# Table of Contents

01  Introduction

02  Sample Roadmap

03  Create and Align Your Strategy

03  Determine Your Current Mainframe Security Maturity

04  Mainframe Workload Security

05  Communicate Value and Set Expectations

06  Conclusion
Introduction

Many organizations have depended on traditional perimeter defenses to prevent threats from compromising their mainframes – that is until recently. In light of the strong pivot to remote work in 2020, large scale change has been enacted to support new security architectures, business transformation and a growing attack surface. All of the above leading many to reassess and adopt a Zero Trust model for their enterprise and pivot to a more holistic eXtended Zero Trust (ZTX) approach.

While much has been written about Zero Trust, systems that are among the ZTX ecosystem are often not as well defined. In this piece, we will look at how to apply “A Practical Guide to a Zero Trust Implementation” by Forrester Research to one of these systems – the mainframe.

Source: A Practical Guide To A Zero Trust Implementation, Forrester, March 3, 2021
The Sample Roadmap is intended to serve as a guide and there are a few areas where it is clear the mainframe should be in view. But where should you begin?

Source: A Practical Guide To A Zero Trust Implementation", Forrester, March 3, 2021
Step 1: Create and Align Your Strategy

Zero Trust has multiple pillars and each has multiple requirements. You need to do your homework and leverage the ZTX framework to help you map out a strategy. This has the added benefit of helping you understand the dependencies and stakeholders who need to be involved. Often Zero Trust implementations are a broader IT project and the mainframe is no exception. A typical list of key players is: C-level participation from security and business owners, IT Operations leadership and Enterprise Architects. Each stakeholder will own a different piece of the puzzle and alignment at this stage will help conflicts later. Mapping dependencies and current projects will also help to set expectations for everyone involved. A new or shifting investment may be required as well as resource or organizational changes across Operations, Security and Infrastructure teams.

Step 2: Determine Your Current Mainframe Security Maturity

The two core components of the ZTX ecosystem are: Identity Management and Device Security. Mainframe organizations often feel that current IAM tools are enough and overlook any sort of device security. This is problematic for two reasons—
1. Mainframe Identity Access often fails to implement effective controls for password management and privileged accounts. Secondly many mainframe organizations do not implement security for their mainframes because they believe the perimeter or the native security controls provided with it are enough. The latter sounding eerily like the “trust but verify” approach Zero Trust is intended to replace! Both of them certainly don’t account for threats and vulnerabilities that are already in your environment.

A proper implementation of Zero Trust for the mainframe must begin with a critical look at the current controls in place and determining how to establish device security that aligns with your existing security teams and tools as much as possible. Implementing Zero Trust for the mainframe should begin with an audit of your current controls (performed by an external or internal resource depending upon your security maturity). The native security of your mainframe should also be examined to identify gaps and to determine what will best complement and address them. Penetration testing is advisable here as a means of uncovering the areas an attacker would attempt to exploit in a real-world situation.

With your newfound visibility and understanding of the current mainframe security maturity, you can take 2 practical actions: Apply least privilege and implement secure configurations to address current security gaps and better manage policy drift. Overprivileged users and credentials with unchecked data access are one of the most common causes of breaches.
Step 3: Mainframe Workload Security

Mainframes process an enormous amount of data and while we often consider their efficiency for cost measures or optimization, we don’t always think of them as sources of operational data that may be indicators of compromise (IOC). If compromised or controlled by an attacker, increases in demand and workload sizes in a production environment may be a symptom that an intruder is leveraging the mainframe in an attack.

The key to proper coverage is visibility for mainframe operations, security and infrastructure teams. Without inclusion into a formal governance process or silos across teams the security of your mainframe workloads will be dependent on manual processes and simple checkbox compliance exercises.

This is again an area that an in-depth assessment of current configurations and controls can shine a light on weak configuration settings. Additionally an investment in tools that aid in automating and integrating data should be considered.

Data should also be considered to understand the valued, lifecycle and the proper steps and technologies to ensure access, use, disposal and obfuscation are taken.
Step 4 Communicate Value and Set Expectations

Considering the commitment and budgets that may be required to include the mainframe into your Zero Trust enterprise strategy, you need to be clear on the threats to the mainframe and the risks associated with not protecting it.

The mainframe is a system that often holds the “crown jewels” of customer or corporate data but that isn’t always clear to the boards and business leaders of large enterprises.

No Hall Passes Allowed
CISOs, CIOs, CEOs or board members should be clear on the data that resides on the mainframe, the cost of not protecting it and that a proper Zero Trust strategy implementation by definition cannot leave the security of the mainframe to trust in a perimeter or the word of the vendors who create or deliver the software that runs on it. The mainframe may have long held a trust but verify (someday) relationship to the enterprise because of its age and long standing relationship. Modern CISO and Business leaders however should be ready to fully commit to Zero Trust and move away from this outdated mindset.

Demonstrate the business value
Asking for investment and commitment will come up as resources and budget are nearly always connected to implementing any new strategy or technology.

Be prepared to reinforce the benefits of applying Zero Trust to your mainframe environment such as:

- securing customer trust
- improving efficiency and leveraging current investments through integrations.
- side benefits like added context and insights on operations and security which can also aid in achieving complementary efforts like extended detection and response (XDR).
Conclusion

Zero Trust is a framework that takes time. We’ve covered the initial steps in this piece to help Security and Operations teams alike understand the place of the mainframe in the scoping, strategy and planning cycles. The work of applying least privilege, integrating the mainframe with security tools and workflows will need to be included in the scope of your Zero Trust implementation. Tools like BMC AMI Security which provides automated detection and response for mainframe security events while delivering alerts in real time to your preferred SIEM can accelerate this stage. If expertise or staff are in short supply, consider leveraging a services provider who can evaluate your mainframe security controls and help you perform regular penetration tests to keep it secured.