change management, meaning it automatically applies the new policies and policy changes, across the entire network. Instead of manually managing configurations for various network and security devices, administrators can utilize FireFlow to completely automate the whole policy change lifecycle: its design, risk analysis, implementation, validation and auditing. Policy management workflows can be set to run completely automatically, without any human involvement – thus reducing the process to seconds instead of days.

Alternatively, each step can be configured to require manual approval with complex logic. In any case, every step is fully documented for accountability and compliance purposes. Needless to say, all change requests are analyzed proactively according to the built-in risk knowledge base to ensure compliance with industry regulations or company’s own policies. In the end, all necessary changes on each device can be implemented automatically, saving time and reducing the “human factor” risks.

On top of the “basic” workflow management, FireFlow offers a number of intelligent features that improve both performance and stability of the underlying infrastructure and productivity of the administrators. For example, by constantly comparing the current configuration of each firewall with the state of opened change requests, the product can detect when the change is implemented and close the corresponding ticket automatically. On the other hand, it can detect rogue changes, which were made manually outside of the workflow and generate an alert and prevent the corresponding ticket from closing.

FireFlow supports leading IT Service Management products like ServiceNow, Remedy and HP Service Manager to integrate its workflows into existing change management systems. Additional integrations can be implemented as a professional service.

AlgoSec BusinessFlow is the module responsible for discovery, provisioning, managing and eventual decommissioning of network connectivity for business applications. This module implements a more business-oriented approach towards network security policy management by letting administrators manage applications as whole business assets instead of configuring each network flow separately.

BusinessFlow does not require any prior knowledge about network infrastructure or applications and does not need any manual configuration: it discovers all enterprise applications and their connectivity requirements automatically. Administrators then have access to an interactive map, where all applications and traffic flows can be monitored, reconfigured or analyzed for problems.

Any change requests in application connectivity can be managed using an intuitive graphical interface that does not involve managing underlying network infrastructure – all the necessary changes are automatically translated into access rules for the FireFlow module.

BusinessFlow natively supports DevOps best practices by managing application connectivity through the various stages – from development to testing to production. The product can automatically adjust connectivity for each environment and ensure that isolation between them is maintained at all times. For DevOps specialists, it provides advanced monitoring and analysis capabilities.

Another popular use case for BusinessFlow is supporting large-scale migration projects – to a different data center or into the cloud. It provides automation for all stages: identifying relevant applications and their connectivity, automating policy changes, risk and compliance assessment, tracking the execution and finally removing the connectivity that is no longer needed.

By integrating with popular vulnerability scanners like QualysGuard or Nessus, the product can aggregate application vulnerability information and correlate it with network connectivity to provide more relevant risk assessments, and then prioritize remediation actions for security teams or help mitigating an issue with an appropriate security policy change.

As an integrated suite, AlgoSec's solution provides a comprehensive solution for all your network connectivity and network security policy management needs with an impressive level of intelligent automation. However, it does not end there – it can and should become a part of the company's global security infrastructure. Integrating with popular SIEM solutions, AlgoSec can help correlate security incidents to specific business assets impacted by them as well as to the security devices that can mitigate them. Not only this information helps security analysts prioritize their actions based on risk assessments, the solution can automatically isolate compromised servers from the network to contain the threat quickly.

3 Strengths and Challenges

Building upon its decade-long expertise in firewall management, AlgoSec now offers a comprehensive, highly integrated, scalable and automated solution for network security policy management across multiple network devices and security products in heterogeneous environments.

Although the declared purpose of the solution may sound a bit too technical first, the company's focus on intelligent automation, integration with numerous third-party products and addressing business-level challenges and requirements ensures that the resulting product is well-suited as a collaboration platform between network, security, application and DevOps teams, where they can address the ever-changing business requirements and mitigate new cyber-risks together. By integrating with SIEM solutions, the suite can become an integral part of the corporate security infrastructure, supporting forensic analysis and mitigation of cybersecurity incidents.

In its current form, the solution is primarily focused on managing network infrastructure devices and thus has a fairly specialized focus with regards to true enterprise-wide security management. However, the product is being actively developed, adding support for additional security tools and cloud provider APIs. A look at the company's roadmap reveals continued focus on orchestration and automation for cloud-based (and especially cross-cloud) workflows.

AlgoSec Security Management Suite can be recommended to any company with a medium to large complex network infrastructure as an excellent network security policy management solution and a valuable addition to the existing security infrastructure.

Strengths	Challenges
● Supports a wide range of network devices and security products on-premises and in the cloud, extensive API integrations ● Application connectivity impact analysis for business risk prioritization and management and faster application delivery ● Complete security policy lifecycle management with full automation capabilities ● Multiple intelligent automation features for improving performance and productivity, ● Integrations with leading vulnerability scanners, SIEM solutions, ticketing systems ● Strong focus on business enablement across multiple teams, risk assessment and compliance	● Comprehensive, but fairly complex tool, primarily targeted at large organizations with heterogeneous environments ● Quite specialized focus on network infrastructure management, limited security capabilities beyond that

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com