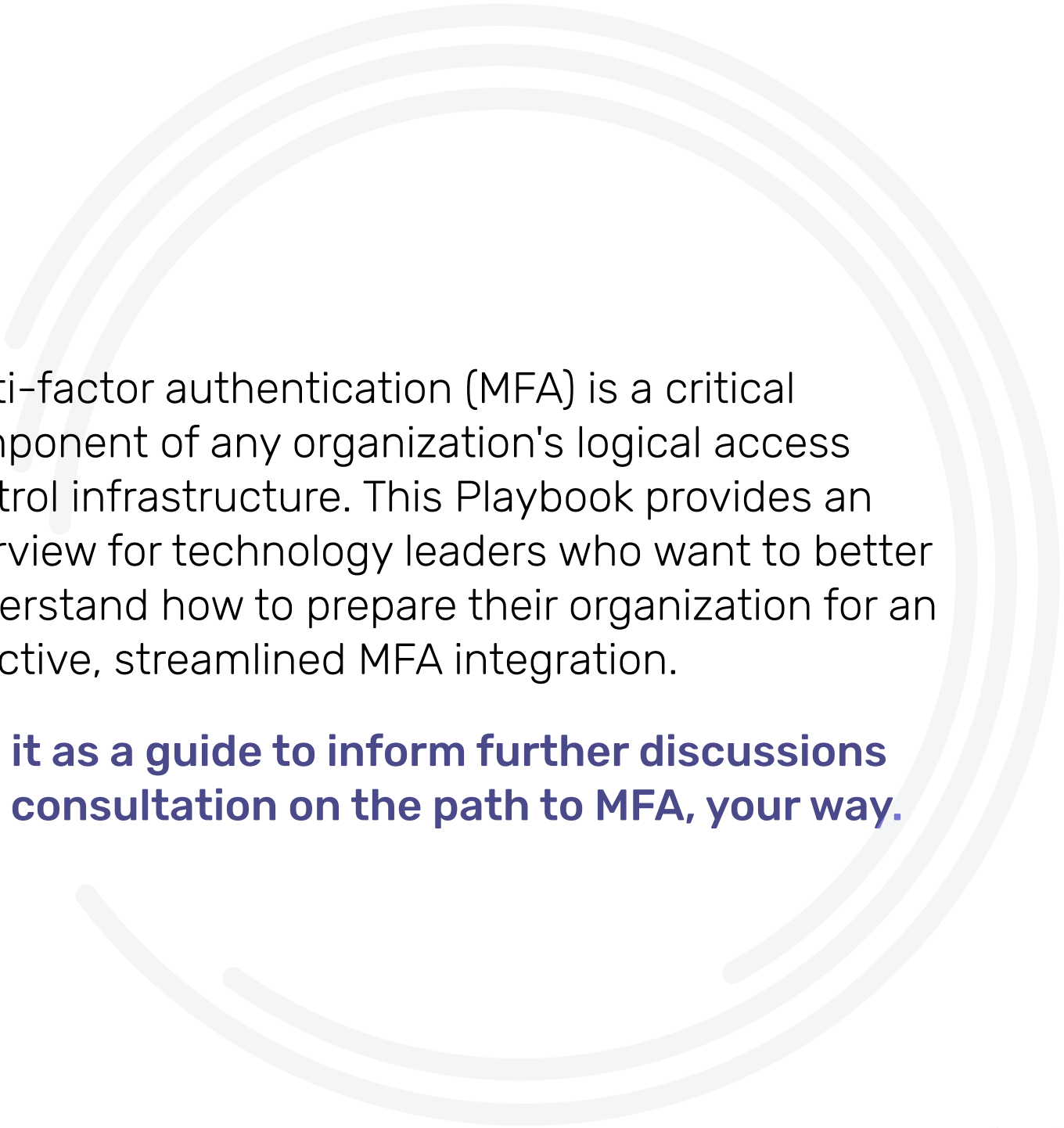




MFA Readiness Playbook

Your Guide to Secure
Multi-Factor Authentication





Multi-factor authentication (MFA) is a critical component of any organization's logical access control infrastructure. This Playbook provides an overview for technology leaders who want to better understand how to prepare their organization for an effective, streamlined MFA integration.

Use it as a guide to inform further discussions and consultation on the path to MFA, your way.

● GETTING READY

Start with a security strategy

Integrating multi-factor authentication begins with a closer look at all technology systems that could be vulnerable to external attacks or insider threats.

Review workstations, secure printers, time clocks, cafeteria POS systems, manufacturing floors, common areas—anywhere users can access critical data or systems. By adding two or more authentication factors, these information systems are **99.9%** less likely to be compromised than when users present just one.¹

In addition, **90%** of passwords are considered vulnerable, so additional authentication factors can virtually eliminate risk here, too.²

Once you've prioritized overall security gaps, established preventative protocols, and clearly understand the risks of direct and indirect attacks, you can focus specifically on getting the most from your MFA solution.



1. www.techbeacon.com/security/state-mfa-4-trends-portend-end-solo-password
2. www.businessinsider.com/90-percent-of-passwords-vulnerable-to-hacking-2013-1

Zero Trust: A policy that protects

A recent U.S. executive order requires federal agencies—and all third-party contractors or vendors operating on behalf of a government agency—to adopt ‘Zero Trust Architecture.’ This adoption makes sense for large organizations and SMB enterprises beyond the government, too.

