SECURITY ANALYSIS & ORCHESTRATION

FIRESEC

Firesec™

Optimize your security architecture while ensuring compliance to PCI DSS, CIS benchmarks, ISO 27001 & other regulatory standards.

NETWORK INTELLIGENCE
Global cybersecurity provider

www.firesec.io info@firesec.io

PRODUCT BRIEF

MOST ORGANIZATIONS FIND IT VERY CHALLENGING TO ANALYZE AND OPTIMIZE THEIR SECURITY ARCHITECTURE THANKS TO A MULTITUDE OF SECURITY TECHNOLOGIES (FIREWALLS INTRUSION PREVENTION SYSTEMS, WEB PROXIES, ETC.), COMPLEX ACCESS CONTROL RULES & MULTIPLE NETWORK SEGMENTS. STANDARDS SUCH AS PCI DSS REQUIRE ORGANIZATIONS TO IMPLEMENT ACCESS CONTROL RULES IN A VERY SPECIFIC WAY AND TO ALSO AUDIT THE RULESETS EVERY SIX MONTHS.

FIRESEC™ AUTOMATES THE TASK OF ANALYZING SECURITY DEVICE CONFIGURATIONS, HIGHLIGHTING NON-COMPLIANCES AND INSECURE RULES, AS WELL AS HELPING YOU OPTIMIZE THE CONFIGURATIONS TO IMPROVE DEVICE PERFORMANCE. THE NETWORK VISUALIZATION FEATURES HELP YOU SEE AND EXPLORE THE ENTIRE NETWORK TOPOGRAPHY AND DETERMINE INSECURE ACCESS PATHS AND FIX THESE PROBLEMS.

SECURITY ANALYSIS AND ORCHESTRATION PLATFORM

FIRESEC™ AUTOMATES THE ANALYSIS & OPTIMIZATION OF YOUR SECURITY TECHNOLOGIES TO REDUCE COST, IMPROVE PERFORMANCE & ACHIEVE COMPLIANCE.

CHIEF INFORMATION SECURITY OFFICER

PROBLEM AREAS

Lack of visibility on the entire network

Surprise findings during audits

Tedious process to get periodic configuration reviews done

Absence of a real-time view of the network security posture

FIRESEC AS A SOLUTION

A CISO dashboard that informs you of what the network security level is.

Compliance status available at the click of a button.

Ability to approve configuration changes by viewing security and compliance impact before the change is made.

Firesec enables access control rules to be reviewed via an automated workflow that reduces the time taken from days to hours to complete complex configuration reviews.

Custom reports that give effective insights as well as provide details to make informed decisions.

SECURITY CONSULTANT

PROBLEM AREAS

Multiple tools and scripts needed to audit different client environments

Configuration reviews take significant amounts of time

Writing up reports

FIRESEC AS A SOLUTION

A single tool that supports a wide variety of security technologies and comes with in-built policies that can be selected to audit against.

Firesec reduces the time taken to do a comprehensive configuration review to a matter of minutes.

Firesec provides complete customization of the reports and allows security consultants to brand reports with their logo and brand.

Customize report contents and layouts

NETWORK ADMINISTRATOR

PROBLEM AREAS

Inability to determine the security and compliance level of a new change.

Tedious troubleshooting to determine access control problems

Clutter of rules and objects makes device operations very difficult and complex.

FIRESEC AS A SOLUTION

Impact analysis of each change can be done using the 'what-if' scenario to ensure all new changes are in line with organizational policies and regulatory requirements.

Single-click navigation via the Network Topology feature allows the network security administrator to determine which system can or cannot access which destination system or network segment.

Firesec helps optimize configurations by identifying unused, redundant and shadowed configuration elements.

SECURITY AUDITOR

PROBLEM AREAS

Ensuring and evaluating the efficacy of the security policies.

Generating reports for network device rule base and configuration analysis.

Limited clarity and interpretation of your network and security policy.

Ensuring the compliance with internal as well as regulatory standards.

FIRESEC AS A SOLUTION

Bird's eye views as well as ability to drill down and explore the entire network architecture.

Support for a wide variety of security technologies & pre-loaded audit policies cover PCI DSS, CI Security Benchmarks, Vendor Guidelines, etc.

With Firesec there is no need to sample the audit, the product provides a comprehensive real-time compliance status.

HOW DOES IT WORK ?

FIRESEC SUPPORTS A WIDE VARIETY OF SECURITY TECHNOLOGIES SUCH AS FIREWALLS, ROUTERS, SWITCHES, PROXIES, ETC. FROM VENDORS SUCH AS CHECKPOINT, CISCO, SOPHOS, FORTINET, JUNIPER, PALO ALTO, BLUECOAT, WEBSENSE AND OTHERS.

CONNECT

Connect your security technologies with Firesec.

SELECT

Choose your compliance policies.

ANALYZE

Run the configurations against these policies.

REVIEW

Review the results and determine actions.

OPTIMIZE

Implement changes via the orchestration

MONITOR

Review configuration changes & critical events in real-time.

SUPPORTED FIREWALLS		
	Manual Mode (Filetype)	Automatic Mode
CheckPoint (GAIA)	R77.30, R80.10 (.zip)	R80.10
Cisco ASA	v8, v9 (.txt | .config)	v8, v9
Sophos-Cyberoam	> v10.6.3 (.xml)	Not Applicable
Fortigate (FortiOS)	v4, v5 (.config)	v4, v5
Juniper (JunOS)	v12, v14 (.config)	Rx
Palo Alto (PanOS)	v6, v7, v8 (.xml)	Rx

SUPPORTED ROUTER & SWITCHES		
	Manual Mode (Filetype)	Automatic Mode
Cisco IOS	v12.x - v15.x (.txt | .config)	v12.x - v15.x

FLEXIBLE DEPLOYMENT OPTIONS

Choose whether you would like to Self-host solution or use it as a Managed-Hosted solution (SaaS).

On-Premises Cloud (SaaS)

SYSTEM REQUIREMENTS AND SIZING*

SERVER	: Microsoft Windows 2012 or 2016	STORAGE	: 250 GB
CORES	: 2	WEB SERVER	: IIS – latest version
MEMORY	: 16 GB	DATABASE SERVER	: SQL Server – latest version

*Solution sizing may differ based on the total number of security technologies to be managed.

NETWORK INTELLIGENCE
Global cybersecurity provider

OFFICES : Mumbai | New York | Singapore | Dubai | Delhi | Bengaluru | Pune

info@firesec.io | sales@firesec.io

www.firesec.io

https://support.firesec.io/portal/home

https://www.firesec.io/contact.html