

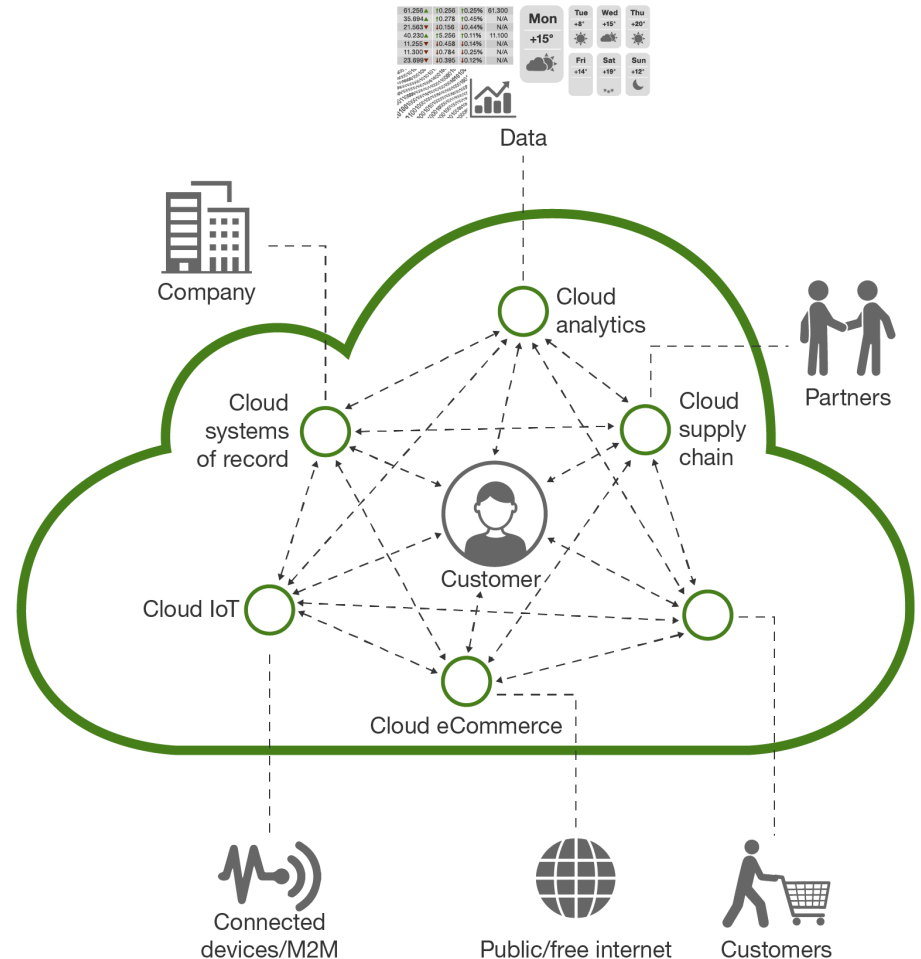
Thinking About Mainframe Modernization? Don't Overlook Security.

Amy DeMartine, Principal Analyst, Forrester
Ray Overby, CTO, Key Resources, Inc.

July 25, 2019

The Big Picture

The fastest digital businesses create **connected cloud ecosystems** with their customers at the center.

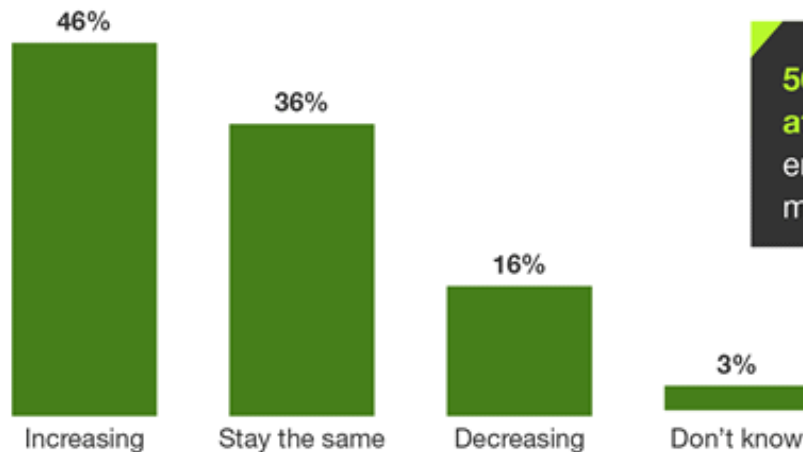


What becomes of mainframes in this world?



Mainframes aren't disappearing, they are growing

"In the next two years, will you be increasing or decreasing your use of a mainframe?"



**56% of decision makers
at North American
enterprises still use
mainframes today.***

Base: 152 North American infrastructure technology decision makers at enterprises (1,000+ employees) that use a mainframe

