



www.algosec.com

AlgoSec

Security. Visibility. Governance.

ALGOSEC WHITE PAPER

Automating Firewall Audits for CIP Compliance

AlgoSec automates and lowers cost of compliance with NERC reliability standards for firewalls – and protects Critical Cyber Assets of the Bulk Electric System

AlgoSec Inc, Algorithmic Security, AlgoSec Firewall Analyzer and the AlgoSec logo are trademarks of Algorithmic Security Inc. All other trademarks are property of their respective holders. For more information about AlgoSec visit: www.algosec.com

Introduction

The threats to critical cyber infrastructure for the bulk electric system are well known to all Registered Entities in North America. Threats may spring from hackers, criminals, sovereign states, or terrorists, and the fallout could be disastrous if an exploit stopped delivery of electric power. In response, the North American Electric Reliability Corporation (NERC) was formed to “ensure that the bulk power system in North America is reliable.” The system includes 211,000 miles of high-voltage transmission line serving 334 million people. NERC has created Critical Infrastructure Protection (CIP) Reliability Standards to help Registered Entities minimize vulnerabilities. After years of preparation, Registered Entities must now prove their controls conform to CIP standards. “Auditable Compliance” is required by 30 June 2010 with conformance to broad, intricate standards for security technology. The processes for CIP compliance – especially with complex deployments of firewalls – are time-consuming and expensive without using automation.¹

This paper describes requirements of CIP, with a focus on automating CIP audits for firewalls. By using a firewall audit tool such as from AlgoSec, Registered Entities can cost effectively automate the audit and documentation process – with instant, real-time snapshots of CIP compliance for all firewalls operated by the organization. Verification of compliance also shows that a Registered Entity is providing optimal firewall protection for the bulk electric system.

NERC Timeline

- 1968** Formed as North American Electric Reliability Council with committee-driven development of standards to protect the bulk electric system.
- 2005** Energy Policy Act of 2005 triggered formation of an “Electric Reliability Organization” to develop and enforce mandatory compliance with standards.
- 2006** NERC was granted this designation. Submitted Critical Infrastructure Protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1.
- 2009** NERC approved CIP version 2 and began audits.
- 2010** “Auditable Compliance” required of all Registered Entities by 30 June 2010. Non-compliance may result in substantial daily fines per violation.

Now Is the Time for CIP Audit Readiness

By now, Registered Entities have had several years to implement CIP standards. Organizations ought to be well past the “what should we buy” stage; hopefully they have finished most, if not all control deployments. NERC is now engaged in three kinds of compliance activities. These include compliance monitoring, compliance enforcement, and managing a due process for contestations by Registered Entities who receive audit violation findings. NERC relies on Regional Entities to enforce CIP standards with bulk power system owners, operators, and users. Auditable compliance is required by 30 June 2010.

¹ John Kindervag, *Market Overview: Firewall Auditing Tools* (Forrester: July 30, 2009).



Guidelines for CIP compliance are specified in the [NERC Compliance Monitoring and Enforcement Program: 2010 Implementation Plan](#). NERC expects all Registered Entities to be subject to self-certifications on CIP requirements for the past year. Inability of passing an audit (including remediation of outstanding critical issues) can result in substantial [financial penalties](#) to each Registered Entity, depending on [severity level](#).

CIP Reliability Standards

All Registered Entities must comply with CIP Reliability Standards. CIP consists of eight categories of controls for securing critical cyber assets that protect the bulk electric system. These are:

CIP-002-2 Cyber Asset Identification. Requires identifying and documenting Critical Cyber Assets supporting reliable operation of the bulk electric system. Process is done with a risk-based assessment.

CIP-003-2 Security Management Controls. Requires deployment of minimum security management controls to protect Critical Cyber Assets.

CIP-004-2 Personnel & Training. Requires employees, contractors and service vendors with cyber or physical access to Critical Cyber Assets to have an appropriate level of personnel risk assessment, training, and security awareness.

CIP-005-2 Electronic Security Perimeter(s). Requires identifying and protecting the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, and all access points on the perimeter.

