White Paper

Using Multifactor Authentication to Authorize Mainframe Access

opentext™

Passwords Are Bad

To be blunt, authenticating users with usernames and passwords is no longer effective. 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

When you rely on usernames and passwords, you're practically handing hackers the keys to your kingdom. Savvy criminals write advanced algorithms to find ports of entry. Then, when the same password is used for multiple apps, hackers who have cracked one password can snoop around wherever they please. For example, a hacker might steal a user's Facebook password and in so doing gain access to your entire corporate infrastructure. That is a huge cause for concern.

The bottom line is that usernames and passwords are things a user has to know. And those things can be captured or stolen with relative ease. On their own, they just aren't secure enough.

Old Mainframe Passwords Are Scary Bad

The password problems just described also apply to mainframe passwords. The difference is that mainframe passwords for older applications—the ones that run your business and contain all your most sensitive data—are protected only by eight-character, case-insensitive passwords. Written decades ago, in a safer time, mainframe applications were hard-coded with weak eight-character password security because that was good enough. Not anymore.

What Is Multifactor Authentication (MFA)?

MFA combines multiple identity sources as a way to authorize access. 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.

What's Not MFA?

When your bank asks you for your PIN and your social security number, that's *not* MFA. PINs and SSNs are both things that you *know*. MFA combines two of three *different* sources from things that you know, have, or are.

The Growing Need for MFA

Organizations are becoming increasingly aware of the risks associated with single-factor authentication for online transactions. "Verizon's 2013 data breach report, which pointed the finger at single-factor authentication as a primary culprit in security spills, reported that 76 percent of network intrusions in 2012 exploited weak or stolen credentials." MFA can reverse this costly problem, making electronic payments as quick and reliable as cash payments.

The proliferation of new government regulations, such as HIPAA, is also driving MFA adoption. On March 26, 2013, new U.S. Department of Health and Human Services rules went into effect. These rules extended HIPAA security and privacy requirements to business associates—including contractors, vendors, and service providers—who perform services on behalf of a health care provider or who provide solutions that integrate with medical or patient data. With hefty fines for noncompliance, many organizations are moving to MFA.

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:

- **Lack of information—**Biometric authentication methods (e.g., fingerprint scanners) have already been built into smartphones and PCs. But many companies just don't know how to incorporate that new technology into their established security infrastructures.
- **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.

MFA and the Mainframe

While security for accessing enterprise applications has grown stronger to meet increasingly sophisticated threats, the security written into your mainframe applications has stood still for decades. Try asking any IT security professional if they think eight-character, case-insensitive passwords provide an appropriate level of authentication for sensitive data. The answer will be a definite "No!" Even so, the mainframe is typically left out of MFA discussions.

Here's the problem: Robust and reliable as it is, the mainframe is typically isolated from the rest of the enterprise. IT Admins consider it an area best left to the mainframe experts. Those experts—Mainframe Systems Admins—know that reengineering mainframe applications to work with strong complex passwords is risky, difficult, and expensive. They have no desire to jeopardize the mainframe's 99.999 percent reliability record. Much as they are concerned about security, they feel stuck.

What's needed to overcome their resistance is a way to extend strong, centrally managed security to mainframe applications—without jeopardizing business operations.

The OpenText Solution

In fact, there is a safe, manageable, economical way to extend strong, centrally managed security to mainframe applications. It's called OpenText™ Host Access Management and Security Server (MSS). MSS works by integrating your mainframe with your Identity and Access Management (IAM) system, managing and securing mainframe access via your OpenText™ 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 14 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 can be installed on a server or on the mainframe—whatever works best for your business. It 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:

- Establish and implement a global authentication policy (rather than taking a piecemeal approach with ad-hoc acquisitions).
- Make MFA easy to manage (avoid different authentication methods for different systems).
- 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.

What to Look for in an MFA Vendor

To ensure a smooth MFA integration, keep these factors in mind during your research:

- Look for solutions that offer multiple authentication options and applications.
- Don't get locked in to a single type of physical authentication (in other words, don't let the hardware you choose dictate your authentication philosophy).
- Look for vendors who develop to an open framework that is aggressively updated as new technologies are launched.
- Look for vendors who can make the system easy for you.

It doesn't make sense to require strong authentication for accessing enterprise applications but only weak authentication for accessing mission-critical mainframe applications, the ones that run your business. As security threats continue to escalate, your organization must rise to the challenge. OpenText offers a safe, manageable, and economical way to do it.

Learn more at
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™