Next-Generation Authentication Security in the AI Era

The Role of Biometric-Based MFA in Enterprise Cyber Defense

White Paper 2026
UNION biometrics Co., Ltd.

union biometrics

Contents

Executive Summary

Generative AI is changing the speed and scale of cyberattacks. Rather than creating entirely new hacking methods, AI enables attackers to identify existing security gaps faster and exploit them at a larger scale. Anthropic notes that AI models are becoming more capable of identifying software vulnerabilities and assessing exploitability, making defensive use of AI increasingly important (Anthropic, n.d.).

This shift shows why enterprise security must move beyond network-device protection and focus more on authentication. In AWS's FortiGate case, the attacker did not use a new FortiGate vulnerability. Instead, the campaign exploited exposed management ports, weak credentials, and single-factor authentication (Moses, 2026). Mandiant also identifies stolen credentials and infostealer malware as key factors in recent enterprise intrusions (Mandiant, 2025, pp. 9, 47–48).

In the AI era, firewalls and security appliances alone are not enough. Organizations must verify who is accessing their systems. Microsoft states that MFA blocks more than 99% of unauthorized access attempts and that phishing-resistant MFA provides stronger protection (Microsoft Threat Intelligence, 2025, p. 8).

01 Background: How AI Is Changing Cyberattacks

Generative AI increases attackers' ability to find targets, analyze vulnerabilities, generate scripts, and repeat attack processes quickly. Microsoft reports that attackers are using AI for automated vulnerability discovery, phishing, malware or deepfake generation, data analysis, and more convincing fraud messages (Microsoft Threat Intelligence, 2025, p. 8).

The main issue is scalability. Large-scale attacks once required advanced skills, time, and manpower. AI lowers those barriers and helps attackers find weak targets faster.
Therefore, AI-driven threats should be understood as the acceleration of existing security problems, such as weak passwords, exposed management pages, single-factor authentication, and poor account management.

AI is Expanding the Scale of Cyberattacks – Strong Authentication is the First Defense ”

02 Key Risk: Existing Security Gaps and Authentication Weaknesses Become Major Attack Surfaces

AI-driven attacks are dangerous because they can turn basic security gaps into large-scale incidents. In the FortiGate case, AWS reported that the attacker used commercial generative AI services to compromise more than 600 devices across more than 55 countries. The attack relied on exposed management ports, weak credentials, and single-factor authentication, not a new FortiGate vulnerability (Moses, 2026).

Authentication is now a primary security risk. If attackers obtain valid credentials, their access may appear legitimate.
Mandiant found that stolen credentials accounted for 16% of initial infection vectors in 2024, and that infostealer malware can collect account and browser data used for enterprise compromise (Mandiant, 2025, pp. 9, 47–48).

This risk is also clear in cloud environments. Mandiant reported that email phishing accounted for 39% and stolen credentials for 35% of initial infection vectors in 2024 cloud intrusions (Mandiant, 2025, p. 33). Recent Korean media reports indicate that growing concerns over AI-driven cyberattacks are prompting enterprises to move beyond traditional network defense and place greater emphasis on stronger authentication systems (Park, 2026).

03 Limitation: ID/Password and Traditional MFA Are Not Sufficient

ID/password-based authentication is not sufficient in an AI-driven threat environment. Passwords can be leaked, reused, phished, or collected through infostealer malware. Once attackers obtain valid credentials, they can attempt to log in as legitimate users.

MFA remains essential. Microsoft states that MFA blocks more than 99% of unauthorized access attempts, even when attackers have valid usernames and passwords (Microsoft Threat Intelligence, 2025, pp. 8, 22).

However, not all MFA methods offer the same protection. SMS OTP, email OTP, and simple push approvals can still be exposed to phishing, session theft, user mistakes, and push fatigue. Microsoft emphasizes that phishing-resistant MFA provides stronger protection (Microsoft Threat Intelligence, 2025, p. 8).

04 Solution: Biometric-Based MFA

Biometric-based MFA strengthens authentication by using factors such as face, fingerprint, or iris recognition. Even if a password is stolen, attackers cannot easily complete access without passing the biometric factor.

Edaily reported that authentication models combining biometrics, device-based authentication, MFA, and public key-based structures are gaining attention as a next-generation security direction (Park, 2026). This means biometrics are most effective when used as part of a broader MFA architecture.