CIP-006-2 Physical Security. Requires implementation of a physical security program for protecting Critical Cyber Assets.

CIP-007-2 Systems Security Management. Requires defining methods, processes, and procedures for securing Critical Cyber Assets, and non-critical Cyber Assets within the Electronic Security Perimeter(s).

CIP-008-2 Incident Reporting and Response. Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

CIP-009-2 Recovery Plans for Critical Cyber Assets. Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

Details for CIP standards are on the NERC website at <http://www.nerc.com/page.php?cid=2|20>



Demonstrating Firewall Compliance for CIP Auditors

When the auditors arrive, they will be verifying a broad range of cyber controls for the eight CIP standards. Our focus here is compliance with CIP standards related to firewalls. The firewall is one of the oldest security technologies, and it remains one of the most vital controls for protecting Critical Cyber Assets. A firewall is the first line of defense. It controls computer traffic into and out of a Registered Entity's network – and into critical areas within the network. If a Registered Entity's firewalls are not properly configured and managed, that organization may well have to react to a disaster much bigger than failing the CIP audit.

Unfortunately, firewalls are one of the most mis-configured security controls in large organizations. For example, Forrester reports about 80 percent of firewalls examined by auditors during breach investigations for the Payment Card Industry Data Security Standard are mis-configured.² The culprit is a maze of complexity in manually creating and managing firewall policies and rules. Enterprises typically process dozens to hundreds of firewall rule-change requests each week – on average, 500 to 5,000 changes annually. Large organizations with hundreds or thousands of firewalls may process 10,000 or more rule changes each year. For perspective, manually changing just one rule can require four to five hours for completion by a team of technicians. Automation of firewall rule changes is necessary for practical management of a Registered Entity's network security. Likewise, a manual audit of those changes is impractical, so automation is also vital for producing data to verify CIP compliance.

Automation of firewall auditing provides three benefits, according to Forrester. First is finding unused rules to remove orphans and delete potential attack vectors. Automation also optimizes the rulebase, which improves firewall performance. Finally, automation produces audit reports to document what the solution found and changed during a firewall audit.

As a result of using a firewall audit solution such as AlgoSec's, a Registered Entity can give the automatically produced, pre-formatted Firewall Analyzer NERC CIP Compliance Report to the CIP auditors. The auditors, in turn, can attach the data to their audit worksheets. Auditors may also use the Registered Entity's AlgoSec solution to automatically drill down to deeper layers of data should they wish to verify details for a particular control.

² John Kindervag, *Market Overview: Firewall Auditing Tools* (Forrester: July 30, 2009).



Steps to the Process of CIP Compliance

The process of CIP compliance is circular and ongoing, particularly as Critical Cyber Assets are added or modified in a Registered Entity's bulk electric system. Steps include:

Identify. Registered Entities identify control requirements for each CIP standard and stipulate corresponding control policies.

Deploy. Registered Entities deploy the controls.

Document. Registered Entities document compliance via self-audit and self-assessment with the [NERC Compliance Questionnaire and Reliability Standard Audit Worksheet](#). There are eight versions, one for each CIP standard. Semi-annual self-certification is required.

Review. Compliance documentation is reviewed by each Registered Entity's Compliance Enforcement Authority. Spot checks may be conducted by Regional Entities, and violations are subject to investigation by Regional Entities. NERC and Regional Entities will collaborate on enforcement and mitigation processes. Substantial financial penalties may apply to non-compliance with CIP.

Pass. All Registered Entities must be capable of "auditable compliance" with all CIP requirements by June 30, 2010.

AlgoSec Automates Key Requirements for CIP Firewall Audits

CIP compliance entails proving that a Registered Entity's security controls are implemented and configured in accordance with the eight standards. The **AlgoSec Firewall Analyzer NERC CIP Compliance Report** fulfills these requirements for firewalls and related security devices.

AlgoSec's report addresses two major areas: controlling changes to firewall rules, and controlling risk affected by firewall rules. The solution automatically aggregates data from all the firewalls and other security devices deployed by a Registered Entity. The resulting "group report" from AlgoSec simplifies CIP documentation and saves a tremendous amount of time for auditors compared to manually cross-checking multiple reports and data elements.