Nearly 50% of all cyberattacks target small businesses.³

Zero Trust delivers cybersecurity by continuously validating every stage of a digital transaction. MFA supports Zero Trust by treating 100% of digital traffic as hostile, including employees. It’s the first defense against costly data breaches and other cyber-crimes.

● STAYING ON TARGET

Focus on your unique MFA goals

Your ultimate goals will impact integration and technology decisions on the path to building your access control infrastructure.



Efficient
Protocols



Compliance



Security

Because employees may be asked to continually update passwords every one to three months, time and money are saved when you eliminate reliance on passwords. In fact, **50%** of IT service desk issues involve password resets, with each reset costing **\$70** on average.⁴

In addition, passwordless technologies save time and effort during each workday and every shift. No more repetitive password entries or forgotten PINs mean more efficient workflows, higher productivity and less employee frustration.

Government-backed cybersecurity mandates are already in place that require companies to comply with strict data security rules. In fact, MFA is the new compliance standard, allowing organizations to adhere to an array of emerging global regulations including:

- HIPPA • GDPR
- EPCS • CJIS
- Executive Order 14028
- CCPA • PIPEDA
- LGDP • POPIA

According to one study, cybercrime will cost the world **\$10.5 trillion** annually by 2025.⁵ By eliminating hackable passwords and vulnerable PINs, MFA adds an extra layer of security to avoid data breaches.

No matter the size of your enterprise, establishing a ‘Zero Trust Architecture’ reinforces the systems that protect your digital infrastructure and data, making your organization a tougher target for hackers and other cybercriminals.

³ <https://www.oryxalign.com/blog/the-5-myths-of-multi-factor-authentication/>

⁴ www.infosecurity-magazine.com/webinars/password-management-getting

⁵ <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

Analyze your deployment decisions

There are many factors that contribute to a successful MFA integration. This checklist can help you make the evaluations necessary for an efficient MFA deployment:

UNDERSTANDING

- Have you conducted a comprehensive security audit?
- Do you know which/how many regulations will impact your MFA deployment?*
- Do you currently leverage credentials for physical access control?
- What credential types will you deploy?
- Who are your users? What do their workflows look like? Do they work onsite or offsite?
- How many users will you support?

ASSESSMENT

- Where do you require logical access control for your organization? Workstations, printers, kiosks, equipment?
- Do you manage guest access or event attendees?

*If you do business globally, it is critical to understand offshore regulations that still apply to your data.

- Do you have manufacturing floors to protect?
- What data will be protected? Will it require multi-factor or even more privileged access levels of protection?
- Do your users currently use passwords and/or pins as the primary means to access critical systems or equipment?

EVALUATION

- What SSO/IAM software do you use? Do you require a recommendation on software partner?
- What is your deployment timeline?
- What is your deployment budget?
- Who will spearhead the organization's MFA integration day to day?
- Who has technical oversight? Financial/operational oversight?
- Post-deployment, what level of technical support will you require?

What makes MFA effective?

Multi-factor authentication methods are proven to be more secure than outdated passwords, outdated passwords or PINs. As a reminder, MFA consists of three key factors:

1. **Knowledge**—This is “something you know.” Traditionally, this means a password or PIN. Alone, these methods are susceptible to hacking and relatively simple data breach potential.
2. **Possession**—This is “something you have” such as a proximity or smart-card credential, smartphone, or hardware token. Authentication factors in your physical possession are more secure than passwords because permissions to these cards can be immediately revoked if lost or stolen.
3. **Inherence**—This is “something you are,” including fingerprints or voice recognition that uniquely identify you. Rf IDEAS supports both technologies.

True multi-factor authentication requires users to present at least two of these three factor types to promote a higher level of workplace protection and data security.

● SELECTING THE TECHNOLOGIES

Consider solutions

RFID authentication is cost-effective and offers straightforward configuration.

rf IDEAS® and our partners can offer built-in tools to identify credential types and configure the technology at the touch of a button. And we can work with you to determine which MFA technology will best meet your security needs.



Passwordless

FIDO2 is a passwordless authentication platform that delivers seamless, secure authentication across credential types, devices and browsers. The WAVE ID® platform is fully compatible with FIDO2.



Mobile

Bluetooth® Low Energy technology and NFC compatibility enable smartphones to provide flexible authentication for reliable WAVE ID® mobile performance.



Secure

WAVE ID® Bio offers mobile, biometric and card-based authentication capabilities in a single reader for the simplest route to three layers of secure MFA implementation.

● WORKING TOGETHER

Consult and collaborate

Successful MFA integration is always a team effort. Your rf IDEAS® sales and technical teams have the solutions and expert insights you'll need to ensure a smooth, productive process.

An online support center and helpful knowledge tools—from product manuals to software downloads—are also available as your deployment unfolds and you require support.

rf IDEAS works with an extensive partner network to meet the specialized authentication and identity management needs of any business, in any industry. Software partners that offer native integration with WAVE ID® readers include: AccessSmart, AuthX, Envoy Data, Identity Automation, Imprivata One Sign, NetIQ, and others.

To learn more about how to integrate our readers with your existing software, contact us:

<https://www.rfideas.com/solutions/multi-factor-authentication>





Get started on MFA, your way. Contact rf IDEAS® for the right technologies and unsurpassed consultative support you would expect from the team that's been leading the industry for more than 25 years.

rf IDEAS Global Headquarters
425 N Martingale Rd, Suite 1680
Schaumburg, IL 60173

Call: 1-866-492-8231
Email: sales@rfIDEAS.com
Visit: rfIDEAS.com