WINMAGIC®

Beyond MFA: Bringing Zero Trust to User Authentication

Sophisticated Attacks Demand More Sophisticated Authentication

For years, traditional forms of multi-factor authentication (MFA) have been considered the preferred means of verifying the identity and access privileges of a user on an endpoint device. However, as the use of remote access has greatly expanded and cybercriminals have become increasingly sophisticated, that is no longer the case.

Attacks in recent years have shown that sophisticated hackers can defeat what most of the world believes is most secure. Simply put, "good" is not good enough if the adversary is knowledgeable and willing to put in the work.

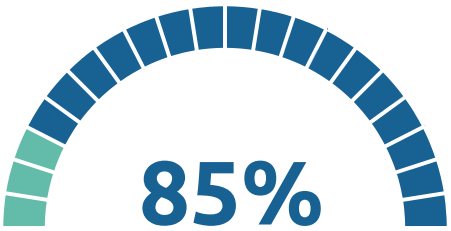
Top government cybersecurity experts understand this and have alerted the world accordingly. In May of 2021, the White House issued an executive order aimed at improving cybersecurity in the United States. The order pointed out the deficiencies of MFA and recommended that organizations implement a zero-trust approach to their security strategies. This white paper explores the shortcomings of traditional MFA and how a new approach can make zero-trust authentication not only stronger but easier to implement and use.

Hackers Are Getting More Sophisticated

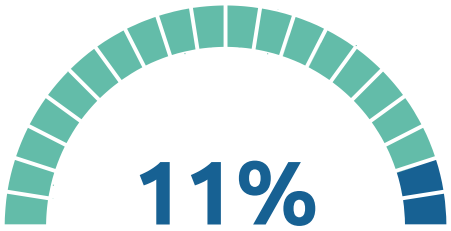
To understand why it is no longer enough to rely on traditional MFA, one needs to look no further than recent breaches by bad actors Cozy Bear (perpetrators of the SolarWinds hack) and Lapsus$. These hacking gangs have successfully used techniques, including "MFA prompt bombing," to compromise scores of companies, including Microsoft, Okta, Nvidia, Cisco, and Intel, as well as several federal agencies, including Treasury, Justice, Energy, and the Pentagon.[1]

MFA prompt bombing is a form of push attack in which the hacker tries to get users to accept phony authentication attempts by bombarding them with prompts. These attacks succeed when a user – often fatigued by the flurry of prompts received on their phone's authenticator app – presses "Approve" by mistake.

Both Cozy Bear and Lapsus$ attacks took advantage of MFA vulnerabilities. The impact of the SolarWinds hack was damaging and costly. A 2021 survey of leading US, UK, and Singapore companies conducted by research firm Sapio[2] revealed that:



85% of companies surveyed were impacted by the SolarWinds attack (31% significantly)



The SolarWinds attack cost companies an average of 11% of their annual revenue

The Cozy Bear and Lapsus$ breaches demonstrate that MFA is not an insurmountable barrier and that hackers will likely employ the same attack vectors in the future, and when they do, it will be costly.

[1]https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/
[2]https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf

The US Government Has Responded

The growth in increasingly sophisticated cyberattacks prompted the US Government in 2021 to release its Federal Zero Trust Strategy in support of Executive Order 14028, Improving the Nation's Cybersecurity. Its zero-trust strategy requires government employees and contractors to discontinue the use of MFA solutions that employ SMS text, one-time passwords (OTP), and push notifications, declaring these MFA methods are not phishing-resistant.[3]

Instead, they are mandated to use phishing-resistant MFA throughout their enterprise and give users the option of using phishing-resistant authentication before the end of January 2023. Private sector organizations would be wise to do the same.

[3] *https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf*

What Is Zero Trust?

Zero trust is an approach to cybersecurity management based on the assumption that no endpoint device or user can be implicitly trusted to access a system. Here's how the executive order describes it:

The term "Zero Trust Architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.[4]

What's needed, then, is an authentication method that fully supports the zero-trust security model, eliminating trust in any one element and providing continuous verification. Traditional MFA is not it.

[4]*https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*

What's Wrong with Traditional MFA?

As noted above, traditional MFA is not phishing-resistant. One reason is that many traditional MFA solutions are smartphone-based. They bring the smartphone into the equation to verify the user because the user cannot be directly verified by the server.