The AlgoSec CIP report presents compliance data in summary form. It also allows drilling down to data for individual devices, ports and rules, which enables accurate, rapid remediation for non-compliant findings. On-demand access to deeper-layer data is also useful for answering pointed questions from auditors about a particular firewall rule and its effect on protecting Critical Cyber Assets.

Specific CIP firewall requirements met by the AlgoSec solution

Firewall auditing by AlgoSec addresses requirements in five of the eight CIP standards. Specific requirements for firewalls are:



CIP-002-2 R3 – Identifies and documents Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

CIP-003-2 R1, R4, R5 and R6 – Documents minimum security management controls that are in place to protect Critical Cyber Assets, including Cyber Security Policy, Information Protection, Access Control, and Change Control and Configuration Management.

CIP-004-2 R4 – Documents people with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific and physical access rights to Critical Cyber Assets.

CIP-005-2 R1 – R5 – Identifies and documents protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, and all access points on the perimeter. Subpart compliance includes Electronic Security Perimeter, Electronic Access Controls, Monitoring Electronic Access, Cyber Vulnerability Assessment, and Documentation Review and Maintenance.

CIP-007-2 R2, R5, R6, R8 and R9 – Documents methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, and other non-critical Cyber Assets within the Electronic Security Perimeter(s). Subpart compliance includes Ports and Services, Account Management, Security Status Monitoring, Cyber Vulnerability Assessment, and Documentation Review and Maintenance.

Example of AlgoSec compliance report for CIP-007-2 R2 (ports and services)

Standard CIP-007-2 requires Responsible Entities “to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).” Section R2 of this requirement is securing ports and services. Key provisions in the Standard state:

R2. Ports and Services – The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled.



Figure 1 below shows how the AlgoSec compliance report fulfills requirements of CIP-007-2-R2. Note how the left column mirrors specific part and sub-part requirements of the Standard. The next column specifies the AlgoSec feature that fulfills respective CIP requirements. The “Setting” column indicates if the particular control is “on” or “off.” Details and status are indicated on the right side. The report automatically aggregates data for all firewalls and routers in the Registered Entity. Hotlinks allow for instant viewing of related information or control data for specific devices or ports.

CIP-007-2 Requirement	AlgoSec Firewall Analyzer Feature	Setting	Details	Status																				
R2 Ports and Services																								
R2.1 Enable only those ports and services required for normal and emergency operations R2.2 Disable other ports and services, including those used for testing purposes	Allowed services	On	Click here to view the list of open services between Outside, Inside, and DMZs.	*																				
R5 Account Management																								
R5.1 Ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed	VPN Analysis	On	<table border="1"> <tr> <td></td> <td>flower_pix</td> <td>-</td> <td>-</td> </tr> <tr> <td></td> <td>orchid_router</td> <td>-</td> <td>-</td> </tr> <tr> <td></td> <td>poppy_juniper</td> <td>-</td> <td>-</td> </tr> <tr> <td></td> <td>rose_checkpoint</td> <td>359 users</td> <td>25 expired</td> </tr> <tr> <td></td> <td>tulip_fortigate</td> <td>-</td> <td>-</td> </tr> </table>		flower_pix	-	-		orchid_router	-	-		poppy_juniper	-	-		rose_checkpoint	359 users	25 expired		tulip_fortigate	-	-	*
	flower_pix	-	-																					
	orchid_router	-	-																					
	poppy_juniper	-	-																					
	rose_checkpoint	359 users	25 expired																					
	tulip_fortigate	-	-																					
R5.3 Require and use passwords, subject to the following: R5.3.1 minimum of six characters; R5.3.2 combination of alpha, numeric, and "special" characters; R5.3.3 Each password shall be changed at least annually.	Default Passwords	On	See the Default Password Risks results below for details	*																				
R6 Security Status Monitoring																								
R6.1 Implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events R6.3 Maintain logs of system events related	Change History	On	The AlgoSec report incorporates and annotates the Check Point audit log within its Change History page. For other firewall vendors the AlgoSec Change History page provides an independent audit trail for activities on the firewall.	*																				

Figure 1: AlgoSec reports automatically aggregate CIP compliance data for all firewalls and routers in the Registered Entity

Example of AlgoSec compliance report for CIP-005-2 R4 (electronic security perimeter)

Standard CIP-005-2 requires Responsible Entities to perform “identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.”

