Identity Credential and Access Management (ICAM) with Phishing Resistant Multi-Factor Authentication (MFA): Strengthening Security for the Modern Enterprise

Introduction

In the current era of digital transformation, protecting our data and systems is paramount. At the FDA traditional username and password credentials are no longer sufficient to protect our high value assets from cyberattacks. This paper explores why implementing an enterprise Identity Credential and Access Management (ICAM) with Multi-Factor Authentication (MFA) is important. We will examine the benefits of ICAM with MFA, especially phishing resistant MFA, and address the growing security threats and the positive impact on our business operations.

The Threat Landscape

According to Verizon's Data Breach Investigations Report (DBIR), 86% of stolen and/or weak passwords contributed to data breaches. Most of these threat actors are externally facing, and these credential incidents are associated with both financial and espionage motives. As these Cyberattacks are becoming increasingly sophisticated, with malicious actors, the FDA will need to constantly devise new defense methods to prevent breaches. Data breaches, ransomware attacks, and account takeovers are just a few examples of the threats that plague Agencies today. These attacks can have devastating consequences, leading to financial losses, reputational damage, regulatory non-compliance, and threatening the FDA's public health mission.

Why Username and Passwords Aren't Enough

For many years, usernames and passwords have served their purpose at the FDA as the primary line of defense for user authentication. However, these credentials are vulnerable to various attacks, such as phishing, brute-force attacks, and credential stuffing. Threat actors can steal or guess passwords, granting them unauthorized access to our systems. Furthermore, Federal Mandate OMB M-22-09 states, "Agencies are encouraged to pursue greater use of passwordless multifactor authentication." Passwordless access offers a stronger security and an enhanced user convenience by leveraging MFA with SSO.

What is Multi-Factor Authentication (MFA)?

MFA is an authentication method that requires two or more authentication factors for successful authentication. The three authentication factors are:

- Something you Know

- Something you Have
- Something you Are

MFA adds an extra layer of security to the authentication process by requiring users to provide more than just a username and password. Here's how ICAM with MFA strengthens our security posture:

- **Stronger Authentication:** MFA adds an extra layer of security by requiring users to provide a second factor, such as a security token, fingerprint scan, or one-time passcode (OTP) received via SMS, email, or a dedicated app. This significantly reduces the risk of unauthorized access even if a password is compromised.
- **Reduced Risk of Human Error:** Automating user provisioning and deprovisioning through ICAM minimizes the chances of human error associated with manual processes, further bolstering our security posture.
- **Compliance with Regulations:** Many regulations mandate strong authentication practices. ICAM with MFA helps us comply with these regulations and avoid potential penalties.

Benefits of Phishing Resistant MFA

Phishing resistant MFA is immune from attempts to compromise or subvert the authentication process through Identity-based Cyberattacks such as social engineering or phishing. The FDA Enterprise ICAM solution for phishing resistant MFA is currently Nok Nok. Beyond the critical security benefits, implementing ICAM with Phishing Resistant MFA offers several advantages for our business operations:

- Improved User Experience
- Simplified IT Administration
- Aligned Zero Trust Principles
- Federal Mandate Compliance (OMB M-22-09)

Investing in ICAM with Phishing Resistant MFA to a Secure Future

ICAM with phishing resistant MFA is a crucial investment for any enterprise looking to safeguard its sensitive data and systems. By adding an extra layer of security to the authentication process (Phishing Resistant MFA), we can significantly reduce the risk of cyberattacks and protect our valuable assets and comply with the federally mandated guidelines.

Furthermore, the streamlined user experience and efficient administration contribute to an overall positive impact on our business operations. In today's digital world, prioritizing security is not just an option; it's a necessity. Implementing ICAM with phishing resistant MFA is a proactive step towards a more secure and sustainable future for our organization.