AI 기반 사이버 위협에 대응하는 차세대 인증 보안

생체인증 기반 MFA가 기업 보안의 새로운 기준이 되는 이유

White Paper 2026
UNION biometrics Co., Ltd.

union biometrics

목차

Executive Summary: 핵심 요약

생성형 AI는 사이버 공격의 속도와 규모를 빠르게 변화시키고 있다. AI는 공격자가 완전히 새로운 해킹 기술을 만들어내는 데만 활용되는 것이 아니라, 이미 존재하던 보안 취약점과 운영상의 허점을 더 빠르게 찾고 대규모로 악용할 수 있도록 만든다. Anthropic은 Project Glasswing을 통해 AI 모델이 소프트웨어 취약점 탐지와 악용 가능성 분석에서 고도화되고 있으며, 이러한 역량이 방어 목적에 활용되어야 한다고 설명한다 (Anthropic, n.d.).

이러한 변화는 기업 보안의 중심이 네트워크 장비 방어에서 인증 체계 강화로 이동해야 함을 보여준다. AWS의 FortiGate 침해 사례에서는 새로운 취약점이 아니라 외부에 노출된 관리 포트, 약한 자격증명, 단일 인증 구조가 공격에 활용되었다 (Moses, 2026). 또한 Mandiant는 탈취된 자격증명과 infostealer malware가 최근 기업 침해에서 중요한 위협 요인으로 부상하고 있다고 분석했다 (Mandiant, 2025, pp. 9, 47–48).

따라서 AI 시대의 보안 전략은 방화벽이나 보안 장비를 추가하는 것만으로는 충분하지 않다. 기업은 이제 “누가 시스템에 접근하고 있는가”를 정확히 검증하는 인증 중심 보안 체계를 구축해야 한다. Microsoft는 MFA가 무단 접근 시도의 99% 이상을 차단하는 핵심 보안 조치이며, phishing-resistant MFA가 더 높은 보안 수준을 제공한다고 강조한다 (Microsoft Threat Intelligence, 2025, p. 8).

01 Background: AI가 바꾸는 사이버 공격 환경

생성형 AI는 사이버 공격자의 실행 능력을 높이고 있다. 공격자는 AI를 활용해 공격 대상을 찾고, 취약점을 분석하고, 자동화 스크립트를 작성하며, 반복적인 공격 과정을 더 빠르게 수행할 수 있다. Microsoft는 공격자들이 AI를 자동화된 취약점 탐색, 피싱 캠페인, 악성코드 또는 딥페이크 생성, 데이터 분석, 사기 메시지 고도화 등에 활용하고 있다고 분석했다 (Microsoft Threat Intelligence, 2025, p. 8).

이 변화의 핵심은 공격의 "확장성"이다. 과거에는 대규모 공격을 수행하려면 높은 기술력과 상당한 인력이 필요했다.

그러나 AI는 공격 준비와 반복 실행에 드는 비용을 낮추고, 취약한 대상을 더 빠르게 탐색할 수 있도록 만든다.

즉, AI 시대의 사이버 위협은 완전히 새로운 해킹 기술의 등장만을 의미하지 않는다. 더 중요한 변화는 기존에 존재하던 약한 비밀번호, 노출된 관리 페이지, 단일 인증 구조, 미흡한 계정 관리가 AI를 통해 더 빠르게 공격 대상이 될 수 있다는 점이다.

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

02 Key Risk: 기존 보안 허점과 인증 취약점이 주요 공격 표면이 된다

AI 기반 공격의 핵심 위험은 새로운 해킹 기술보다, 기존 보안 허점이 더 빠르고 대규모로 악용될 수 있다는 점이다. AWS의 FortiGate 침해 사례에서 공격자는 여러 상용 생성형 AI 서비스를 활용해 55개국 이상에서 600대 이상의 장비를 침해했다. 이 공격은 새로운 FortiGate 취약점을 이용한 것이 아니라, 외부에 노출된 관리 포트, 약한 자격증명, 단일 인증 구조를 악용한 사례였다 (Moses, 2026).

이러한 흐름은 인증 체계가 기업 보안의 핵심 방어선이 되어야 함을 보여준다. 공격자가 정상 사용자의 계정을 탈취하면 시스템은 이를 합법적인 접근으로 인식할 수 있으며, 이후 내부 시스템 접근, 권한 상승, 데이터 탈취로 공격이 이어질 수 있다. Mandiant는 2024년 침해 조사에서 탈취된 자격증명이 전체 초기 침투 벡터의 16%를 차지했으며, infostealer malware를 통해 수집된 계정 정보와 브라우저 데이터가 기업 침해에 활용될 수 있다고 분석했다 (Mandiant, 2025, pp. 9, 47–48).

