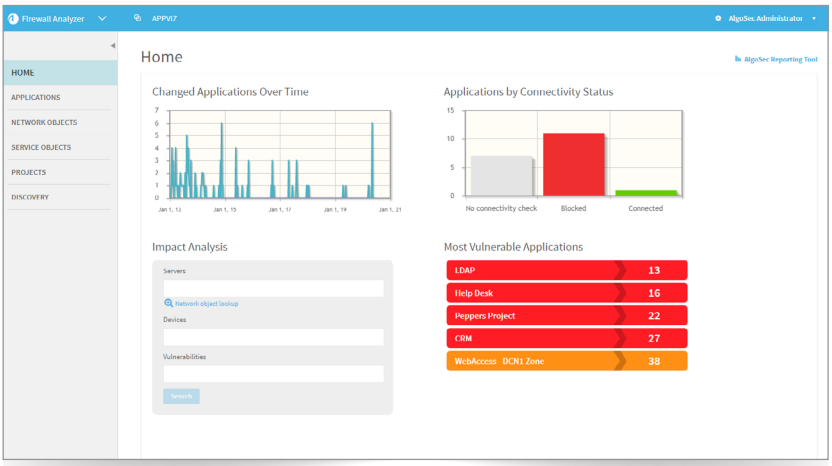
Assess and prioritize vulnerabilities from the business perspective

Vulnerability management has always been a cornerstone of a sound information security program, but traditional scanners uncover too many vulnerabilities for any business to adequately address. Additionally, vulnerability information is typically presented for IP addresses and servers, and not in a context that business owners can understand.

Given the number of vulnerabilities across the network, effectively prioritizing risk and remediation efforts based on the business application and existing firewall risks has a major impact on security and business productivity.

Application-centric vulnerability management

AlgoSec AppViz integrates with leading vulnerability scanners to map vulnerabilities with their associated data center applications, including their servers and complex connectivity requirements. Organizations can view network vulnerabilities with the business in mind. As application components, connectivity requirements, and vulnerabilities frequently change, AlgoSec ensures organizations have the most up-to-date and accurate information to prioritize risk.

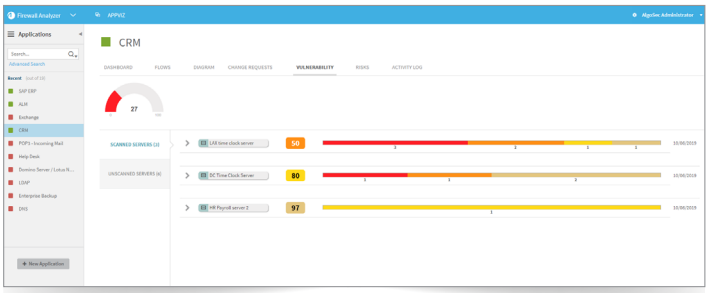


KEY BENEFITS

- Map vulnerabilities and severity levels to business applications
- Ensure the most effective prioritization of vulnerabilities with application context
- Improve accountability by enabling business owners to "own the risk"
- Reduce risk of faulty firewall rules by associating the related vulnerabilities

Enable the business to "own the risk"

Vulnerability information can be aggregated to provide an application-centric view, displaying all risks associated with a line of business. Security teams can then effectively communicate with business and application owners, giving them visibility so they can be accountable and "own the risk."



Seamless integration with network vulnerability scanners

AlgoSec seamlessly integrates with QualysGuard, Tenable Nessus Professional, and Rapid7 Nexpose vulnerability scanners to automatically pull in the vulnerability information including CVSS scores, details, and remedy recommendations.

Security rating per application

Get a holistic view of business risk. Vulnerabilities and their severity are scored across each application server as well as aggregated per application.

Continuously updated vulnerability scores

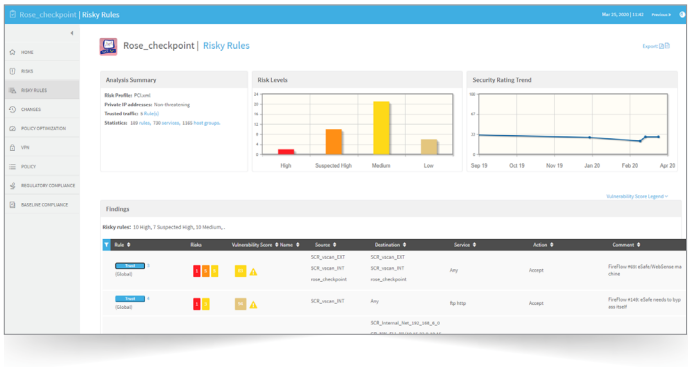
As application connectivity flows change, the vulnerability scores automatically update to ensure a continuous view of the application's risk.

Visibility of unscanned servers per application

AlgoSec also highlights all servers that have not been scanned for vulnerabilities within a specific time frame.

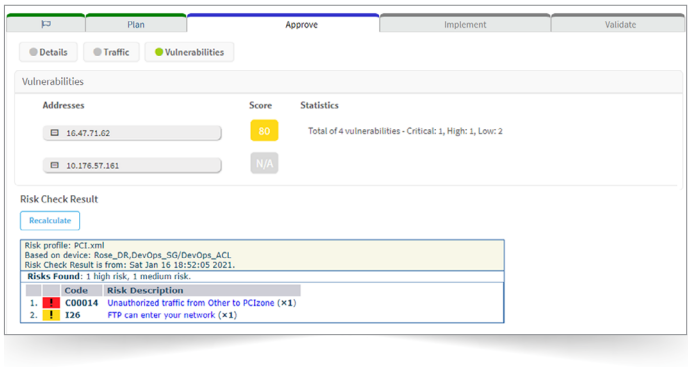
Tie vulnerability scanner data to risky rules

AlgoSec provides calculated vulnerability scanner data as part of the risky rules report. Now you can access vulnerability data, such as vulnerability scores and counts, at the level of each rule.



Identify vulnerabilities before making a change

Before implementing a security policy change, identify the potential vulnerabilities introduced by the change. Be confident these changes are not posing new risks on the network.



Comprehensive Support for Heterogeneous Environments

AlgoSec supports all the leading brands of traditional and next generation firewalls and cloud security controls, as well as routers, load balancers and web proxies across any heterogeneous and multi-vendor cloud, SDN or on-premise enterprise network environments. Additionally, AlgoSec seamlessly integrates with the leading IT service management, SIEM, identity management, orchestration systems and vulnerability scanners to deliver unified security policy management. To find out more about AlgoSec's ecosystem of technology partners, click here.

algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

AlgoSec.com