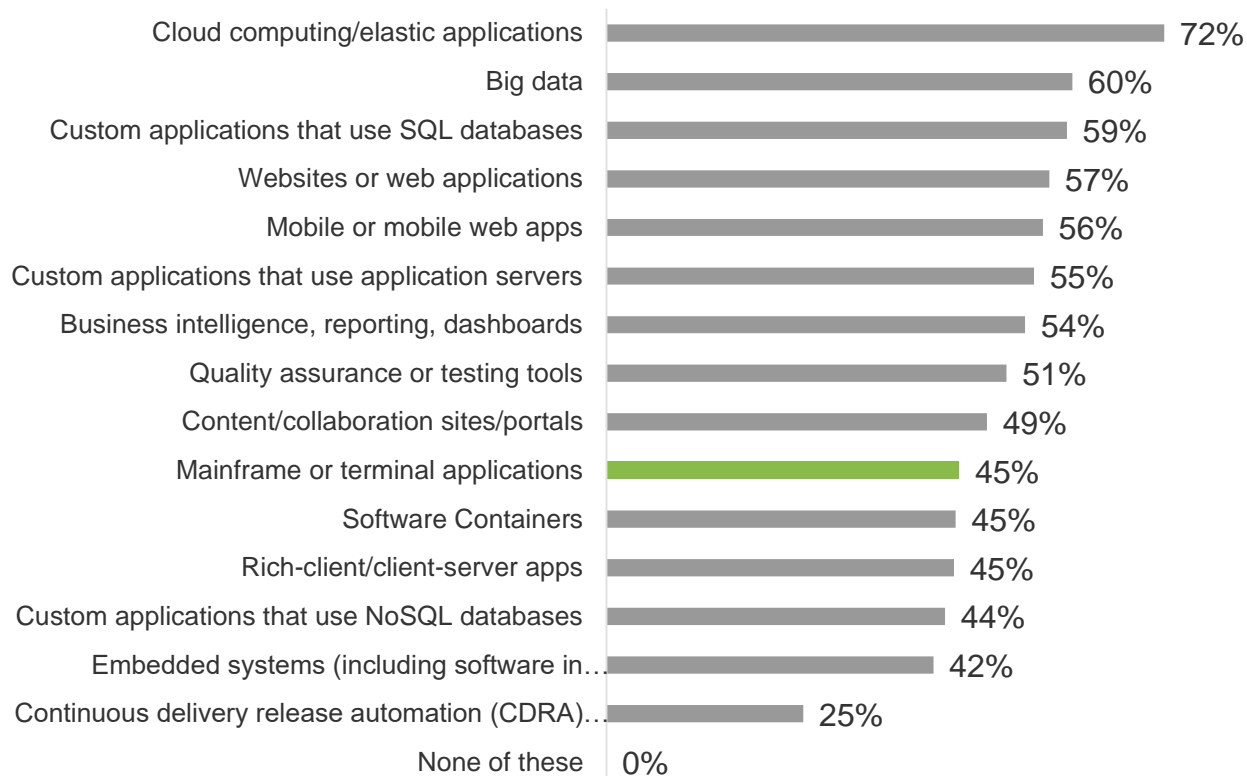
*Base: 273 North American infrastructure technology decision makers at enterprises (1,000+ employees)

Note: Percentages do not total 100 because of rounding.

Source: Forrester Analytics Global Business Technographics® Infrastructure Survey, 2018

Almost half of infrastructure professionals have used mainframe development tools in the past year

Which of the following types of development technologies have you worked with in the past 24 months?



Base: 722 North American and European enterprise infrastructure decision-makers
Source: Forrester Data Global Business Technographics Infrastructure Survey, 2018

What do you do?

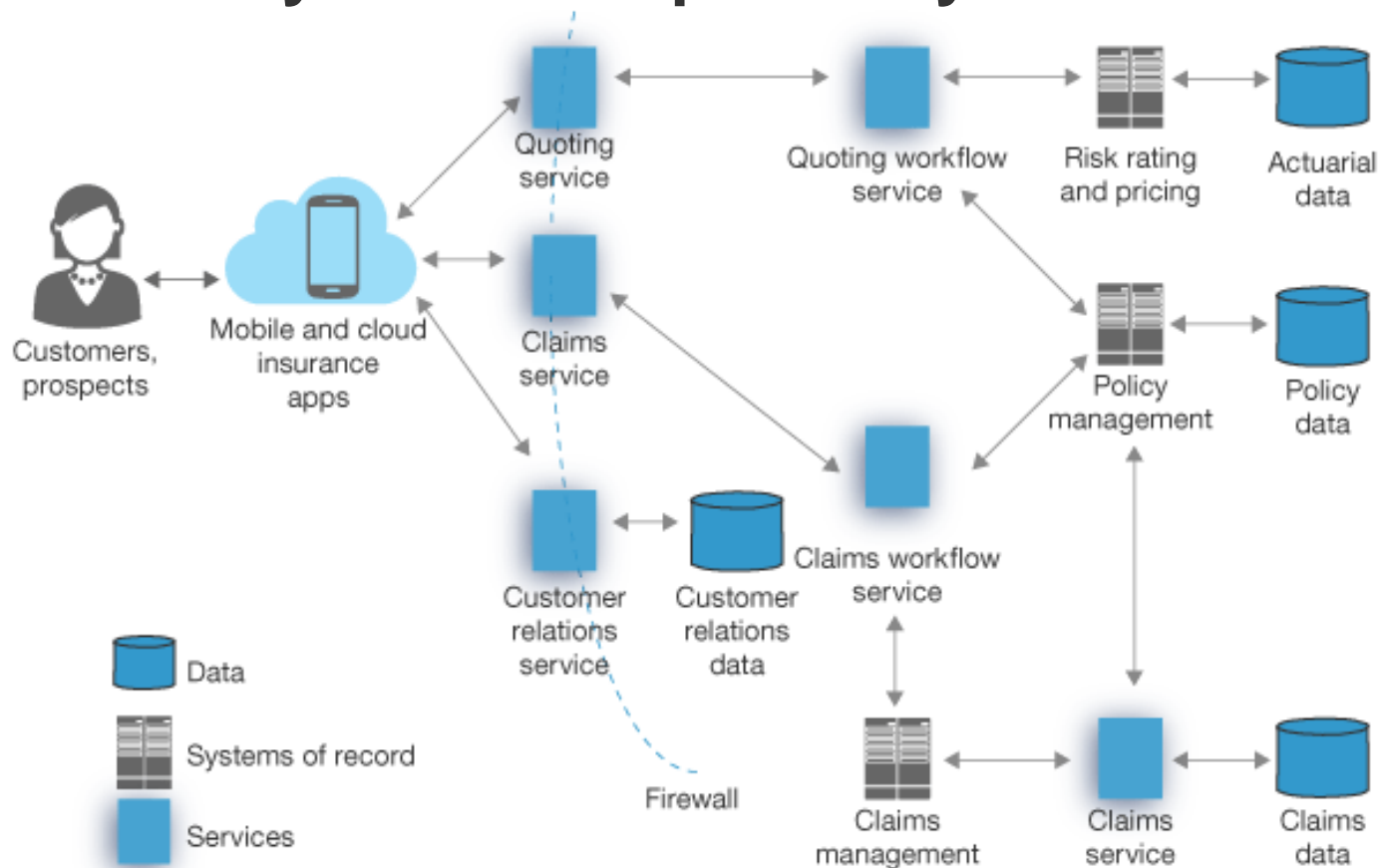
No approach is inexpensive.

