Prioritizing 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.

With volumes of vulnerabilities throughout the network, having an effective way to prioritize risk remediation efforts can have a major impact on both security and business productivity. And given the choice, organizations prefer to view and prioritize risks by business application[1].

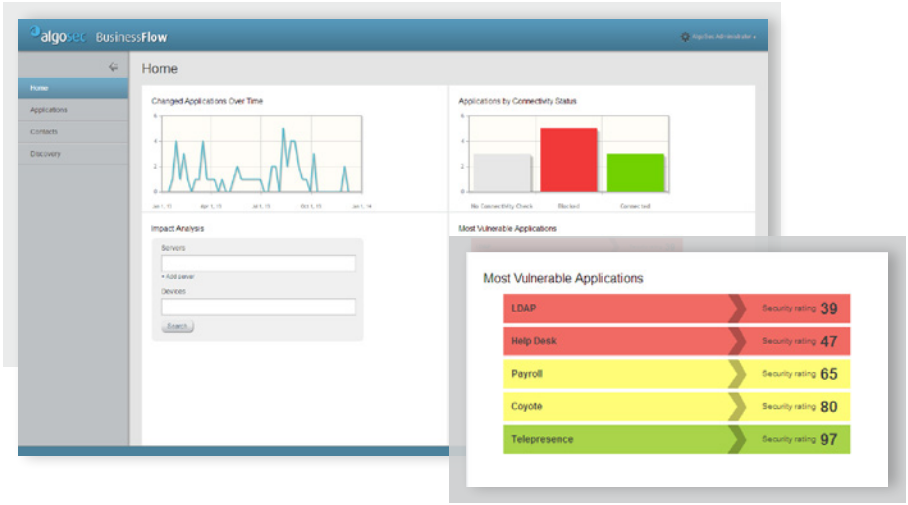
Application-Centric Vulnerability Management with BusinessFlow

AlgoSec BusinessFlow 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.

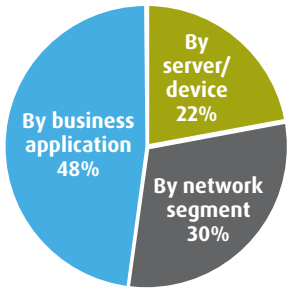
"Risk and the accountability for risk acceptance are - and should be - owned by the business units creating and managing those risks." - Paul Proctor, Analyst, Gartner Inc.

Highlights

- 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"



Ideal method for prioritizing network vulnerabilities



[1] Source: Examining the Impact of Security Management on the Business, October 2013

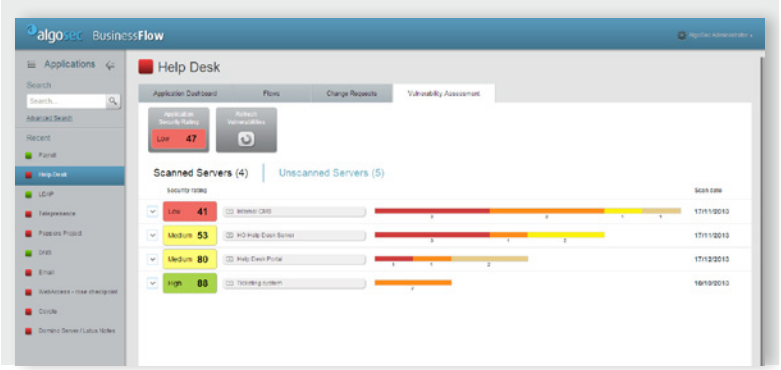
Enabling the Business to "Own the Risk"

With AlgoSec BusinessFlow, 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".

Key Capabilities include:

Security Rating Per Application

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

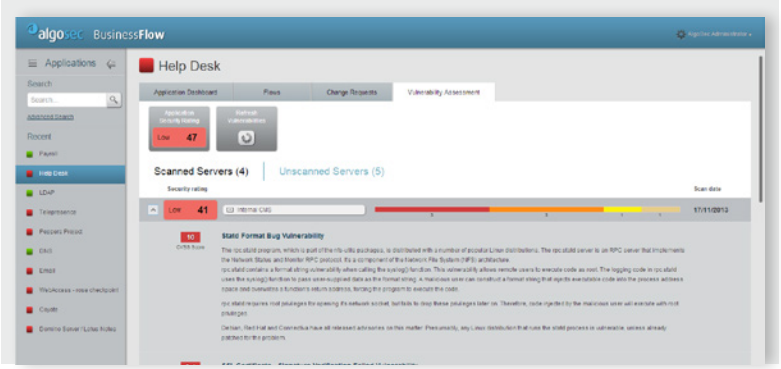


Continuously Updated Vulnerability Scores

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 provides application owners with an immediate view of any server that has not been scanned for vulnerabilities within a specified interval.



Seamless Integration with Network Vulnerability Scanners

AlgoSec integrates with Qualys and Nessus to automatically pull in the vulnerability information including CVSS scores, details and remedy recommendations.

Nessus® vulnerability scanner

QUALYS® CONTINUOUS SECURITY

AlgoSec.com

Follow Us On:

Headquarters
265 Franklin Street
Boston, MA 02110
USA
+1-888-358-3696

EMEA Headquarters
33 Throgmorton Street
London, EC2N 2BR
United Kingdom
+44 207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

algosec