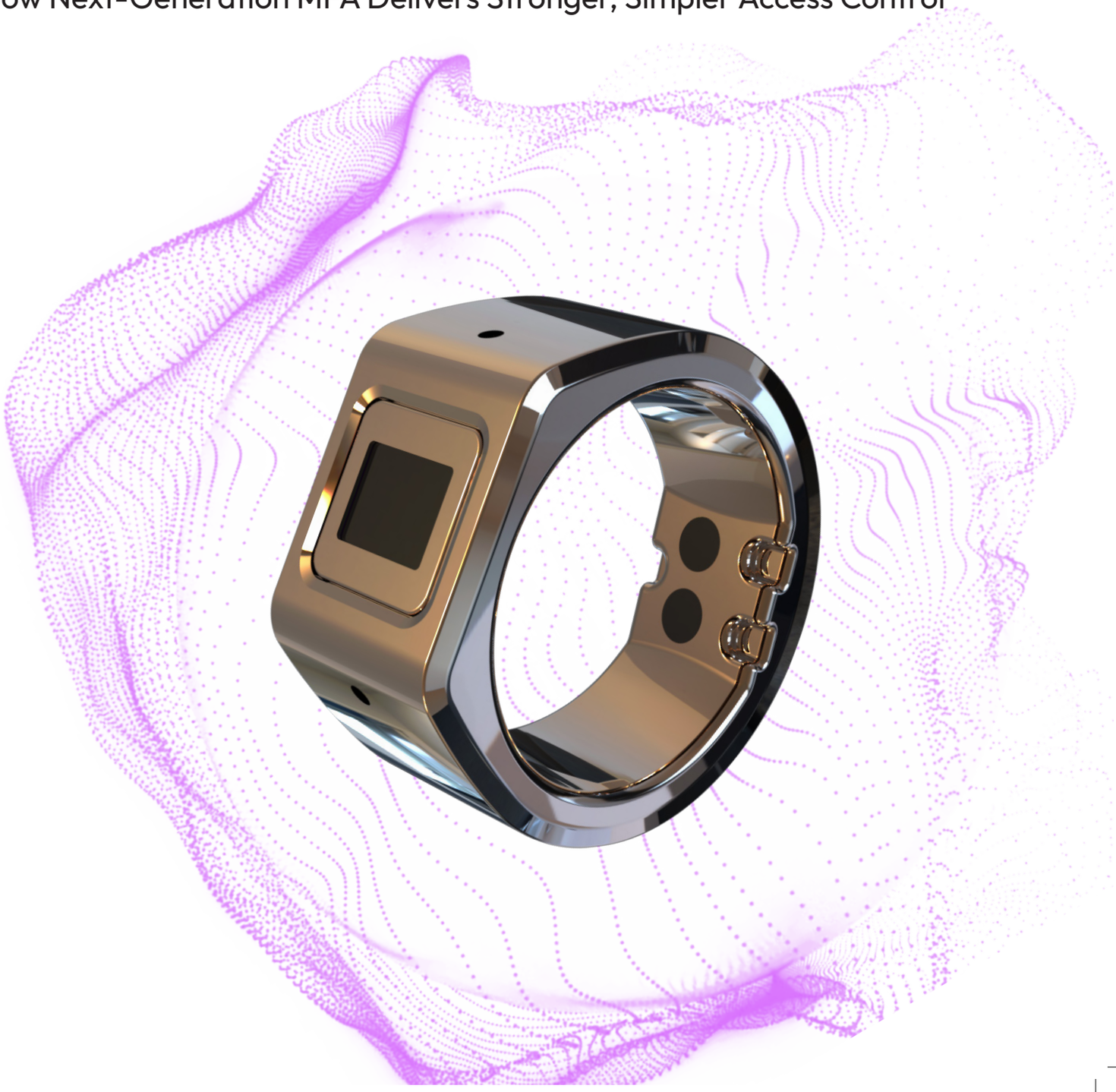
Token

iSMG
INFORMATION SECURITY
MEDIA GROUP

Secure Your Data With Phishing-Resistant MFA

How Next-Generation MFA Delivers Stronger, Simpler Access Control



Introduction

As sophisticated and state-sponsored cybercriminals devise increasingly shrewd and effective intrusion techniques, attacks rise unabated. In particular, organizational leaders are concerned about the relentless proliferation of phishing scams, ransomware and social engineering.

