THE BUSINESS CASE FOR NETWORK SECURITY POLICY MANAGEMENT

Quantifying the Annual Savings with the AlgoSec Security Management Solution

An AlgoSec Whitepaper

BUSINESS-DRIVEN
SECURITY MANAGEMENT

Ensure Quantifiable Savings with the AlgoSec Security Management Solution

Looking at IT security through an ROI lens is a hard sell to make. Organizations do not get credit for protecting data or for keeping the business running, only take the fall if data is lost or stolen, or business is disrupted. Security is like an insurance policy for which you hope to never have to file a claim. It is there to minimize the risk and/or impact of an unfortunate event. While arguing a positive ROI on security is typically a non-starter, you can however, show quantifiable savings around how you MANAGE your security policies.

The AlgoSec Security Management Solution provides IT security and operations teams with visibility and control of network environments – even complex and geographically dispersed networks with multi-vendor firewalls – through the intelligent automation of firewall policy management.

AlgoSec manages complex network security policies throughout their lifecycle— from discovering application connectivity requirements, through ongoing change management and proactive risk analysis, to secure decommissioning. With powerful visibility across firewalls and cloud security controls, AlgoSec simplifies, automates and orchestrates security policy management to accelerate application delivery while ensuring security and continuous compliance across the enterprise.

Automating business processes relating to security management provides organizations quantifiable savings in terms of personnel time by freeing up staff to focus on more strategic, business-critical tasks. This paper will examine five business challenges that many organizations face and present a savings calculation and business justification based on operational efficiency that can be used to facilitate budget approval. In addition, this paper will examine less tangible benefits of network security policy management, such the prevention of network outages, data loss, etc.

Throughout this paper, we will calculate expected savings for a medium/large environment with the following characteristics:

- 50 network firewalls
- A loaded IT cost per hour of $60 (i.e. the cost to the organization)
- 1,200 change requests per year (2 changes per firewall per month)

These average estimates are meant to give you an idea of the potential savings, but you should calculate your own savings based on your organization's specific environment and costs. To request a calculation that is tailored to your environment, please visit https://www.algosec.com/roi-calculator/.

Business Justification #1: Reduce the Cost of Audits and Audit Preparation

Organizations are increasingly subject to corporate governance and compliance requirements. Even if an organization does not have to comply with specific government or organizational standards, it is now commonplace to conduct regular, thorough firewall audits. This not only helps ensure that firewall configurations meet the correct criteria for an external standard or internal security policy, but a firewall audit can also play an important role to reduce overall risk factors and actually improve firewall performance by its inclusion of certain tasks such as optimizing the firewall rule base.

In today's network environments, which typically include thousands of firewall rules, the ability to complete a manual audit of the firewall has become, as Forrester Research puts it, "nearly impossible". When this process is conducted manually, the firewall administrator has to rely on his own experience and expertise — which can vary greatly across organizations — to determine if a firewall rule should or should not be included in the configuration file.

Furthermore, if performed manually, documentation of rules and/or rule changes is usually lacking. The time and resources required to pour through all of the firewall rules and determine compliance/non-compliance significantly impacts IT staff.

Instead of a manual review, in which it can take a significant amount of time to produce a report for each firewall in the network, AlgoSec enables organizations to automatically generate compliance reports and reduce audit preparation time by 80%.

AlgoSec provide out-of-the-box compliance reports for the standards such as PCI-DSS, SOX, NERC CIP, ISO 27001 and Basel II. AlgoSec aggregates data across a defined group of firewalls and devices for a single compliance view, instead of running reports for each individual device, saving a tremendous amount of time and effort that may be wasted on collating individual device reports.

"With AlgoSec we can now get, in a click of a button, what took two to three weeks per firewall to produce manually."