R4. Cyber Vulnerability Assessment – The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process.

R4.2. A review to verify that only ports and services required for operations at these access points are enabled.

R4.3. The discovery of all access points to the Electronic Security Perimeter.



R4.4. A review of controls for default accounts, passwords, and network management community strings.

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

Figure 2 below shows how the AlgoSec compliance report fulfills requirements of CIP-005-2-R4.

R4 Cyber Vulnerability Assessment				
R4.1 Identify the vulnerability assessment process	Risk Analysis	On	The AlgoSec Firewall Analyzer provides an automatic independent review of the security policy of the firewalls. This compliance report can be provided to the organization's security auditors as part of the periodic vulnerability assessment process.	✓
R4.2 Verify that only ports and services required for operations at these access points are enabled	Risk Analysis	On	<p>See the Offline Security Scan results below for details</p>	≈
R4.4 Review controls for default accounts, passwords, and network management community strings	Default Passwords	On	See the Default Password Risks results below for details	≈
R4.5 Document the results of the assessment	Compliance Report	On	The AlgoSec Firewall Analyzer automatically documents the results of the assessment of the firewalls' and routers' security policy.	✓

Figure 2: AlgoSec reports automatically aggregate CIP compliance data for a Cyber Vulnerability Assessment

Example of AlgoSec compliance report for CIP-003-2 R1.1 (assess risks)

Standard CIP-003-2 requires Responsible Entities to have minimum security management controls in place to protect Critical Cyber Assets. Section R1 of this requirement is about the Registered Entity's ability to prove its security policy is working. The Standard states:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

Figure 3 below shows how the AlgoSec compliance report fulfills requirements of CIP-003-2 R1.1. This particular capability of the AlgoSec firewall audit solution automatically performs an Offline Security Scan of the Registered Entity's firewalls and routers. The scan verifies if the organization's controls are working by simulating the effects of 183 risks that could be exploited through mis-configured firewalls and routers. The report displays each risk simulation and associated status within the Registered Entity's



network infrastructure. Since scans are off line, there is no risk of disruption to operations of Critical Cyber Infrastructure.