- › Delay.
- › Slowly expand.
- › Migrate off.
- › Outsource.
- › Refactor.
- › Completely rewrite.
- › Double down.

What do most
companies do?

Integrate.

Integrate into your development cycles





Mainframe modernization best practices.



Say yes to DevOps on mainframe.

A close-up photograph of a vibrant red apple with a green leaf on its stem. A white measuring tape with blue markings is wrapped diagonally around the apple. The numbers 26, 27, and 28 are clearly visible on the tape. In the background, two more red apples are visible but out of focus. A semi-transparent dark grey banner is overlaid across the middle of the image, containing the text "Measure success with modern metrics." in white.

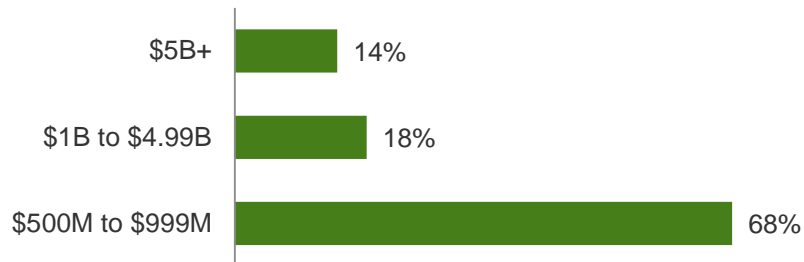
Measure success with modern metrics.



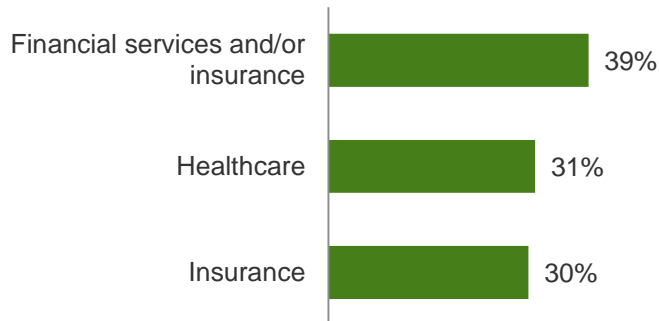
Stay current.

Firmographics and Demographics

Company revenue



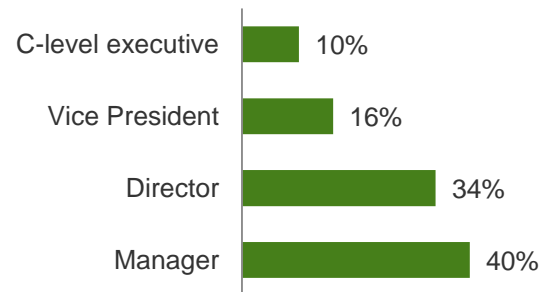
Industry



100% in IT, Security, or Risk/Governance/Compliance roles



Respondent level



Base: 225 IT management or security decision makers at companies with \$500M+ in annual revenue in North America

Source: "KRI Opportunity Snapshot", a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

We asked: **What are your top five mainframe priorities for the next year?** 95% say the most concerning ramification of mainframe security is a breach of customer data.