What's wrong with using a smartphone for authentication? Take "SIM swap" attacks, for example. This occurs when an attacker uses a variety of nefarious means to convince a mobile service provider to assign a user's phone number to a Subscriber Identity Module (SIM) that the attacker owns. Once the SIM has been swapped, the attacker can log in, receive the SMS OTP, enter it, and gain access. For this and other reasons, the National Institute of Standards and Technology (NIST) has restricted the use of SMS as a second authentication factor.

The issue is that using an out-of-band smartphone introduces a new vulnerability: the association between the authentication device and the endpoint. This requires the user to establish the association between the authentication device and the endpoint through a means (such as SMS text) that is not phishing-resistant. And since 87% of all breaches are the result of human error, any solution that relies on humans to take action is inherently vulnerable.

A New Way of Thinking

The notion that MFA is required for secure remote authentication comes from the obsolete idea that the remote server (the service provider SP) should authenticate the user, e.g., the entity that receives the services. As we've noted, this puts the onus on the user to take an action. That action is typically mobile device-based – typing in a passcode received via SMS text, responding to a push notification, or entering an OTP. None of these methods is phishing-resistant.

A more effective and user-friendly approach is to make authentication a two-step process:

Step 01

The user authenticates to the endpoint.

Step 02

The endpoint authenticates to the server using public key-based encryption on behalf of the user and device, with no user action required.

There are several advantages to this approach:

It takes advantage of the existing Trusted Platform Module (TPM) crypto chip within the endpoint to provide unbreakable public key-based authentication magnitudes stronger than anything the user can do.

It takes any user action, such as entering an OTP or pressing “accept” on a mobile authenticator app, completely out of the equation.

It supports zero trust because the endpoint can perform continuous verification.

It requires no additional authentication devices.

It ensures a better, more seamless user experience.

It makes IT management easier.

It reduces IT total cost of ownership.

Can the endpoint authenticate or verify the user reliably? Yes. That's what endpoints have always done since they came into existence, such as when millions of users log in to Windows every day. And after all, shouldn't the endpoint be in a better position to verify the user in front of it versus a remote server?

Furthermore, the endpoint can verify not only the user's presence but also the user's intent to access the service. This is unlike out-of-band methods, such as push authentication, in which the user is relied upon to explicitly make the association of intent. Local gestures, such as pressing a button or even submitting to a facial recognition scan, don't communicate the user's exact intention to the remote server.

It's worth mentioning that using the endpoint for re-authentication is nothing new. Most websites and enterprise solutions already re-authenticate using some form of cookies on the endpoint. However, as the SolarWinds MFA bypass attack showed, cookies are vulnerable and not secure enough against sophisticated hackers. A TPM-equipped endpoint can authenticate and re-authenticate better than passive cookies.

The Value of Cryptography

Online, everything is data – from the voice you hear to the webcam video you watch. All of that data can be manipulated, even in real time. The best technology to protect that data and support zero trust is cryptography. That's because only cryptography can guarantee data integrity, confidentiality, authenticity and non-repudiation.

Cryptography is well-suited to defense. Generating a new encryption key to either protect data or authenticate a device or user can be done easily in a matter of milliseconds. Conversely, finding and attacking a key takes infinitely longer; it would require hundreds of years of effort using all the computers on Earth. For this reason, the best defense for online data is to use cryptography to prevent attacks.

The Solution: MagicEndpoint

A solution is now available that exemplifies this new way of thinking, avoiding the limitations of traditional MFA and fully supporting zero trust. It's called MagicEndpoint from WinMagic. MagicEndpoint is the passwordless authentication solution that protects remote access by leveraging the endpoint to do the work, requiring no user action and no extra devices. It's seamless, phishing-resistant, and virtually invisible to the user.

