Case Study:

zTRUST™ helped an international bank improve network security, reducing complexity and costs

Summary

Network discovery and segmentation using zTrust™ software enabled this international financial institution to meet PCI DSS compliance requirements in more efficient, cost-effective, & automated ways.

Client

With millions of customers, this organization has a wide-ranging mainframe estate and cross-border network infrastructure. Cyber security and data protection are priorities, with the international business subject to many requirements, including global standards focused on payment account data protection.

Challenge

This client operates several mainframe data centers worldwide that are interconnected with a flat corporate network; any network device can potentially connect to any system in any data center. Consequently, an upcoming PCI DSS audit in one country would have to include all interconnected systems worldwide. The independent auditor strongly recommended network segmentation to reduce the audit's scope, complexity and cost. While this was accepted, the client faced what seemed to be an impossible task due to the network's size and complexity, and the availability of knowledge and skills to identify what should be segmented and how.

zTRUST™ Solution

Vertali was consulted about implementing segmentation in an automated way that would require no detailed knowledge of the network or in-depth network skills. Following detailed discussions, a mainframe resident software solution was developed and deployed, first on development systems before migrating to production. There are three linked stages:

- *Network Discovery* – building and maintaining a knowledge base of all connections to and from each mainframe application. Then a client can fully understand the current connectivity to each application to form the basis of segmentation rules.
- *Defining Segmentation Rules* – new System Authorization Facility (SAF) resources were used to define the segments permitted to access mainframe applications, initially RACF, subject to PCI compliance.
- *Implementing Segmentation* – the security team controls segmentation using standard commands, bringing the responsibility for network segmentation into the same team as other compliance tasks. To minimize workload, the solution was developed to automatically generate SAF resources and permissions.

A critical component is the IP Filtering capability of the IBM z/OS Communications Server, managed by the IBM Policy Agent. IP filtering definitions are complex, with potentially severe consequences if defined incorrectly. To solve this, the Vertali solution automatically generates definitions directly from access controls defined in SAF. Management tools were also added for the controlled implementation and rollback of new rules.

The zTrust solution is rolling out worldwide prior to audits in each country.

Findings by implementation team:

"In addition to audit savings, the Network Discovery component is providing valuable insights into the network activity of z/OS applications, highlighting inbound and outbound connection activity, and their encryption status."

"Therefore unknown connections were discovered, together with connections still transmitting sensitive data in clear text – highlighting an urgent need to investigate and implement encryption."

Powered by VERTALI

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS WOMEN OWNED

For more information on Vanguard's services, call (702) 794-0014 or visit www.Go2Vanguard.com

6625 S. Eastern Ave., Las Vegas, NV 89119
(702) 794-0014 Business.Development@go2vanguard.com www.Go2Vanguard.com