Among cybersecurity professionals, multifactor authentication is widely understood to be the most effective way to defend enterprise systems, applications and data. MFA, which includes two-factor authentication or 2FA, uses at least two factors – such as something the user has, knows or is – to validate a user's identity. The goal is to stop attackers logging into a network as a trusted user and then gaining access to valuable digital assets, applications and data. It's not surprising that 83% of organizations say they are currently enforcing MFA.[1]

What is eye-opening is that technically adept and persistent threat actors have found ways to bypass MFA and other authentication methods. Consider that 89% of organizations experienced a phishing attack in 2022[2] and 28% were hit by ransomware.[3]

Given widespread adoption of MFA, many victims believed they had implemented adequate security capabilities to defend against attacks. And many did. But the truth is: MFA is essentially broken. Don't believe it? Let's take a look at the rise and consequences of ransomware incidents last year. According to IBM's 2022 Cost of a Data Breach report,

11% of all global breaches were attributed to ransomware attacks, a 41% jump over the prior year.[4] The repercussions are significant: This type of malware cost businesses an average total of $4.54 million in 2022.[5] Ransomware breaches are also difficult to identify and contain. On average, it took victims 326 days to find and contain ransomware attacks, giving intruders ample time to move laterally through an organization's systems, causing serious financial and reputational harm.[6]

Source[1]: Watchguard State Password Security
Source[2]: Watchguard State Password Security
Source[3]: IBM Security

Source[4]: IBM Security
Source[5]: IBM Security
Source[6]: IBM Security

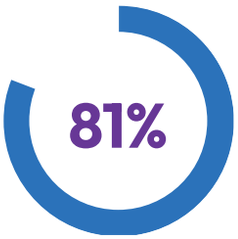
MFA Breaches: By The Numbers

of businesses use MFA

Source: Watchguard

Rise in MFA fatigue attacks in the first nine months of 2022

Source: Microsoft Office Today



of breaches caused by stolen or weak passwords

Source: Verizon DBIR 2022

of businesses experienced a phishing attack in the last year

Source: Watchguard

Increase in ransomware attacks in the past year

Source: IBM Data Breach Report

The damages wrought by ransomware can be devastating to all organizations. Potential consequences include huge ransomware payments, loss of revenue, reputational damage, theft of source code and IP, decreased employee productivity, loss of customers, operational downtime, mitigation costs and public relations nightmares, to name a few.

Increasingly, cyberattacks are not being prevented using current MFA tools. Because hackers are finding ways around MFA, there's a need for a truly secure MFA solution, especially for high-level users, such as C-suite executives and others with access to highly sensitive information.

MFA Failure: How it Happens

The rise in cybersecurity incidents underscores the fact that legacy MFA solutions are vulnerable and not foolproof. It's a complex, multifaceted technology that can be difficult to implement and maintain. Other potential downsides include:

- There is technical complexity and costly implementation.
- A shortage of skilled cybersecurity pros slows deployment.
- Fobs, hardware keys and other physical devices can be lost or stolen.
- Physical MFA devices are seldom tied to higher levels of security, such as biometrics.
- Employees are often reluctant to perform multiple steps to log into corporate systems.
- Users can be locked out of their accounts.
- MFA solutions may not be compatible with all business applications.

Spotting Real-World MFA Failures

Increasingly, today's MFA technologies are being hacked, and even organizations with mature cybersecurity programs are not immune. Over the past year, a new category of attack rose to the forefront – MFA fatigue. Threat actors blast a barrage of authentication requests to users until the users finally fold and hand over MFA approval requests or user credentials. MFA fatigue attacks are estimated to have started in 2020 and have resulted in a rash of MFA failures in 2022, including the following:

Even identity management providers aren't immune. In January 2022, the hacking group Lapsus$ infiltrated the laptop of a third-party provider to Okta, an identity and access management provider. Lapsus$ did so via an overnight blitzkrieg of MFA approval requests to the contractor. The sleep-deprived victim eventually approved the MFA request, which allowed Lapsus$ to gain privileged access to Okta systems for at least five days. Lapsus$ subsequently posted screenshots purporting to depict Okta internal systems. Okta[7] officials reported significant brand/reputational damages and estimated that more than 350 of the company's customers had been affected.

Credentials in a browser led to MFA failure. In May 2022, networking company Cisco[8] fell victim to an MFA failure. Attackers used stolen credentials to take control of an employee's personal Google account and then lift their Cisco system credentials stored in the user's Chrome browser. Next, hackers launched a voice-phishing campaign in which they impersonated trusted sources who encouraged the employee to accept MFA push notifications. The employee eventually did, granting hackers free reign to multiple internal systems and the ability to implant malware, compromise servers, obtain privileged access and pilfer data.

Attackers message a messenger. In August 2022, the Twilio[9] messaging service fell victim to a sophisticated social engineering attack that compromised its MFA service. Using information obtained through phishing attacks against Twilio employees, adversaries convinced several users to share credentials and MFA authorizations. Once inside the system, more than 100 Twilio customers were breached, including Okta and Signal.