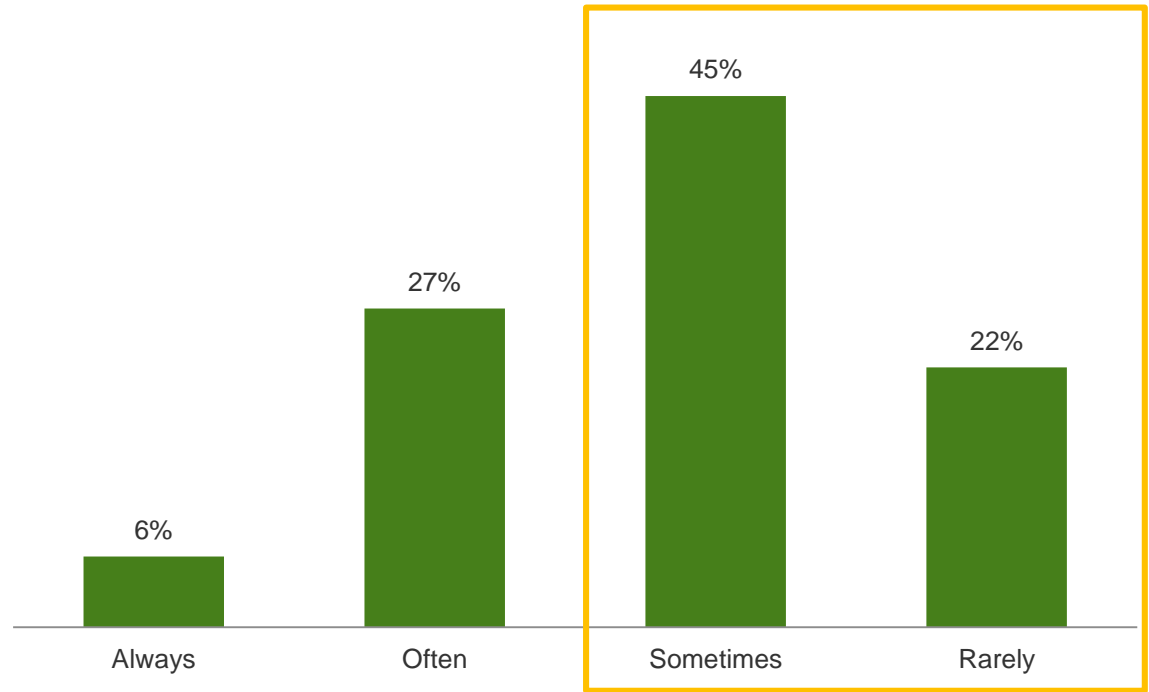
- 1 DATA BREACH PREVENTION
- 2 COMPLIANCE
- 3 RISK MANAGEMENT
- 4 IT COST REDUCTION / OPTIMIZATION
- 5 APPLICATION AVAILABILITY

Base: 225 IT management or security decision makers at companies with \$500M+ in annual revenue in North America

Source: "KRI Opportunity Snapshot", a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

Although 85% say mainframe security is a top priority (Q1), 67% of companies only either sometimes or rarely make mainframe decisions based on security.

My team and I make mainframe environment changes or process decisions based on security _____.

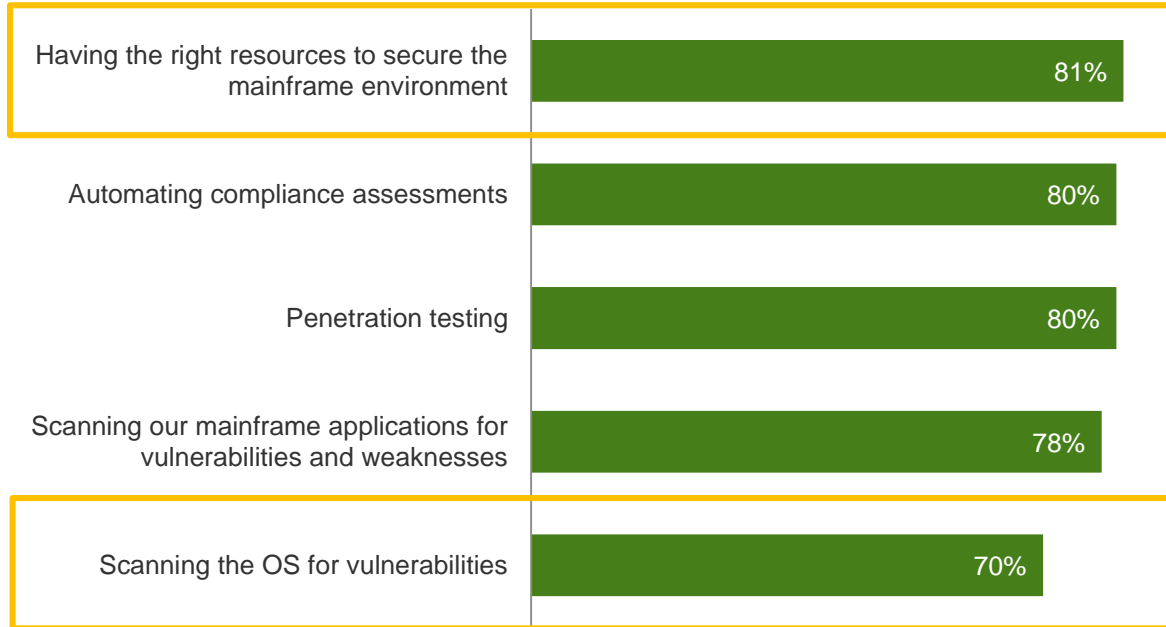


Base: 225 IT management or security decision makers at companies with \$500M+ in annual revenue in North America

Source: "KRI Opportunity Snapshot", a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

We asked: How important are the following factors when managing your organization's mainframe security?

■ Critical and High Priority



Base: 225 IT management or security decision makers at companies with \$500M+ in annual revenue in North America

Source: "KRI Opportunity Snapshot", a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

Factors of Mainframe Security

Even though data breach prevention is the top priority for companies, scanning for vulnerabilities does not rank high (70%) among important factors when managing mainframe security.

