KEY RESOURCES
The Key to zSystems Integrity

CASE STUDY

# An Investment Firm Opens Its Eyes to Mainframe Security Vulnerabilities

## CHALLENGE

- Initially not aware that the mainframe operating system was vulnerable to security flaws, nor that their mainframe was inflicted with vulnerabilities.
- Original scope of PCI auditing did not include mainframe scanning.
- PCI audits conducted annually, with risk reports only analyzed by CIO.

## SOLUTIONS

- Key Resources z/Assure® VAP conducts yearly mainframe vulnerability scans, as part of the company's expanded PCI auditing process.
- The investment firm's executive audit committee reviews the results of the mainframe vulnerability assessments.

## BENEFITS

- More thorough and regularly-held PCI security audits that now include mainframe vulnerability scanning.
- Compliance with New York state cybersecurity regulations.

One of Key Resources' earliest relationships, dating back to 2009, is with an investment firm that got off to a surprising start. Our founder Ray Overby was part of a team asked to come in and poke around the firm's mainframe systems, just to see if they could find anything unusual or potentially problematic. Within 15 minutes of arriving, that's exactly what Ray found.

Suddenly, a room full of the firm's technology executives had their eyes opened to the realization that the mainframe is not as inherently secure as they believed.

## Found Within Minutes

Until then, the firm's executives were completely unaware of the threat that zero-day vulnerabilities on the mainframe can pose to the security and stability of a company's IT landscape.

In fact, their PCI audits didn't even include the mainframe as part of their internal reviews. Because PCI auditing requirements didn't explicitly state that the mainframe should be under malware and antivirus protection, the mainframe was never highlighted as a potential point of vulnerability, and was thereby excluded from these internal audits.

## A Strategic Need for Expanded Security Auditing

This experience prompted two revelations. For Key Resources, the discovery of potential zero-day vulnerabilities on the mainframe spurred the development of the z/Assure® VAP solution to perform scheduled, automated mainframe vulnerability scans. For the investment firm, the discovery of mainframe vulnerabilities prompted a total rethink of how they approach security risks on the mainframe.

“Key Resources provided us with a technically elegant tool that has been able to meet a strategic need for mainframe security,” said the company’s Director of Enterprise Security.

Prior to this, only the CIO would review the PCI audit results – results that were based on network scans that glossed over mainframe security.

Following this discovery, though, the investment firm’s executive audit committee – comprised of VPs from across the company’s departments – issued a new directive that stipulated an expansion of PCI auditing to include the mainframe.

> “Key Resources provided us with a technically elegant tool that has been able to meet a strategic need for mainframe security”
>
> DIRECTOR OF ENTERPRISE SECURITY

With this new requirement, the committee chose Key Resources’ z/Assure VAP solution to conduct regular mainframe vulnerability scans, in order to weed out potential malware and zero-day vulnerabilities on the mainframe.

## A Future-Proofed Mainframe

The investment firm’s executive audit committee now knows full well that the security threats on the mainframe are real.

With an expanded vulnerability management policy and Key Resources’ z/Assure VAP, the company now has regular, real-time mainframe security assessments.

Before, the company’s executives didn’t even know the mainframe was susceptible to security problems. Now, they know they not only exist, but have the tools necessary to find and fix any right away.

Additionally, the implementation of new mainframe vulnerability scanning brings the investment firm’s vulnerability management processes and policies in line with other requirements.

The state of New York issued new mandatory cybersecurity requirements for financial services companies, effective March 1, 2017. While these directives don’t explicitly address the mainframe, their definitions are fairly clear that a cybersecurity breach can occur on any information system and what, accordingly, needs to be included in a cybersecurity program.

With its improved mainframe security scanning, the investment firm is now future-proofed in complying with this particular regulation.

Key Resources Inc. has decades of expertise providing software, services and consulting to enterprises running critical apps on IBM® z/OS. We help CIOs, CISOs and programmers take control of mainframe security so they can protect their data, avoid costly breaches and maintain regulatory compliance.

**Contact Key Resources**

Call 1-800-574-1339 ext 701

Visit www.krisecurity.com/contact