Hackers in the driver's seat. In September 2022, a threat actor gained access to an Uber[10] contractor's password and repeatedly attempted to log into the worker's corporate Uber account. That triggered a torrent of two-factor login requests. The contractor eventually accepted an MFA login request, allowing cybercriminals to infiltrate Uber's system. The attackers then accessed other employee accounts to gain permissions to a number of essential tools, forcing the ride-sharing and food-delivery company to disconnect communications and other systems.

Source[7]: Okta
Source[8]: Talos Intelligence
Source[9]: Tech Crunch
Source[10]: Uber

How to Prevent MFA Failures

Imagine a biometric authentication device that fuses the highest level of protection against phishing and ransomware with ease of a device that's always with you. That's Token's smart ring, the next generation of MFA solutions.

The award-winning Token biometric authentication ring is like no other authentication method. It combines biometric user verification, public-private key cryptography, secure hardware and decentralized credential deployment in a convenient, wearable device that creates phish-resistant MFA. It's the only authentication device that completely shields user credentials from hacking, prevents theft of biometric information and expedites user logins. This next-generation MFA solution easily integrates with IAM systems to provide easy-to-use protection with minimal implementation effort and zero user friction.

Here's how the smart ring works: Individual users register the device with their systems accounts using a built-in fingerprint scanner. The individual's authentication and biometric fingerprint data is stored on the ring, rather than a mobile device or server, to safeguard it from hackers. The ring functions only when it detects the registered user's paired fingerprint. Remove the ring and it automatically locks to block unauthorized access.

At the core of a Token authentication ring is the FIDO2 authentication protocol, which reduces password use and strengthens authentication standards.

FIDO2 biometric MFA specifications comprise the W3C's Web Authentication protocol and the FIDO Alliance's Client-to-Authenticator Protocol. **Combined, these protocols create a next-generation MFA authentication capability that strengthens and simplifies MFA.**

In addition, the Token biometric authentication smart ring uses near-field communications to secure the wireless exchange of data. NFC transmits over a very short distance of approximately 4 inches, which makes it all but impossible for threat actors to intercept the transmission of data and carry out man-in-the-middle attacks. NFC is more secure because you must be close to it, and you also must enable the NFC communication with a gesture. It's not "always on," as is common in other MFA solutions. In addition, the ring isn't connected to a network, so hackers can never compromise the ring.

It's the only authentication device that completely shields user credentials from hacking, prevents theft of biometric information and expedites user logins.

Token

Next-Generation MFA

Wearable MFA with Token Ring offers the ultimate protection for access control. Token Ring is a next-generation biometric wearable device that delivers strong MFA to protect organizations from any cyberattacks that rely on defeating access controls, such as phishing or OTP over SMS. Unlike traditional MFA, it's impossible for attackers to bypass Token Ring with malware, MFA fatigue attacks, adversary-in-the-middle attacks and other attacks.

The device will respond only to authorized users, so no one else can use or compromise it. Token Ring's biometric authentication eliminates vulnerabilities inherent in outdated authentication methods. It also provides enhanced protection against today's biggest threats, including account takeover attempts, phishing, credential stuffing, MITM attacks, ransomware and data breaches.

Token

Next-Generation MFA for Your Most Targeted Users

The Token biometric authentication smart ring provides the strongest level of security for top executives, finance and human resources personnel, and systems administrators. These are the users whose access requires greater protection to safeguard financial assets, intellectual property and sensitive or personal information that is subject to regulation. A technically advanced device with zero friction is appreciated by CIOs, CISOs and CFOs, who need fast, frictionless access to sensitive corporate information and resources.

Token provides a hardware-as-a-service pricing model, at a cost that provides incredible ROI many times better than other MFA solutions that provide a fraction of the security protection organizations need today. Organizations that have suffered the multimillion-dollar consequences of a ransomware attack understand the value that FIDO2 biometric MFA can bring. They also recognize that lower-priced MFA alternatives are worthless if the technology can be hacked and is not hack-proof.

Achieving Next-Generation MFA Protection

Deploying effective MFA requires innovative technology that goes beyond current solutions to ensure the highest level of protection. Token can assist you with an Access Control Audit. Here are the key factors to consider to successfully deploy MFA:

- Analyze the ability of your current MFA tools to be compromised.
- Understand which systems, applications and resources require the absolute highest-level of MFA protection.
- Implement advanced FIDO2 biometric MFA across applicable systems, applications and resources, starting with access to your organization's network.
- Educate employees and executives on the protective value of advanced MFA.
- Provide ongoing training on the need for MFA protection, along with emerging ransomware and phishing scams.
- Perform a pilot testing program using privileged users and admin accounts.
- Consider adding passwordless access.
- Expand MFA capabilities through single sign-on, and identity federation services.