KEY RESOURCES
The Key to zSystems Integrity

THE LEADER

In Mainframe Security

Our Team

Cynthia Overby
President

30+ years of diverse IT experience in network, infrastructure security, risk management, technical architecture, and policy development.

Lou Losee
Director
Services

30+ years of experience in development, consulting, and certifying hardware and software products to national and international government

Ray Overby
CTO

Founded KRI in 1988
30+ years of experience in IT security, providing consulting services to Fortune 500 institutions focusing on configuration-based compliance audits, comprehensive z/OS pen tests and code-based vulnerability assessments
Published in z/Journal, HealthIT, TechTarget, InfoSecurity, CIO Magazine, eWeek, and IBM Enterprise Magazine.

Accreditations

Certified WBENC Women's Business Enterprise

Certified SBA WOSB Woman Owned Small Business

GSA Contract Holder
Contract # 47QTCA21D00B2

Company Snapshot

Strategic Clients:

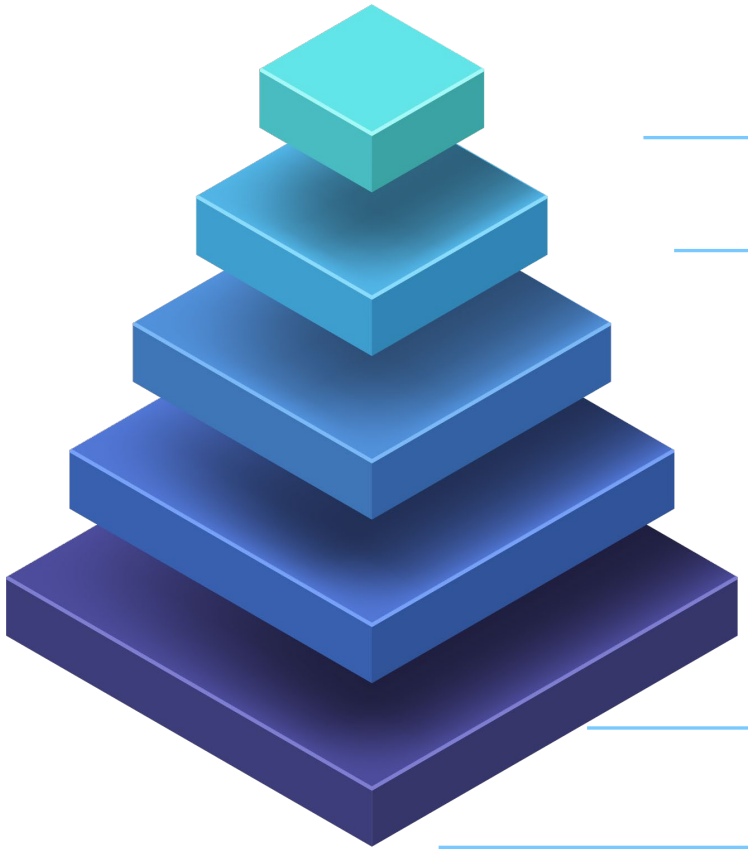
Strategic Partnerships:

- **2 products Modernizing Mainframe Security** - Code scanner and config scanner
- **100+** Enterprise customers in US, Canada, and Europe
- Services Launched in 1988
- VAP launched in 2011
- CAM for RACF launched in 2015

KEY RESOURCES
The Key to zSystems Integrity

Mainframe Vulnerability Mgmt.

75% of organizations do not include the operating system in their vulnerability and risk management programs; nor even consider it an asset. Most risk teams don't know you have to go through the operating system to get to the data!!!



- Data
- **Operating System** **Why the Gap?**
- Applications
- Internal Network
- Perimeter
- Physical
- Policies, Procedures, and Awareness

KEY RESOURCES
The Key to zSystems Integrity

Why the Gap?

Because – evidence of Mainframe Hacks are kept in-house - we call this the Conspiracy of Silence.

IBM Quote about Mainframe Security (2018)

"IBM does not make Security / Integrity data publicly available for IBM Z. This Security Portal provides a controlled notification and distribution mechanism to help ensure this critical information is available only to those IBM Z clients that have a need to know without publicly posting information that could put their systems in danger."

IBM statement in 2020 - has the tune changed?

"The boundary between an unauthorized caller and a PC or SVC routine running Supervisor State Key 0 is an essential part to the System Integrity of the z/OS solution stack."