Biometric-based MFA can reduce credential-based access, account sharing, proxy login, and automated login attempts. It is especially useful for administrator accounts, VPN access, cloud consoles, internal systems, and access-control management portals.

05 Implementation Strategy

Organizations should modernize authentication in phases, starting with the highest-risk accounts and access points.

1. Identify High-Risk Account

Prioritize administrator accounts, VPN accounts, remote access accounts, cloud console accounts, access-control administrator accounts, and security appliance management accounts.

2. Remove Single-Factor Authentication

Systems accessible only with ID/password should be reviewed first. AWS's FortiGate case shows that weak credentials and single-factor authentication can enable large-scale compromise (Moses, 2026).

3. Apply MFA to Administrator and VPN Accounts

Administrator and VPN accounts are major entry points into internal systems. MFA should be applied to these accounts first (Microsoft Threat Intelligence, 2025, p. 8; Mandiant, 2025, p. 9).

4. Expand Biometric-Based MFA

Biometrics should be combined with device-based authentication, public key-based structures, and additional authentication factors to reduce reliance on passwords (Park, 2026).

5. Strengthen Phishing-Resistant MFA

Organizations should move beyond SMS, email OTP, and simple push approval. Microsoft highlights phishing-resistant MFA, and Mandiant recommends AiTM-resistant MFA to reduce infostealer-related risks (Microsoft Threat Intelligence, 2025, p. 8; Mandiant, 2025, p. 49).

6. Monitor Authentication Logs

Stolen-credential attacks may look like normal logins. Organizations should monitor login behavior, access location, device information, privilege escalation, and VPN access history (Mandiant, 2025, pp. 48–49).

06 Expected Benefits

Biometric-based MFA can help enterprises achieve:

- Stronger protection against credential-based attacks
- Better protection for administrator accounts
- Reduced account sharing and proxy login risks
- Improved user convenience
- Better resilience against AI-driven automated attacks
- A shift toward authentication-centered security

07 Conclusion

Cybersecurity in the AI era is no longer only about protecting network devices. AI helps attackers find existing weaknesses faster and exploit them at scale. AWS's FortiGate case shows that exposed management ports, weak credentials, and single-factor authentication can be abused without relying on a new vulnerability (Moses, 2026).

Mandiant also identifies stolen credentials and infostealer malware as important factors in enterprise compromise (Mandiant, 2025, pp. 47–48). This means enterprise security must move from perimeter-focused defense toward stronger authentication and access control.

Biometric-based MFA helps prevent stolen passwords from being enough to complete access. By combining biometrics, device-based authentication, and phishing-resistant MFA, enterprises can build a stronger authentication model for AI-driven threats.

> In the AI era, cybersecurity cannot rely on network perimeter defense alone. As attackers use AI to exploit stolen credentials and existing security gaps faster and at greater scale, authentication must become the starting point of enterprise security. Biometric-based MFA is a key strategy for preventing account-based attacks and verifying legitimate user access.

08 References

Anthropic. (n.d.). *Project Glasswing: Securing critical software for the AI era*. Retrieved May 14, 2026, from https://www.anthropic.com/glasswing

Mandiant. (2025). *M-Trends 2025 report*. Google Cloud Security. https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

Microsoft Threat Intelligence. (2025). *Microsoft Digital Defense Report 2025: Safeguarding trust in the AI era*. Microsoft. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf

Moses, C. J. (2026, February 20). *AI-augmented threat actor accesses FortiGate devices at scale*. AWS Security Blog. https://aws.amazon.com/ko/blogs/security/ai-augmented-threat-actor-accesses-fortigate-devices-at-scale/

Park, J.-S. (2026, April 21). *"AI 해킹에 생체인증 뜬다"…앤트로픽 '미토스' 충격에 인증체계 재편 필요성 '쑥'* ["Biometric authentication rises amid AI hacking concerns"… Need for authentication system restructuring grows after Anthropic "Mythos" shock]. *Edaily*. https://www.edaily.co.kr/News/Read?newsId=03102886645418416&mediaCodeNo=257&OutLnkChk=Y

2026 UNION biometrics Co., Ltd. All Right Reserved.

Address

12F, Daemyung Valeon bldg.,
127, Beobwon-ro, Songpa-gu,
Seoul, 05836, Republic of Korea

Contact

Email: onlinemarketing
@unionbiometrics.com