Rocket® software

Using Multifactor Authentication to Authorize Mainframe Access

Let's Talk about Passwords

Authenticating users with usernames and passwords is no longer secure.
Why? Because users are careless with passwords. They choose obvious ones. They use the same password over and over again. And they write passwords down on sticky notes that anyone can find.

But users aren't the only problem

Relying on the human element is dangerous in today's cyber environment. Strong passwords are essential for maintaining security. However, if a user has a complex password, they may forget it. If the password is weak, it can be easily guessed. In other words, securing your mission critical data should not be based on just one password typed in by a user.

Eight character, case insensitive passwords

In many instances organizations are still using eight character, case insensitive passwords on the mainframe. This can leave business-critical, sensitive mainframe data vulnerable to an attack. Change can be difficult, but it essential to do away with this practice to ensure that your mainframe stays secure.

What is multifactor authentication (MFA)?

MFA combines multiple identity sources as a way to verify the identity of the user or process. The most effective MFA solutions combine at least two of the following three types of identity sources:

- Something you know, such as a PIN code or password.
- Something you have, such as a key card, phone, or token.
- Something you are, such as a fingerprint, retina scan, voice recognition, or facial recognition.

By requiring at least two of these three identity sources, you greatly strengthen your authentication requirements and reduce the risk of a security breach.

The growing need for MFA

Organizations are becoming increasingly aware of the risks associated with single-factor authentication for online transactions. Verizon 2022 Data Breach Investigations Report found that compromised credentials are the primary attack vector, with 63% of breaches attributed to leveraged credentials. MFA can mitigate this costly problem, making electronic payments as quick and reliable as cash payments.

The proliferation of new government regulations, is also driving MFA adoption. The updates include:

In March 2022, PCI DSS 4.0 was released to replace the current PCI DSS 3.2.1 standard by March 2025. Requiring organizations to become compliant with 4.0, focusing on security incidents that occur on an end user's computer rather than on an organization's servers or on the network in between the two.

- Recently, the U.S. federal government announced the National Cybersecurity Strategy, which includes the following goal: expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance.

- The Internal Revenue Service (IRS) in the United States has issued Publication 1075 (IRS 1075), which provides guidance for U.S. government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practice practices, and controls to protect FTI's confidentiality.

If MFA is so great, why haven't we been using it?

Change often goes hand-in-hand with resistance, and migrating to MFA is no different. Resistance to MFA is usually attached to one or more of the following reasons:

- **Difficult to setup and enforce** — Biometric authentication methods (fingerprint scanners,. retina scanners, facial recognition, etc.) are readily available on mobile devices and PCs. However many organizations have not adopted this technology, as the setup and enforcement can be too difficult for some organizations. Couple that with external users that need access — even if they have biometrics, what if they are not setup correctly and how do you properly enforce biometrics on these users? This becomes almost impossible to manage.
- **Fear of the unknown** — For example, will MFA complicate the user experience? Because ease of use often translates to efficiency, organizations are hesitant to change the status quo for any reason — even stronger security.
- **Fear of failure** — In order to reap all the benefits of MFA, you need to set it up across-the-board. If you don't, you'll get only mediocre results. The breadth of implementation required can be daunting.

When it comes to implementing MFA for authorizing mainframe access, the roots of resistance can be even harder to overcome.

> According to Verizon's 2022 Data Breach Investigations Report, the human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike.
>
> **VERIZON'S**
> 2022 Data Breach Report

MFA and the mainframe

Many organizations are faced with a growing problem — they generally use one system for the enterprise and another for the mainframe. This creates complexity and additional costs for the organization as they have to manage and maintain multiple systems. And when it comes to MFA, it's not easy on the end user as they may have to use different authenticate methods depending on the system the are using.

Organizations need to extend strong, centrally managed security to mainframe applications — without jeopardizing business operations.

The Rocket Software solution

In fact, there is a safe, manageable, economical way to extend strong, centrally managed security to mainframe applications. It's called Rocket® Host Access Management and Security Server* (MSS). MSS works by leveraging your existing Identity and Access Management (IAM) system to manage and secure mainframe access via your Rocket Reflection Desktop, Rocket InfoConnect Desktop, and Rocket Rumba+ desktop terminal emulators.

Sitting between the user and the mainframe, MSS uses your existing LDAP authentication structure to validate a user's credentials before granting mainframe access. In other words, users can't get near the host logon screen until they've been authenticated and authorized with strong IAM credentials — i.e., strong complex passwords.

MSS works in tandem with an add-on product called MSS Advanced Authentication to provide the strongest possible authentication for your mainframe systems. Together, these two products currently support many different authentication methods — from smart cards and mobile text-based verification codes to fingerprint and retina scans. From this range of options, you can pick the ones that are easiest for your organization to adopt and sustain.

MSS and MSS Advanced Authentication provides a flexible, highly secure solution for mainframe access that doesn't jeopardize business operations.

Rethinking MFA for the mainframe

When new technology gets rolled out, it often fails because no one thought through all the implications. For MFA, there are several things you need to consider before you start:

01

Establish and implement a global authentication policy (rather than taking a piecemeal approach with ad-hoc acquisitions).

02

Make MFA easy to manage (avoid different authentication technologies for different systems).

03

Make MFA easy to use (consider implementing single sign-on at the same time to simplify the authentication process).

Done right, MFA actually makes life easier for your users. After all, swiping your finger across a scanner and entering a PIN is easier than remembering a username and password.

*formerly a Micro Focus® product

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X.

Rocket software

Modernization. Without Disruption.™

Visit RocketSoftware.com ›

Learn more

MAR-10409_WP_UsingMFAToAuthorizeMainframeAccess_V7