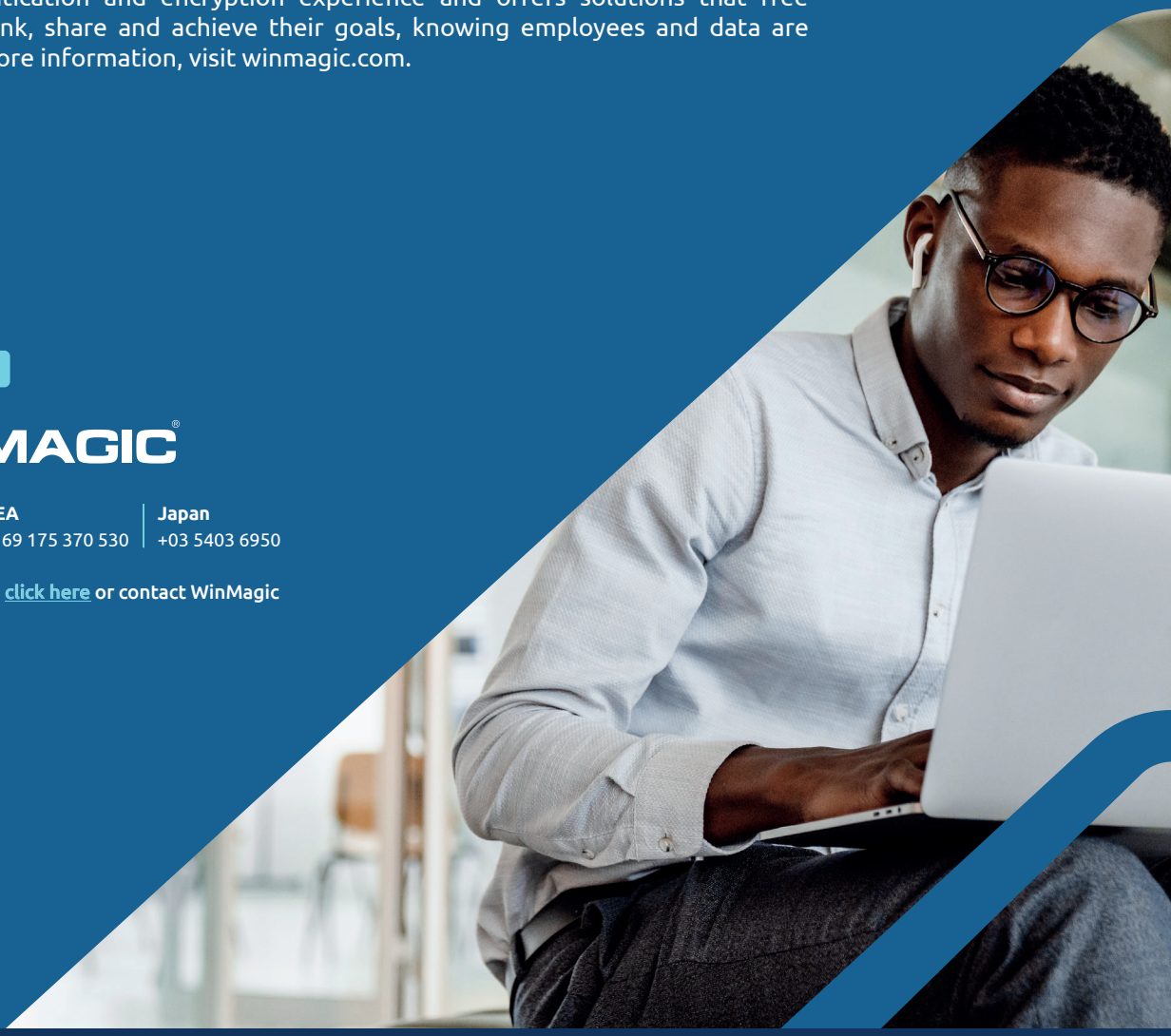
To learn more about how MagicEndpoint can take you beyond MFA and bring zero trust to user authentication, visit **winmagic.com** or contact us **here**.

WinMagic

Authenticate. Encrypt. Achieve.

Contact WinMagic to Learn More

WinMagic is a leading developer of cybersecurity solutions that, over the course of 20 years, has raised the bar for endpoint encryption. As a result of extensive experience with securing the endpoint – and a commitment to continuous innovation – WinMagic is trusted by over 2,500 businesses and government agencies around the world and has over 3 million active licenses globally. WinMagic's authentication and encryption suite of products protects data within any laptop, physical or virtualized data center, on-premise or in the cloud. The company's solutions are platform-independent, able to secure data on devices using Windows, Linux, and Mac systems. WinMagic has earned wide recognition for protecting against threats and data loss while helping businesses meet privacy and regulatory compliance requirements. WinMagic delivers a secure, seamless authentication and encryption experience and offers solutions that free customers to think, share and achieve their goals, knowing employees and data are protected. For more information, visit winmagic.com.



WINMAGIC

US & Canada +1 888 879 5879 | **EMEA** +49 69 175 370 530 | **Japan** +03 5403 6950

For more information, click here or contact WinMagic