Marc Silver, Security Manager, Discovery SA

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements	AlgoSec Feature	Setting	Details	Status
1.1 Establish firewall configuration standards that include the following:				
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configuration	Change Management	On	The AlgoSec FireFlow product performs a "what-if" risk check on every change request (prior to implementation). To learn more about AlgoSec FireFlow please visit the AlgoSec web site, or contact your AlgoSec representative. Algosec FireFlow is licensed in your environment.	✓
	ActiveChange	On	The AlgoSec ActiveChange technology can be used in order to changes firewall configuration. Algosec ActiveChange feature is licensed in your environment.	✓
	Change History	On	No previous records available	✓
	E-Mail Notification	Off	These users get an email when the following occurs: None	✗
1.1.2a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Connectivity Diagram	On	 The connectivity diagram is current as of 2015-12-01	✓
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	Network Map	On	The Network Map tab on AlgoSec web interface homepage allows running a routing query to trace problems of traffic traveling from and to specific IP addresses.	✓
	BusinessFlow Application Diagram	On	The AlgoSec BusinessFlow product includes a visual representation of every applications' flows in an Application Diagram. To learn more about AlgoSec BusinessFlow please visit the AlgoSec web site, or contact your AlgoSec representative. Algosec BusinessFlow is licensed in your environment.	✓
1.1.4a Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	-	-	Verify that firewall configuration standards include this requirement	*
1.1.4b Verify that the current network diagram is consistent with the firewall configuration standards	Connectivity Diagram	On	Review the connectivity diagram and verify that this requirement is met	*
1.1.4c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	Connectivity Diagram	On	Review the connectivity diagrams and verify that this requirement is met.	*
			Verify that device configuration standards include this requirement.	

Figure 1: Example of a PCI DSS firewall compliance report automatically generated by AlgoSec.

Savings Calculation:

Below are the costs for undergoing an audit with and without AlgoSec, and the potential savings.

Without AlgoSec:

# of firewalls	# of hours to audit each firewall (80% reduction)	Average cost/hour for staff	TOTAL
50	40	$60	$120,000

With AlgoSec:

# of firewalls	# of hours to audit each firewall (80% reduction)	Average cost/hour for staff	TOTAL
50	8	$60	$24,000

*****AlgoSec reduces the time to audit each firewall by 80%, for a total savings per audit of $96,000. Assuming two audits per year and the annual savings is $192,000.**

Business Justification #2: Reduce Time Required to Process Firewall Changes

Many organizations struggle with change processes. Relying upon manual processes minimizes business agility because it typically takes too long to process a change, which often involves members from multiple departments (security, security operations, network operations, audit, etc.).

By automating previously manual processes, organizations can save time and resources - ultimately enabling IT to respond more quickly to evolving business requirements. AlgoSec customers reduce the time required to process a firewall change by more than 50%. This is achieved using intelligent automation - from pinpointing the exact devices that need to be changed, to proactively assessing the risk and designing the change in the most optimal way.

About 25% of performed firewall changes are not necessary, and many others are implemented incorrectly. AlgoSec helps organizations become more operationally efficient by automatically identifying and closing "already works" requests, while ensuring changes are performed exactly as requested. Additionally, by avoiding adding unneeded rules to the policy, organizations can achieve significant savings from future clean-up projects.

Savings Calculation:

Below are the annual costs for managing change requests with and without AlgoSec, and the potential savings.

Without AlgoSec:

# of change requests/year	Average time (hours) spent per change*	Average cost/hour for staff	TOTAL
1,200	4	$60	$288,000

With AlgoSec:

# of change requests/year	Average time (hours) spent per change*	Average cost/hour for staff	TOTAL
900	2	$60	$108,000

*****AlgoSec dramatically reduces the time to process change requests, which correlates in this example to $180,000 in annual savings.**

Business Justification #3: Save Time Troubleshooting Connectivity Problems

In today's always-on business environment, it is critical to quickly respond to and remediate connectivity issues. Enterprises and MSPs cannot afford to have downtime, which directly and indirectly impacts the bottom line:

- Directly - The inability to process transactions results in loss of business
- Indirectly – The number of personnel hours needed to identify the cause of a problem and remediate

With network environments growing in complexity (i.e., multiple-firewall, multiple-vendor environments; traditional, next-generation and hypervisor-level firewalls, etc.), this has become very challenging for most organizations. AlgoSec enables administrators to easily determine if the connectivity problem is caused by a firewall or group of firewalls and if so, allows the troubleshooter to immediately restore connectivity. Using AlgoSec's troubleshooting query function to identify the cause of the connectivity issue, organizations can typically reduce the time taken to debug an issue by more than 50% of what was traditionally required.