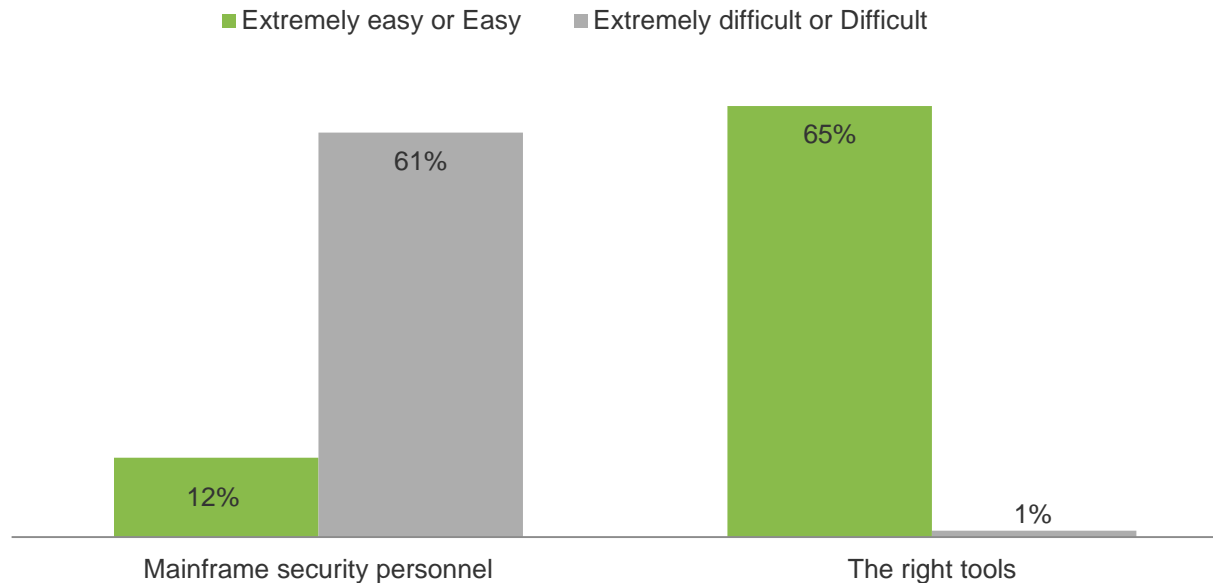


Challenges of Performing Mainframe Security

Companies think it is easy to find the right tools for mainframe security, but difficult to find the right mainframe security personnel.



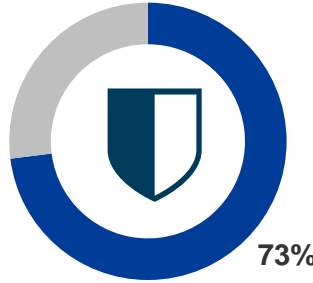
We asked: How difficult is it to obtain the following to perform mainframe security?



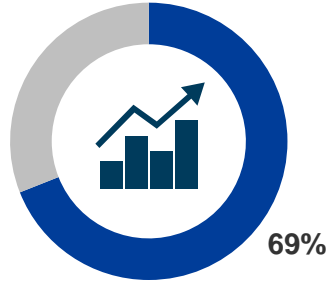
Base: 225 IT management or security decision makers at companies with \$500M+ in annual revenue in North America

Source: "KRI Opportunity Snapshot", a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

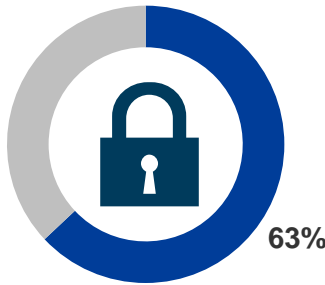
We asked: Which of the following benefits are you currently experiencing, or do you anticipate as a result of using mainframe security tools and resources?



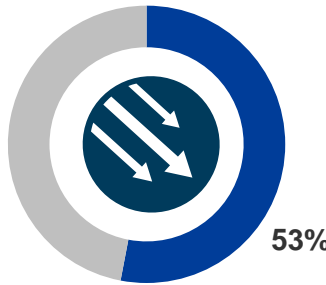
Reduced risk of data breaches



Improved privacy



Decreased data vulnerability



Reduced risk of mainframe downtime

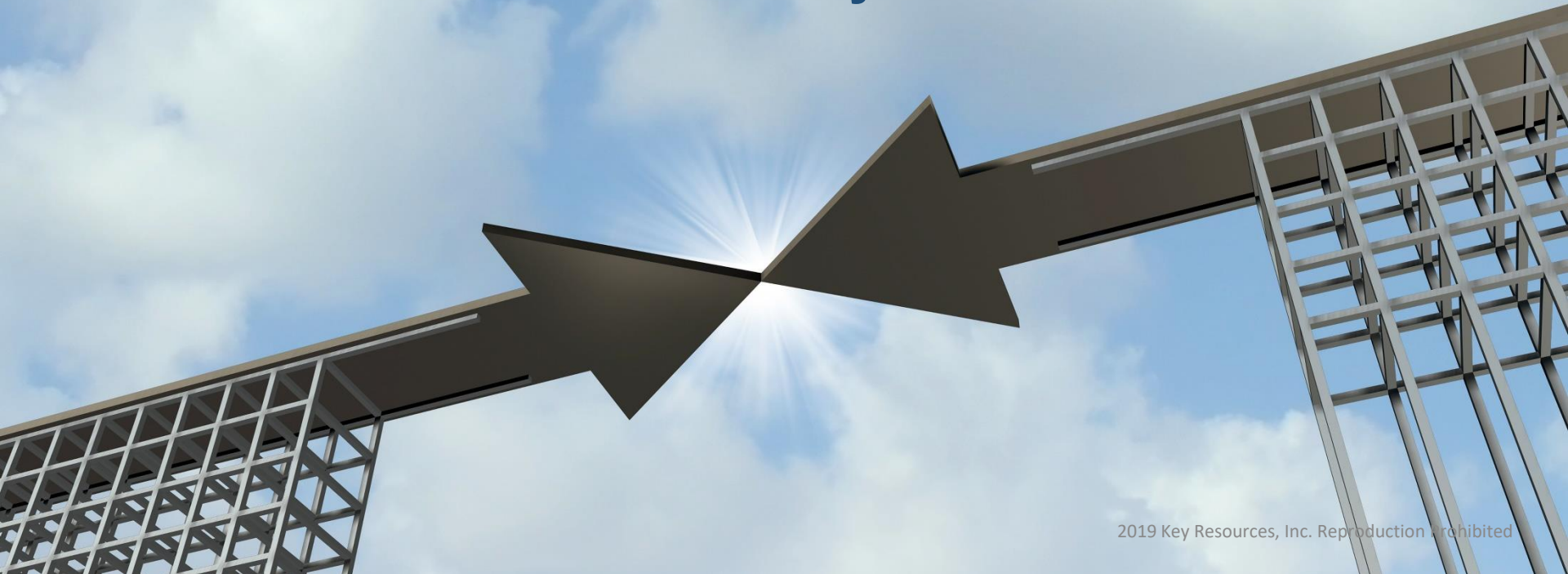
Base: 225 IT management or security decision makers at companies with \$500M+ in annual revenue in North America