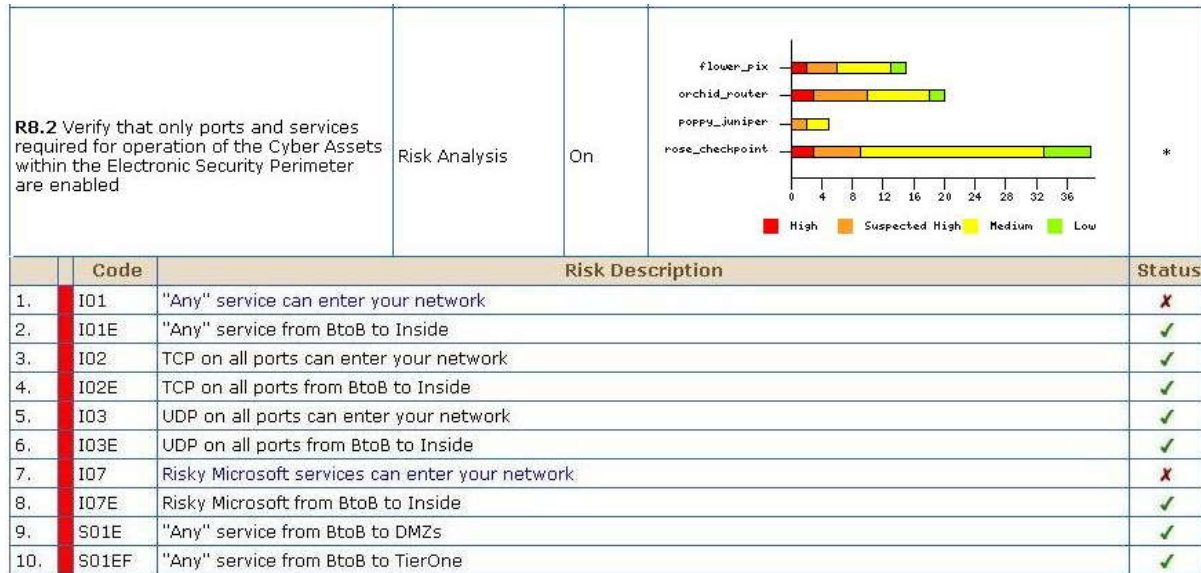


Figure 3: AlgoSec automatically scans all firewalls and routers in the Registered Entity and simulates 183 risks

Other CIP report examples

The AlgoSec firewall audit solution also provides documentation for other CIP compliance reporting requirements. For example, CIP requires changing vendor-supplied default passwords before installing a system on the network (CIP-005-2 R4.4, CIP-007-2 R5.3, and CIP-007-2 R8.3). AlgoSec checks to verify fulfillment of this requirement.

	Code	Risk Description	Status
1.	P22	Local password not set	✓
2.	P23	Enable password not set	✓
3.	P26	Password set to factory default value	✓
4.	P27	Password set to factory default value	✗
5.	P28	Password set to factory default value	✓
6.	P29	Enable password set to factory default value	✓
7.	P30	Enable password set to factory default value	✓
8.	P31	SNMP community string set to factory default value	✓
9.	P32	SNMP community string set to factory default value	✓
10.	P33	SNMP community string set to factory default value	✓

Figure 3: AlgoSec helps you verify that vendor-supplied passwords have been changed.

CIP audits also require production of a network topology or connectivity diagram (CIP-003-2 R4.1). AlgoSec fulfills this requirement by automatically producing network topology diagrams based on routing tables in a Registered Entity's network environment. The automation saves considerable time versus creating one from scratch with Microsoft Visio or other manual diagramming tool. Network diagrams created by AlgoSec are based on your actual network routing tables so they are accurate and up-to-date.



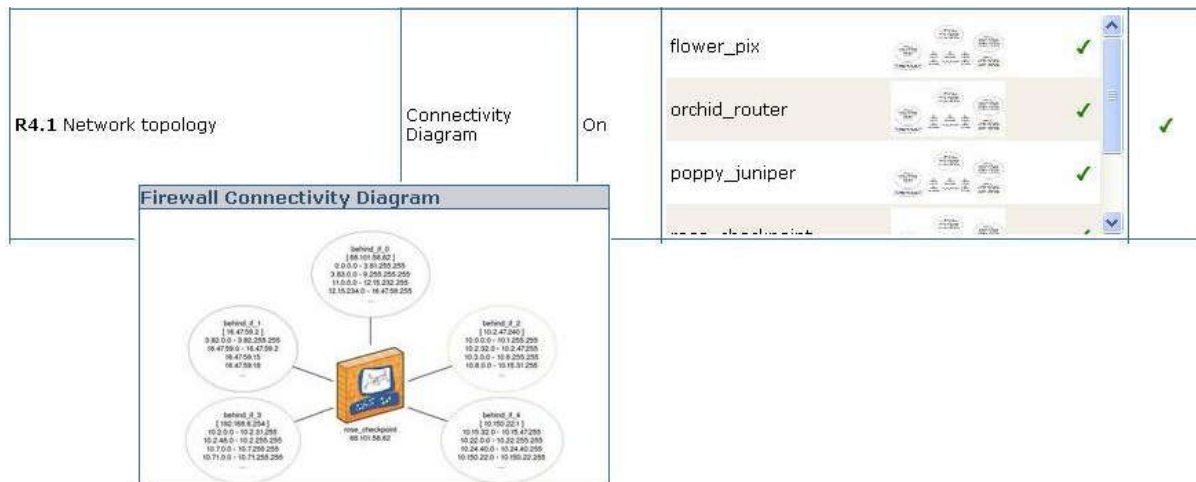


Figure 5: AlgoSec automatically provides a Network Topology Diagram based on actual routing tables in the Registered Entity

