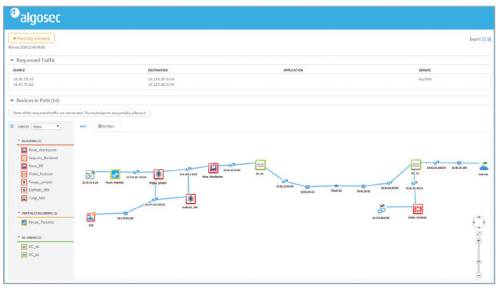

AlgoSec

Security Management Solution

This is one of the more interesting products that we saw this month. Its premise is that it can manage security – and, thus, risk and policies – by managing the data flows within the enterprise. It uses the enterprise's firewalls as a key point of reference to do this. There are three modules in the Security Management Suite: Firewall Analyzer, FireFlow and BusinessFlow. Firewall Analyzer is the glue that holds everything together and BusinessFlow is the application side of things. It defines the construct of a business application and tells FireFlow how to configure to support the application.

We dropped into the BusinessFlow dashboard. This is the starting point for setting up the system. Each application has detailed information entered here including technical, business and responsibility entries. The technical details include such things as how the application connects with other applications and what the flow paths need to be to achieve the application's mission. The paths are layer 3. The result, when all of the applications are entered into the system, is a connectivity map. When the connectivity between an application and one of its endpoints breaks, an alert tells the analyst that there is a problem.

Vulnerability scans generate remediation workflows and, in some cases, can provide automated firewall configuration change orders. Policies are based on all of the current standards such as PCI, HIPAA, etc. The dashboards have excellent drill-down and, in many cases, present their information in formats comfortable for business managers rather than technical personnel.

We really liked the reporting capability of this tool. Reports can be generated on the fly. We have seen numerous situations where a report is needed immediately, whether to answer a management question or to support an audit. One thing that we found unique is that the applications that talk to each other can be tagged. To understand the communications involved, searches on the tags reveal information quickly.

Additionally, the tool can decommission an application without breaking the other applications with which it communicates. So dependencies are handled neatly and seamlessly. The reverse of that also is true. New deployments can be staged without breaking applications or flows that may be involved. The system has a nice closed loop remediation feature that is implemented through an API that can connect the tool to ticketing systems.

Firewall Analyzer supports auto discovery and traffic simulation. So, when a change order is entered, it theoretically reconfigures the firewall involved, simulates traffic and determines the consequences of the change. Using its policy engine, the product can examine devices and see the risk, including risky rules nd perform rule cleanup.

The website has a good support portal that includes a knowledge base, the documentation is straightforward and no-cost, eight-hours-a-day/five-days-a-week support is included with basic, while preferred and premium support are available at fees ranging from 20 to 40 percent.

DETAILS

Vendor AlgoSec

Price Starting at $10,000.

Contact algosec.com/products

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Very strong security management tool with strong emphasis on layer 3 connection between applications. Pricing is attractive and support is good.

Weaknesses None that we found

Verdict This is an excellent tool, especially for mid- to large-sized organizations. It has everything you need and is comfortably manageable. We compare it to a sailboat – even though it's fairly large and complex, can be sailed effectively by a single person.

algosec
65 Challenger Road, Suite 320
Ridgefield Park, NJ 07660
+1-888-358-3696
info@algosec.com • www.algosec.com