Source: "KRI Opportunity Snapshot", a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

Three quarters of companies **(73%)** expect to experience / do experience a reduced risk of data breaches as a result of using mainframe security tools and resources.



Based on the results of both studies we would argue that mainframes are worth modernizing, but security practitioner's need to take action to modernize mainframe security.....



Let's Discuss:



Why a mainframe security architect is essential and what their role entails.



The risks of not including excessive access checking in your security processes.



Why separation of functions is so important in maintaining security.



Why scanning application and operating system code should be your number one priority.



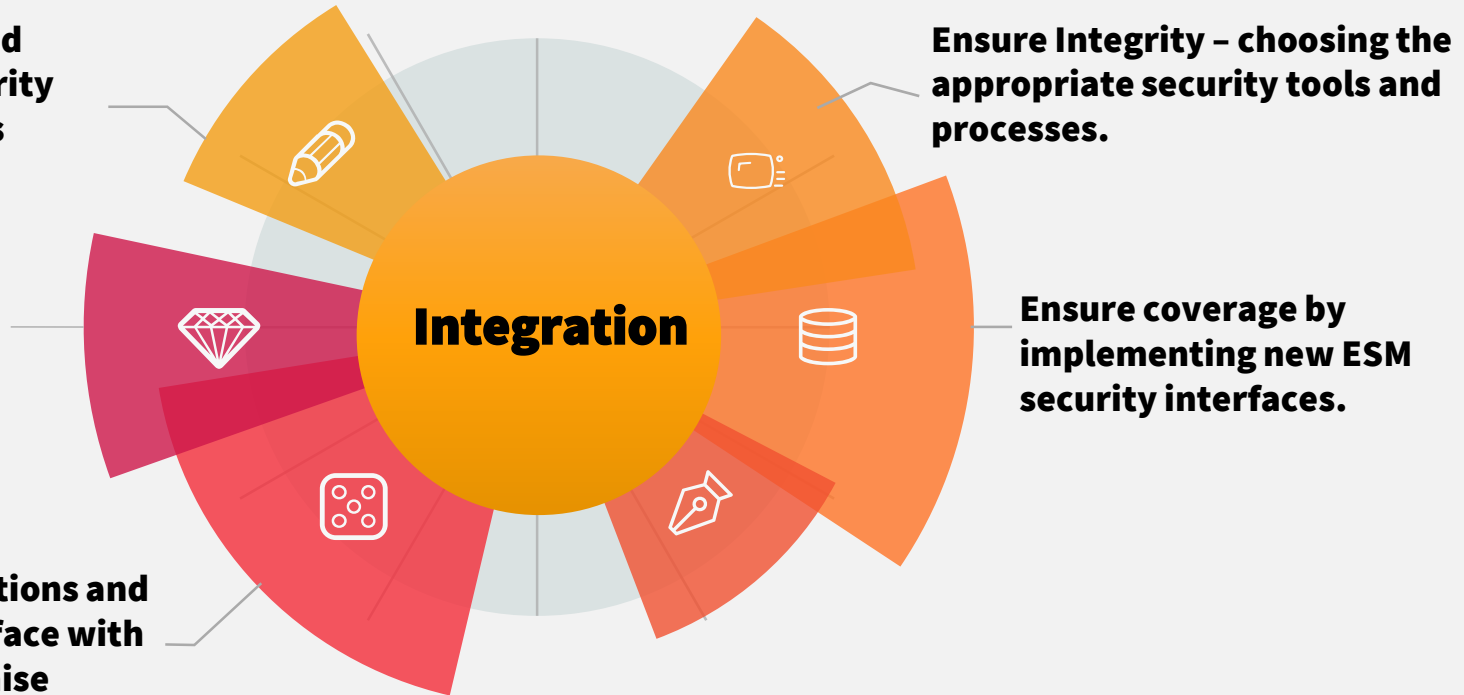
The differences between mainframe Penetration Testing and Vulnerability scanning.

Reasons why a mainframe security architect is essential and what their role entails.