AlgoSec Lowers Costs of CIP Compliance and Improves Security

Registered Entities must perform many tasks related to risk mitigation and compliance – not just for CIP, but also for other laws and regulations. Preparing for a CIP audit alone can be both time consuming and costly. On average, organizations devote about five hours per device to prepare data for a CIP audit, which is an event that usually happens every quarter.³ On an annual basis, the total cost of preparing for CIP audits can be \$3,000 per device when factoring the additional annual cost of \$1,000 per device for a vulnerability assessment. Table 1 on the next page shows cost-saving opportunities for CIP audit preparation with an automated solution such as from AlgoSec.

Devices	Work Hours	Quarterly Direct Cost	Annual Direct Cost	Annual VA Cost	Annual Budget	with AlgoSec	Cost Savings
25	125	\$12,500	\$50,000	\$25,000	\$75,000	\$20,000	\$55,000
100	500	\$50,000	\$200,000	\$100,000	\$300,000	\$80,000	\$220,000
200	1000	\$100,000	\$400,000	\$200,000	\$600,000	\$160,000	\$440,000

Table 1: Cost-saving opportunities when automating CIP audit preparation with AlgoSec*

*Assumptions:

- 5 hours per device to compile CIP compliance data* \$100 per hour
- Annual cost of a Vulnerability Assessment for one firewall = \$1,000
- \$100 hourly rate for FTE work costs

Based on customer experiences, AlgoSec believes that automating audit preparation via the AlgoSec Firewall Analyzer can reduce the costs associated with audit preparation by up to 60 percent. Using estimates in Table 1, this could result in annual savings of \$220K for Registered Entities with 100 devices. Additional savings are likely for Registered Entities that require firewall audit documentation for other regulations. The AlgoSec solution also automatically presents firewall audit data for reporting

³ Based on AlgoSec customer data reported in 2010.



requirements of the Payment Card Industry Data Security Standard, Sarbanes-Oxley, ISO 27001, and Basel 2.

Conclusion

Automating firewall audits with AlgoSec technology is a common-sense solution for compliance with the Critical Infrastructure Protection Reliability Standards of NERC. With automation, Registered Entities can quickly and cost-effectively surmount the operational hurdles of manually implementing and managing firewall rule changes. Automation of firewall audits provides instant, real-time snapshots of CIP compliance for all firewalls operated by a Registered Entity. Verification of compliance ensures that a Registered Entity's vital firewall controls for CIP are providing maximum cyber protection for the bulk electric system.

About AlgoSec

AlgoSec is the leading provider of Network Security Lifecycle Management and Firewall Operations and Security Risk Management solutions. AlgoSec's exclusive technology is optimized for critical services providers, enterprises, managed service providers, auditors and consultants to quantifiably increase their operational effectiveness. Its products intelligently automate the traditionally manual tasks surrounding firewall, router and VPN management. This translates to significant cost savings and greater output for organizations without increasing headcount. AlgoSec also allows IT organizations to get more from their current infrastructures by extending the lifespan of existing security devices.

AlgoSec solutions are compatible with multiple firewall vendors including Check Point, Cisco and Juniper in standalone and integrated environments and ensure an organization is compliant and that its security policy matches configuration. More than 20 percent of AlgoSec customers are Fortune 500 organizations, as well as scores of leading enterprises across industry verticals. The company's management team is led by security experts, including founders [Yuval Baron](#) and [Avishai Wool](#), with extensive backgrounds in network security and research and development. AlgoSec has partners in the Americas, EMEA and Asia-Pacific.

For More Information

For more information about AlgoSec products and services, please contact AlgoSec sales at:

North America: northamerica.sales@algosec.com or 1-888-358-3696 (toll free)

EMEA: emea.sales@algosec.com or +44-2070997545

APAC: apac.sales@algosec.com or +972-3-922-1490

Latin America: latam.sales@algosec.com or +972-3-922-1490

You can also find more information on our web site: www.algosec.com

