FORRESTER®

Zero Trust Frameworks: The Missing Piece To Mainframe Security

Why investing in a Zero Trust Framework increases stakeholder buy-in for investments in mainframe security and reduces business risk

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY KEY RESOURCES INC., | OCTOBER 2020

A Zero Trust Framework Is The Catalyst To Effectively Securing The Mainframe

Mainframes play a critical role in achieving business success, but organizations still aren't prioritizing mainframe security. This is dire, as an under-secured mainframe can lead to data breaches, malware propagation, and incorrect data ownership and access.

Forrester surveyed 209 IT and security managers with visibility into mainframe operations and found that the main challenge with building robust mainframe security is obtaining the necessary resources and buy-in.

Respondents are using their budgets to invest in Zero Trust frameworks, as they believe this technology will reduce overall risk to the business and increase stakeholder buy-in for mainframe security.

Key Findings

Firms understand that mainframes are critical for success, but less than 50% prioritize mainframe security. Nominal mainframe security leads to data breaches and vulnerable data.

IT and security leaders understand the value of the mainframe, but they have a hard time gaining stakeholder buy-in.

IT and security leaders prioritize investments in Zero Trust frameworks, believing the benefits will increase internal prioritization of mainframe security and reduce business risk.

Mainframes Are Essential, But Firms Still Aren't Prioritizing Mainframe Security

The argument for mainframes is tried and true: 86% of respondents agreed that mainframes are essential for driving a highly scalable workload, and 75% said they are critical for business continuity.

Considering the mainframe's value is universal, it's shocking that only 45% of respondents said that mainframe security is an organizational priority. IT respondents expressed that their firms prioritize other technology (e.g., cloud) instead of mainframe security, which makes securing the mainframe exceptionally difficult.

This is extremely problematic, as 62% of respondents said failure to secure the mainframe will lead to data breaches.

"What are the top challenges of implementing mainframe security at your organization?"

77%

of respondents are focused on cloud or other tech.

72%

of respondents said IT leaders/stakeholders are not prioritizing mainframe security.

62%

of respondents said IT leaders/ stakeholders believe the mainframe is inherently secure.

Base: 209 enterprise IT managers and above with visibility into mainframe management and monitoring
Source: A commissioned study conducted by Forrester Consulting on behalf of KRI, August 2020

Lack Of Prioritization Leads To Poor Data Ownership

Sixty-five percent of respondents said they struggle to classify and categorize data ownership. When asked why, they indicated that stakeholders would rather invest in cloud and they do not have budget for data ownership. Firms are following that shiny gold nugget (the cloud), but they are forgetting to allocate resources to the fundamentals and essential prerequisites to securing their enterprises. Not investing in a data ownership strategy has vast consequences to the business.

"What are the consequences of not having a strong strategy for data ownership?"

1. Increased exposure to risk/ data breaches
2. Unauthorized access to critical data
3. Lack of control of who has data access

FORRESTER OPPORTUNITY SNAPSHOT:

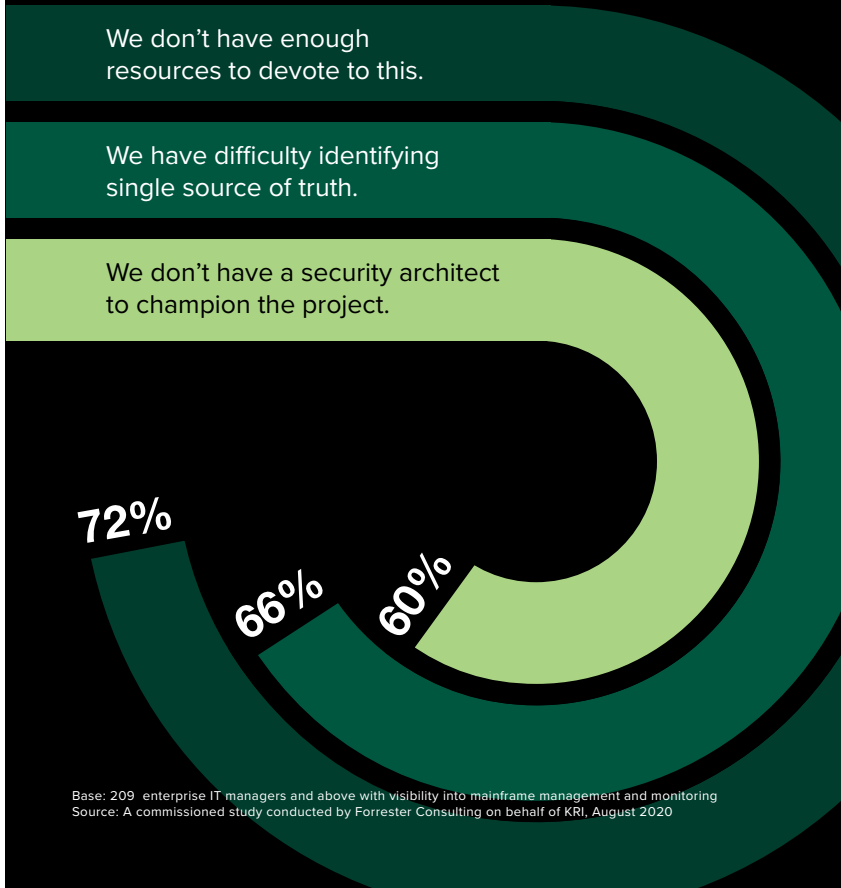
Base: 209 enterprise IT managers and above with visibility into mainframe management and monitoring
Source: A commissioned study conducted by Forrester Consulting on behalf of KRI, August 2020

Zero Trust Is The Solution, But IT Leaders Lack The Resources To Implement

Respondents stated that adopting a Zero Trust framework is the key to achieving a secure mainframe. However, IT and security leaders are running into the same problem: They do not have the resources to make this a reality.