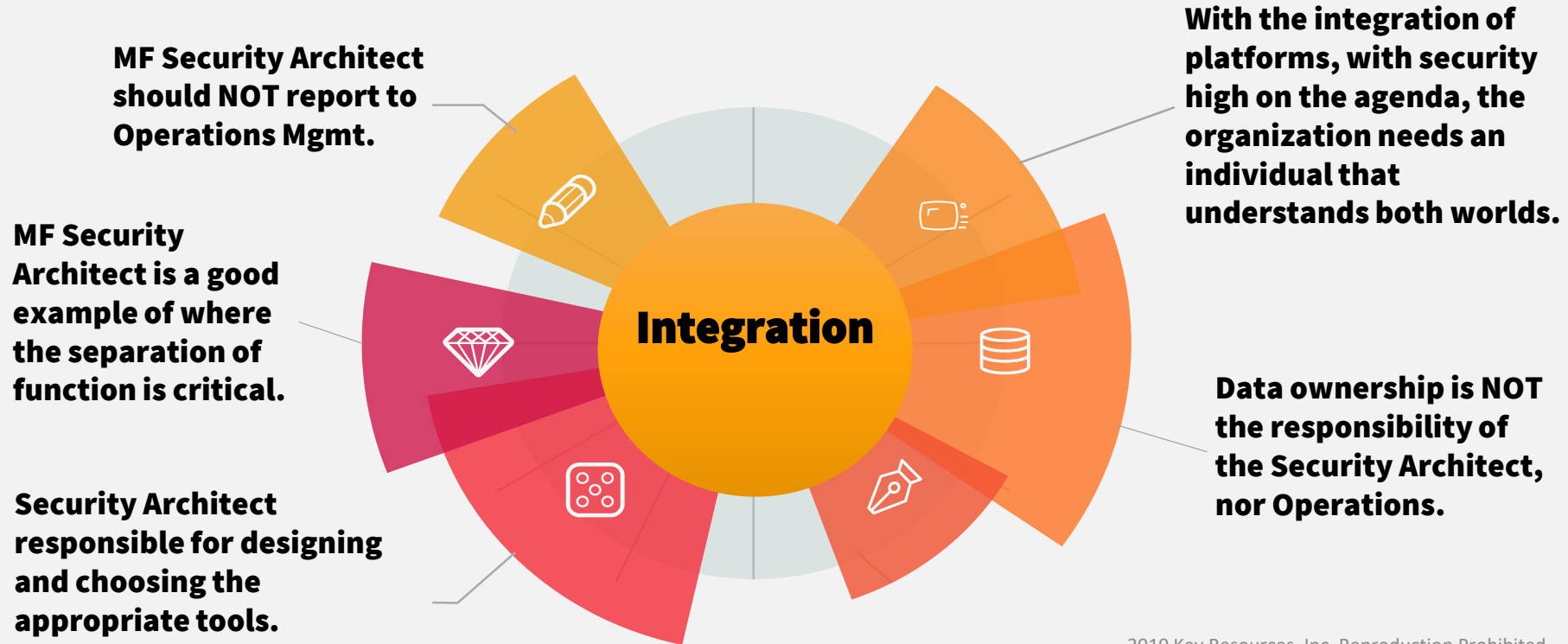
Continually review and enhance current security policy and procedures based on standards.

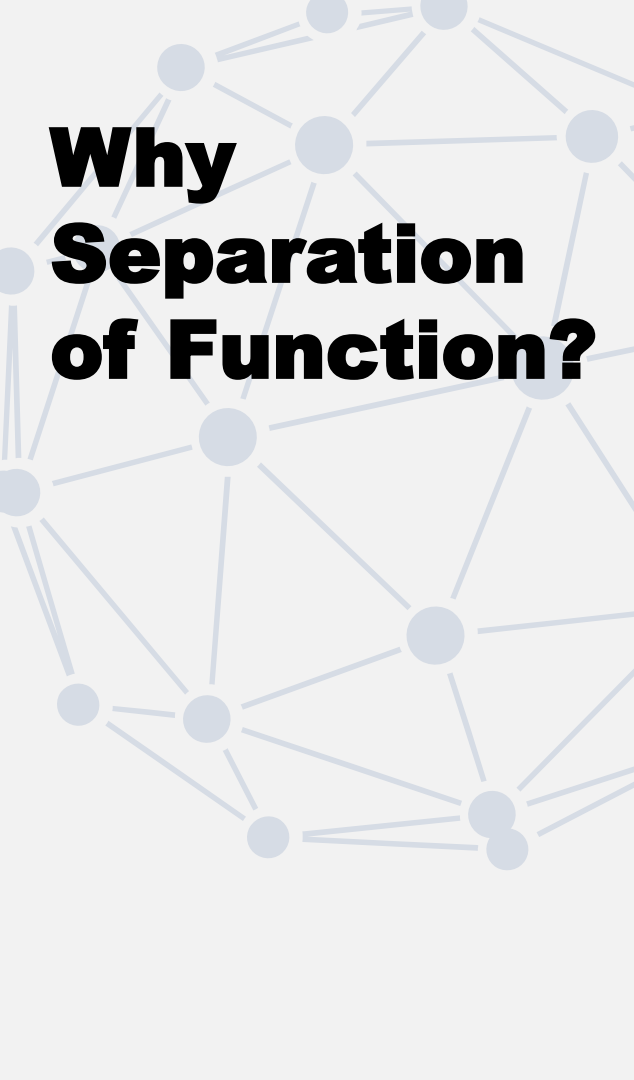
Review the security policy and procedures to take advantage of new ESM features

Ensure new applications and software that interface with MF do not compromise individual accountability.