Savings Calculation:

Below are the annual costs for managing change requests with and without AlgoSec, and the potential savings.

Without AlgoSec:

# of change requests/year	Average time (hours) spent per change*	Average cost/hour for staff	TOTAL
4	500	$60	$120,000

With AlgoSec:

# of change requests/year	Average time (hours) spent per change*	Average cost/hour for staff	TOTAL
1	500	$60	$30,000

***AlgoSec dramatically reduces the time to troubleshoot connectivity issues, which correlates in this example to $90,000 in annual savings.**

Business Justification #4: Extend the Lifespan of Your Hardware

Having been deployed for several years, most firewall policies are cluttered, and contain many rules which are no longer needed by the business. In addition to increasing the likelihood of misconfiguration, this clutter negatively impacts the firewall performance, requiring the firewall to process a significant amount of rules until a rule that "matches" the traffic is found. Ultimately, organizations are required to invest in costly hardware upgrades to counteract the degradation in performance.

AlgoSec enables organizations to optimize and clean up cluttered policies with actionable recommendations to consolidate similar rules, discover and remove unused rules and objects, as well as shadowed, duplicate and expired rules. In addition, AlgoSec provides recommendations for reordering rules for optimal firewall performance, moving commonly used rules higher in the policy, while retaining policy logic.

All of this allows organizations to save on or postpone expensive hardware upgrades, and effectively increase the lifespan of the existing hardware.

Business Justification #5: Less Quantifiable Benefits

The first four business cases of this paper focus on the operational and quantifiable benefits of deploying a solution such as AlgoSec. However, while hard to quantify, there are significant benefits from this solution that should be examined, which include:

- **Improved productivity and improved network uptime.** If a misconfigured firewall rule takes the network down and thus the business offline, the impact goes well beyond the operational aspect of troubleshooting connectivity issues – an outage could mean that business transactions cannot occur, which impacts the bottom line. AlgoSec enables organizations to eliminate firewall misconfigurations, ensuring that the SLAs are maintained and that the business is "always-on".

- **Improved risk mitigation and data protection.** Today's attackers are targeting sensitive, valuable information. Not only does a data loss event cause significant operational cost in terms of incidence response, notifying customers, etc., it also typically results in a loss of customers. With the firewall as the first line of defense, ensuring that overly permissive rules are tightened and that risky rules are quickly remediated can help reduce the chance of these unfortunate events.

- **Improved business agility.** Organizations in which IT operations and security teams are not aligned typically lack the necessary agility to adapt to changing business requirements, which can be a significant competitive advantage. Through AlgoSec's intelligent automation of firewall policy management, organizations can not only be more efficient in their operations, but also use that newfound time to focus on ways to improve the business.

- **Improved corporate governance and regulatory compliance.** Ensuring continuous compliance and thus avoiding penalties for non-compliance with regulatory or industry-mandated requirements (i.e. NERC CIP fines can be as high as $1 million/day) has a significant impact on the organization's bottom line. AlgoSec's out-of-the-box compliance reports give an organization a real-time view of all the firewalls in the environment and the status per the requirements to minimize the risk of penalties for non-compliance.

"AlgoSec now does the heavy lifting for us. It allows the engineers to focus more on providing greater levels of security than on process and change, so we're able to provide a much more secure infrastructure for BT." **Phil Packman, GM Security Gateway Operations, BT**

Conclusion

Although it may be hard to sell ROI for security, there are quantifiable savings, immediately available in Year 1, when implementing a network security policy management solution such as AlgoSec. Reviewing the business cases presented in this paper, the total quantifiable savings from implementing AlgoSec are:

Business Justifications	Annual Savings in $
Reduction in Audit Preparation Costs (assuming 2 audits per year)	$192,000
Reduction in Change Request Processing Time	$180,000
Reduction in Troubleshooting Resolution Time	$90,000
Extended Lifespan of Hardware	$57,750
Annual Savings	**$519,750**
3 Years Savings	**$1,559,250**

About AlgoSec

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.