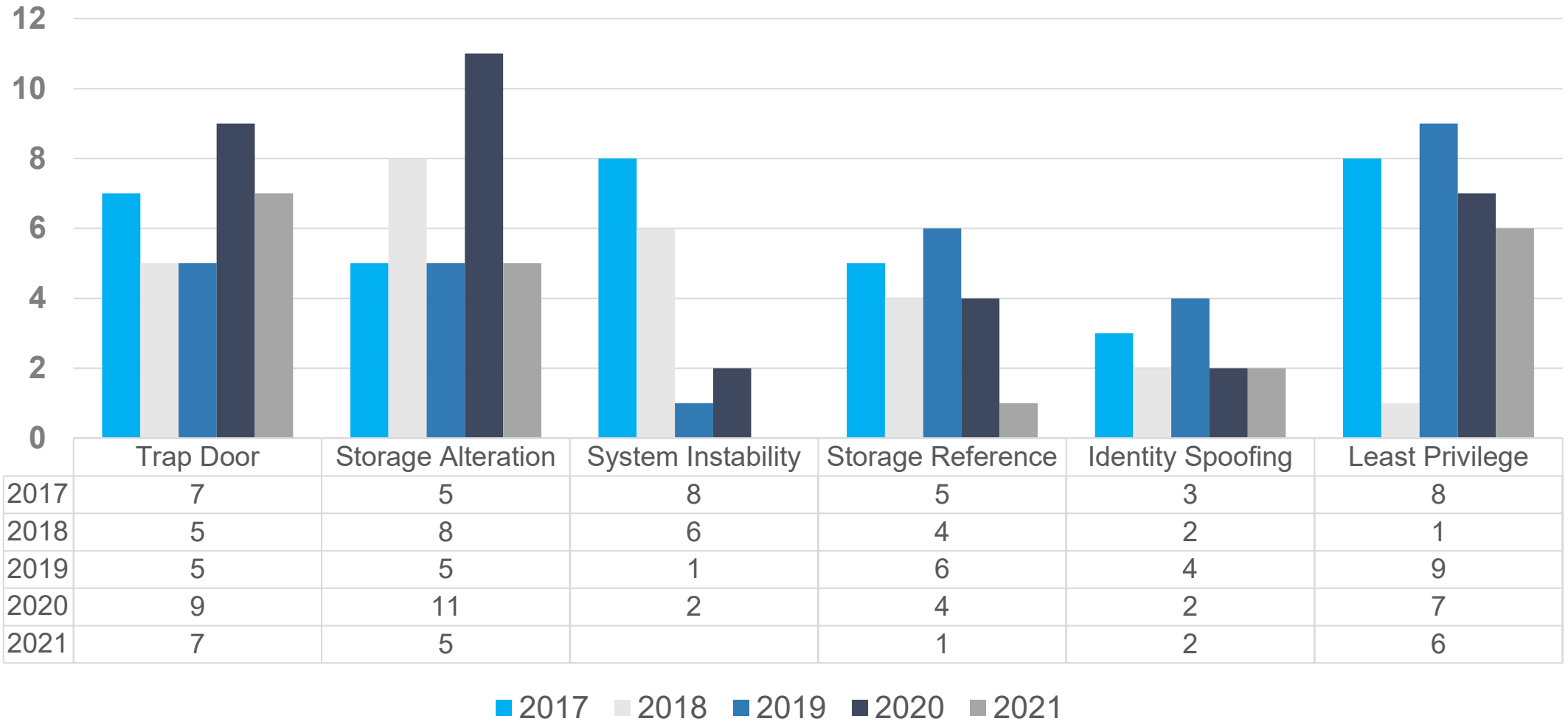
KEY RESOURCES
The Key to zSystems Integrity

Why is the Operating System Layer Vulnerable?

- **With respect to the z/OS Statement of Integrity, the attack surface is between user or non-authorized user programs and authorized system services:**
  - **Program Calls (PCs)**
  - **Supervisor Calls (SVCs)**
  - **Authorized Programs (APF)**
- **These three interfaces are the methods used for requesting authorized system programs to provide services to a user (application) program. If one of these authorized services breaks the rules a vulnerability can occur.**
- **If a User program bypasses the controls put in place by z/OS and the installation and the program can get authorized, it has broken through the attack vector and is able to circumvent the integrity of the system.**
- **The User program can modify any area of memory, i.e assume credentials of other users including administrators or system personnel.**

Why VAP?

z/OS Zero Day Vulnerabilities by Year



	Trap Door	Storage Alteration	System Instability	Storage Reference	Identity Spoofing	Least Privilege
2017	7	5	8	5	3	8
2018	5	8	6	4	2	1
2019	5	5	1	6	4	9
2020	9	11	2	4	2	7
2021	7	5		1	2	6

KEY RESOURCES
The Key to zSystems Integrity

Why VAP?

01 Onboarding

02 Discover

03 Report

04 Remediate

05 Verify

06 Repeat

CIO:

"Key Resources understands the mainframe inside and out, and the potential risks we need to address. They knew exactly what kind of problem we were dealing with and what we needed to do resolve that problem, with the level of specificity it required."

Case Study – Client using z/Assure VAP

Results - in the first 3 months of 2020, detected and stopped 33 possible attacks, potentially saving billions of dollars a day.

KEY RESOURCES
The Key to zSystems Integrity

Metrics / Benefits

Trap Door, Storage Alteration
System Instability, Storage Reference
Identity Spoofing, Security Probing
Least Privilege

Scans SVC's, PC's, APF Authorized Libraries,
User Key Common Storage

Data from detail reports provided in CSV format for porting to risk mgmt. systems,

z/Assure VAP is a real-time Binary code scanner

Establishes whether a vulnerability exists in each routine it scans.

Detailed Reporting: Pinpoints the exact location of the identified code vulnerability.

False positives negligible, fewer misallocated resources, high trust level

KEY RESOURCES
The Key to zSystems Integrity

Metrics / Benefits

Categorization of Vulnerabilities: Provides a risk rating using CVSS standardized scoring, therefore aiding in assessment of risk, minimizing collateral damage and down time.

History Tracking: Of vulnerabilities to ensure patches are incorporated into future releases of the product

Automated Operating System Integrity Testing (OSIT) of the operating system, third-party software, and in-house written software and exits.

Immediate Results: Results are rapid, accurate, detailed and accepted by vendors.

Quality of Data : 99% accuracy rate with very few false positives, resulting in fewer mis-allocated resources, high trust level.

Detailed Reporting: Pinpoints the exact location of the identified code vulnerability.

Ensuring that all code residing within the OS layer meets IBM standards for System Integrity.

KEY RESOURCES
The Key to zSystems Integrity

DEMO

Ray Overby | Ray.Overy@krisecurity.com | m: 847-219-9100

Thank You

Cynthia Overby | Cynthia.Overby@krisecurity.com | m: 847-219-9100