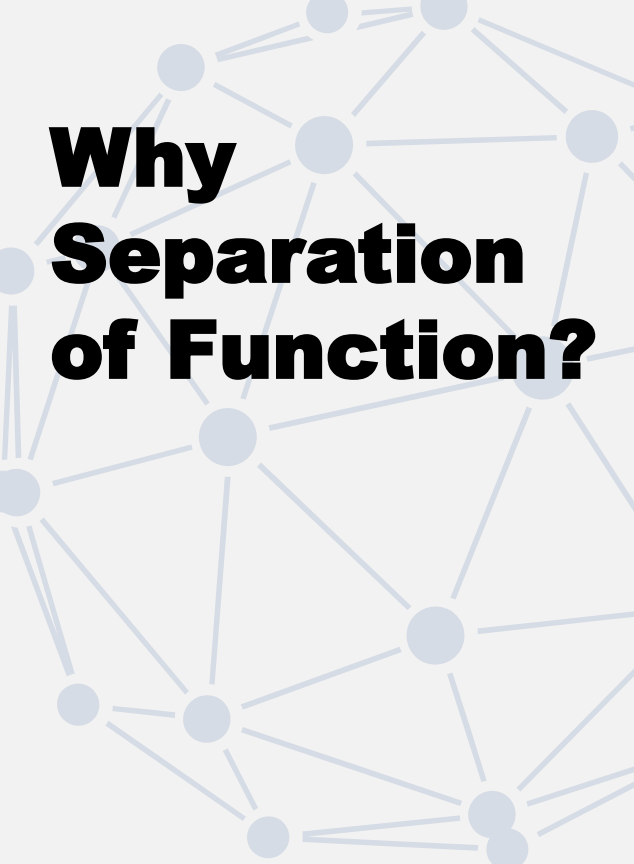
Reasons why a mainframe security architect is essential and what their role entails.





Why Separation of Function?

- Correct SoF is designed to ensure that individuals are not responsible for reporting on themselves or their manager(s). SoF, as it relates to security, has two primary objectives:
 - The first is the prevention of conflict of interest (real or apparent), wrongful acts, [fraud](#), abuse and errors.
 - The second is the detection of control failures that include security breaches, information theft and circumvention of security controls.
- New regulations such as GDPR now require that you pay more attention to roles and duties on your security team.
- The person(s) responsible for designing MF security must not be the same as the person(s) responsible for implementing, testing, conducting audits, or monitoring and reporting on MF security.
- The reporting relationship of the individual responsible for MF security should no longer be to the CIO, as has traditionally been the case.



Why Separation of Function?

- Possible Solutions as defined by GDPR:
 - Have an individual responsible for ALL of Information Security report to chairman of the audit committee.
 - Use a third party to monitor security, conduct surprise security audits and security testing. The reports go to the board of directors or the chairman of the audit committee.
- A CISO, responsible for all information security, who reports to the board of directors.
- A CISO report to internal audit, as long as internal audit does not report thru the CFO.

Understanding the risks of not including excessive access checking in your security check processing.



- ❖ It's a matter of compliance – [DISA STIGS](#) requires government agencies to do excessive access checking (EAC).
- ❖ In a fashion GDPR now requires corporations to do EAC. We've observed through the years that corporate America is somewhat averse to excessive access checking. These checks can uncover hundreds of thousands of findings, which the organization then must address.
- ❖ Doing manual excessive access checking finds which groups have access to data sets or resources, but you don't drill down to the user level. So, you won't know if there's a user in a group who shouldn't have access.
- ❖ Automation drills down into the detailed level of what people have access to, dramatically reducing the time it takes to verify compliance. Automation can help your organization stay on the right track, so you don't suddenly find 250,000+ issues to resolve at once.

Understanding the risks of not including excessive access checking in your security check processing.



- ❖ The new GDPR regulations require data ownership. This entails knowing who owns the data, who gave approvals to access the data, and who has access to your data.
- ❖ Security should not be making access decisions. They do NOT own the data.
- ❖ This access must be periodically reviewed as defined by your security policy.
- ❖ The point is that as excessive access increases, so do the risks to the organization.

Why should you scan application and operating system code?

Application and vendor software releases are hurried with less testing; developers do not always have the skillset necessary to write integrity-based software. Let's face it. Software has holes; not just distributed software.

IBM's System Integrity architecture is the reason mainframes are highly secure, but vulnerabilities in OS level code will allow breaches (without the Enterprise Security Manager (ESM) issuing any type of log entry or warning).

Without integrity you cannot have security; once the OS layer is breached the hacker has access to all of the data and all of the application layer code.....

ESM's: RACF, CA ACF2, and CA Top Secret are essential for establishing permissions and access control, but they were not architected to protect against operating system integrity vulnerabilities.

What you need to know about the differences between Distributed and Mainframe Pentesting and Vulnerability Scanning

Mainframe Pentesting

Mainframe pentesting is specifically focused on finding ways to elevate standard user privileges, gain access without permission, or exfiltrate data, by looking for vulnerabilities in the hardware/infrastructure and software.

Standards Definition of Vulnerability Scanning

The Standard definition of vulnerability scanning is: search for known vulnerabilities, be they misconfigurations, missing patches, weak versions of crypto, and default or weak passwords.

Mainframe Vulnerability Scanning

Vulnerability scanning in a mainframe context is about scanning code delivered by your application / software vendors, as well as and in-house developed code, to identify any zero-day vulnerabilities that could be exploited.

Key Takeaways

Mainframe usage is increasing to support digital transformation.

Most companies integrate mainframe into modern development cycles.

But don't integrate and forget to modernize security as software and applications are still the biggest attack vector.

Properly test and secure all of the components in the mainframe environment.

Use mainframe security tools as much as possible; fill in gaps with third party resources.



RESOURCES

The Key to zSystems Integrity

Ray Overby
ray.overby@krisecurity.com

Thank You