Client Showcase

App Segmentation

Segmenting Legacy Systems and Improving Visibility

PROJECT FRAMEWORK

INITIATE

- Assessment, gap analysis and define end state.
- Solution review and planning
- Define scope, objectives, success criteria, risk, and approach
- Communication and escalation plan

PLAN

- Introduce key participants, stakeholders and project teams
- Review and approve project plan
- Task and resource scheduling and assignment
- Kickoff and regular status meetings

EXECUTE

- Discovery
- Design & implementation
- Migration & validation

MONITOR

- Ensure adherence to scope, schedule, and budget
- Follow client's change management process

CLOSE

- Formal turnover
- Project deliverables
- Lessons learned, client satisfaction feedback, and survey

BACKGROUND

A global organization was facing a critical vulnerability risk involving legacy systems across multiple data centers. The internal IT team had engaged a large VAR to resolve the issue through a single-technology solution, but after 18 months, the project had not succeeded and had caused multiple outages. KNZ was brought in to assess the environment, identify gaps in the previous approach, and determine a more effective path forward. After reviewing the client's requirements, KNZ concluded that the desired outcome required a holistic, multi-technology segmentation strategy.

OUTCOME

KNZ designed and implemented a software-defined networking solution that successfully segmented legacy operating systems across the client's data centers. The solution improved visibility, enabled policy enforcement, supported malware and file detection, and allowed access rules to be tightened over time. As a result, the client corrected the security vulnerability, reduced operational risk, and gained a stable platform for managing segmentation and security policies going forward.

SOLUTION

Applying KNZ's holistic approach, we developed a solution that consisted of 5 technologies, and required modifications to the existing environment. KNZ created a software defined networking (SDN) design to segment legacy operating systems in multiple datacenters, and provided customized formal training. The segmentation project included:

• Enable visibility and policy enforcement
• Intrusion policy set to typically drop appropriate traffic and allow an acceptable number of false positives
• Configure malware & file detection and blocking
• Overtime lock down of access rules to restrict communications

The technology solution consisted of:

- Cisco ACI with Service Graph
- Cisco FirePower
- Bricata
- VMware
- Gigamon