

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. Moreover, vulnerability information is typically presented for IP addresses and servers, and not in the context that business owners can understand.

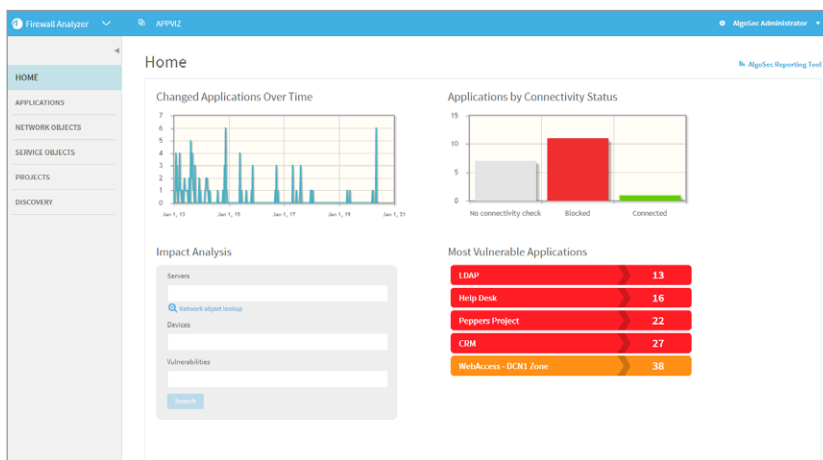
Given the number of vulnerabilities across the network, having an effective way to prioritize risk and remediation efforts based on the business application and existing firewall risks will have a major impact on both security and business productivity.

Application-Centric Vulnerability Management

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

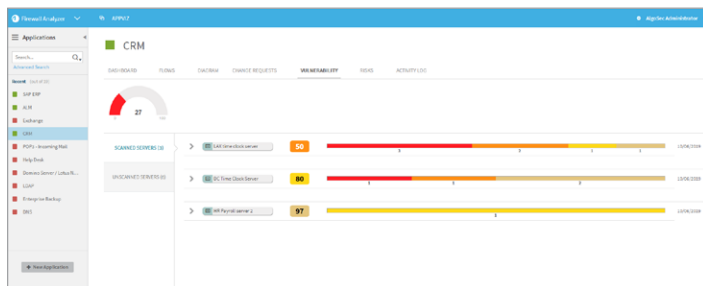
KEY BENEFITS

- 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”

With AlgoSec, vulnerability information can be aggregated to provide an application-centric view, displaying all risks associated with a line of business. Security teams can now more effectively communicate with business and application owners, giving them the visibility that enables them to 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

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

Continuously Updated Vulnerability Scores

As application connectivity flows change, the vulnerability scores automatically update to ensure a continuously current view of the risk to the application.

Visibility of Un-Scanned Servers Per Application

AlgoSec also highlights all servers that have not been scanned for vulnerabilities within a specified interval.

Tie Vulnerability Scanner Data to Firewall Risky Rules

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



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](#).