Eight out of 10 respondents indicated their mainframe security management is understaffed. They said they do not have the necessary general resources or people like a security architect to implement a Zero Trust framework. Without the right resources and as stakeholders champion a Zero Trust framework, firms and their data are left out in the open.

“What are the top challenges with implementing a Zero Trust framework on the mainframe?”

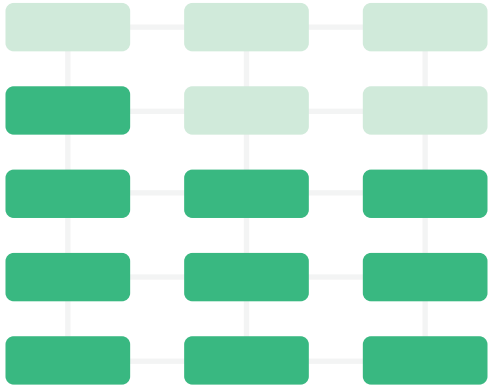


Base: 209 enterprise IT managers and above with visibility into mainframe management and monitoring
Source: A commissioned study conducted by Forrester Consulting on behalf of KRI, August 2020

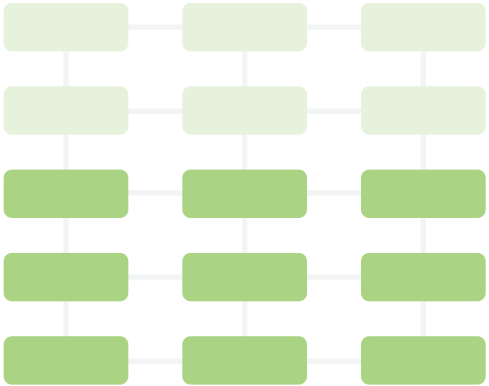
Leaders Push To Adopt Zero Trust Frameworks

IT and security leaders are not letting the lack of stakeholder buy-in hold them back; they have reserved resources to invest in a Zero Trust framework. Forty percent of respondents indicated they have already adopted a Zero Trust framework, and 60% said they plan to adopt one in the next 12 months. Respondents view this as a business imperative, as 67% expect the framework to reduce overall risk and 61% expect it to increase mainframe security prioritization.

Zero Trust frameworks are expected to effectively secure the mainframe.



67%
of respondents expect Zero Trust frameworks to reduce overall risk.



61%
of respondents expect a Zero Trust framework to increase mainframe security prioritization.

Base: 209 enterprise IT managers and above with visibility into mainframe management and monitoring
Source: A commissioned study conducted by Forrester Consulting on behalf of KRI, August 2020

Zero Trust Frameworks Yield Strong Technology Benefits

Outside of the business benefits, IT and security leaders expect strong technology benefits from investing in a Zero Trust framework. Respondents indicated a Zero Trust framework would directly solve some of their top mainframe security challenges, like achieving stronger data ownership (56%) and creating a more efficient data management process, (63%), while also improving access visibility and control and more efficient data management processes overall. Zero Trust will also supply the extra peace of mind mainframe owners need when it comes to their ability to detect data breaches (60%).

“What technology benefits would you expect to see from adopting a Zero Trust security framework?”

Base: 209 enterprise IT managers and above with visibility into mainframe management and monitoring
Source: A commissioned study conducted by Forrester Consulting on behalf of KRI, August 2020

Conclusion

Businesses that do not prioritize mainframe security risk vast consequences: data breaches, compliance fines, and insurmountable data ownership issues. In today's world, weak data management will impede your business. Securing the mainframe must take precedence.

Zero Trust frameworks not only provide the structure necessary to effectively secure the mainframe and prevent data breaches and malware propagation, but they also create a strong value proposition for investing in mainframe security. IT and security leaders are investing in Zero Trust framework architectures to build the business case for mainframe security in tandem with other rising technologies like cloud.

Project Director:

Vanessa Fabrizio, Market Impact Consultant

Contributing Research:

Forrester's Security and Risk research group

Methodology

This Opportunity Snapshot was commissioned by Key Resources Inc. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 225 IT or security decision-makers at companies with a revenue band of $500 million or more. The custom survey began and was completed in August 2020.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY
KEY RESOURCES INC., | OCTOBER 2020

Demographics

COMPANY SIZE

- $500M to $999M: 49%
- $1B to $5B: 42%
- >$5B: 10%

COMPANY GEOGRAPHY

- United States: 71%
- Canada: 29%

RESPONDENT LEVEL

- Manager: 47%
- Director: 33%
- Vice president: 12%
- C-level executive: 7%

INDUSTRY

- Retail: 10%
- Business or professional services: 9%
- Financial services and/or insurance: 7%
- Construction: 7%
- Chemicals and/or metals: 7%
- Telecommunications services: 6%
- Consumer product goods/ manufacturing: 6%
- Agriculture, food, and/or beverage: 6%
- Consumer services: 5%


FORRESTER®