

Effective Risk Mitigation with ZIF's Vulnerability Management

for a Leading Communications Company

Customer Overview

The customer, an American Fortune 500 integrated communications company, offers marketing, business communications, and commercial printing services. With a large global presence and customer base, they empower organizations worldwide to execute effective multichannel communications strategies.

The Business Situation

The customer faced critical IT infrastructure vulnerabilities and was at heightened risk for security breaches and operational disruptions. Seeking a comprehensive solution, they partnered with ZIF to systematically identify, assess, and address vulnerabilities. ZIF's remarkable vulnerability management capabilities helped mitigate risks, and restored security, stability, and most importantly restored confidence.

The Solution

The implementation of AIOps platform ZIF helped address vulnerability gaps rapidly and eliminate threats. AI led intelligence automatically detects vulnerabilities and suggests ways to remediate, thereby accelerating resolution several fold. ZIF also simplifies ongoing security management and provides real time insights ensuring a healthy infrastructure. Key features and capabilities of the solution include:

- Automation bots to resolve issues identified by vulnerability assessment tools
- Integration with Nessus vulnerability assessment tools
- Triggering of automation processes across multiple servers with pre-established access privileges
- Categorization of vulnerabilities from assessment reports for proactive risk mitigation
- Development and execution of automated bots to address newly identified vulnerabilities
- Initiation of new scans to check for open risks
- Timely reports with key findings and insights

Challenges

- Outdated software and systems
- Lack of timely patching and updates
- Inadequate incident response and recovery plans
- Ineffective vulnerability scanning and management processes

Solution Highlights

- Integration with existing monitoring tools via APIs
- Remediation using bots
 - Mitigation applied within 24 hours of identification across all devices when remediation available in ZIF for the identified vulnerability
 - Mitigation bots developed and released for execution within 14 days from identification when new remediation needs to be developed for the identified vulnerability
- User-friendly reports for analysis

Solution Outcomes

- Automatic execution of resolutions
- Over 75% success rate every month on mitigations done
- Workflows and automation bots implemented to mitigate vulnerabilities identified in client servers in APAC region
- Healthy infrastructure by regular vulnerability scanning, identifying and prioritizing vulnerabilities for prompt remediation
- Drastically reduced incident response times and potential damages due to improved incident response workflows, automated actions and responses to security incidents
- Streamlined compliance processes through task automation