클라우드와 원격 접속 환경에서도 인증 리스크는 더욱 커지고 있다. Mandiant는 2024년 클라우드 침해 사례에서 이메일 피싱이 39%, 탈취된 자격증명이 35%의 초기 침투 벡터로 관찰됐다고 밝혔다 (Mandiant, 2025, p. 33). 국내 보도 역시 생성형 AI 기반 공격 우려가 커지면서 기업 보안의 초점이 네트워크 방어에서 인증체계 강화로 이동하고 있다고 설명한다 (박정수, 2026).

03 Limitation: ID/Password와 기존 MFA의 한계

ID와 비밀번호만으로 구성된 Single-Factor Authentication은 AI 기반 공격 환경에서 충분한 보안을 제공하기 어렵다. 비밀번호는 유출될 수 있고, 여러 서비스에서 재사용될 수 있으며, infostealer malware나 피싱을 통해 대량으로 수집될 수 있다. 공격자는 이렇게 확보한 계정 정보를 활용해 정상 사용자처럼 로그인할 수 있다.

Microsoft는 MFA가 무단 접근 시도의 99% 이상을 차단하는 핵심 보안 조치라고 설명한다. 또한 공격자가 유효한 사용자 이름과 비밀번호를 갖고 있더라도, MFA가 적용되어 있으면 99% 이상의 경우 접근을 차단할 수 있다고 강조한다 (Microsoft Threat Intelligence, 2025, pp. 8, 22).

그러나 모든 MFA가 동일한 수준의 보안을 제공하는 것은 아니다. SMS OTP, 이메일 OTP, 단순 푸시 승인 방식은 피싱, 세션 탈취, 사용자 실수, 푸시 피로 공격 등에 노출될 수 있다. Microsoft는 phishing-resistant MFA가 일반적인 MFA보다 더 강력한 보안 수준을 제공한다고 설명한다 (Microsoft Threat Intelligence, 2025, p. 8).

따라서 기업은 MFA를 도입하는 것에서 멈추면 안 된다. 어떤 인증 방식을 적용할 것인지, 해당 인증 방식이 피싱과 계정 탈취에 얼마나 강한지, 실제 사용자를 얼마나 정확히 확인할 수 있는지를 함께 검토해야 한다.

04 Solution: 생체인증 기반 MFA

생체인증 기반 MFA는 얼굴, 지문, 홍채 등 사용자의 고유한 생체 특성을 활용해 인증 강도를 높이는 방식이다. 이 방식은 비밀번호가 탈취되더라도 공격자가 추가 인증을 통과하기 어렵게 만든다. 즉, 생체인증 기반 MFA는 계정 정보 탈취만으로는 접근을 완료할 수 없는 구조를 만든다는 점에서 AI 시대의 계정 기반 공격에 효과적으로 대응할 수 있다.

이데일리는 AI 기반 공격 우려가 커지면서 생체인증, 단말 기반 인증, 다중인증, 공개키 기반 구조를 결합한 인증 체계가 차세대 보안 방향으로 주목받고 있다고 보도했다 (박정수, 2026). 이는 생체인증이 단독 인증 수단으로 사용되는 것보다, MFA 구조 안에서 다른 인증 요소와 결합될 때 더 높은 보안 효과를 낼 수 있음을 의미한다.

생체인증 기반 MFA는 보안성과 편의성을 동시에 높일 수 있다. 사용자는 복잡한 비밀번호나 OTP 코드를 매번 입력하지 않아도 되고, 기업은 계정 공유, 대리 로그인, 자동화 로그인 시도, 탈취 계정 기반 접근을 줄일 수 있다. 특히 관리자 계정, VPN, 클라우드 콘솔, 내부 업무 시스템, 출입통제 관리자 페이지처럼 침해 시 피해가 큰 접근 지점에는 생체인증 기반 MFA를 우선 적용할 필요가 있다.

05 Implementation Strategy: 기업 적용 전략

AI 기반 사이버 위협에 대응하기 위해 기업은 인증 체계를 단계적으로 고도화해야 한다. 모든 시스템에 한 번에 적용하기보다, 침해 시 피해가 큰 계정과 접속 지점부터 우선 강화하는 방식이 효과적이다.

1. 고위험 계정부터 식별한다

기업은 먼저 침해 시 피해가 큰 계정을 분류해야 한다. 관리자 계정, VPN 계정, 원격 접속 계정, 클라우드 콘솔 계정, 출입통제 관리자 계정, 보안 장비 관리 계정 등이 우선 대상이 될 수 있다. 이러한 계정은 공격자가 탈취했을 때 내부 시스템 접근, 권한 상승, 데이터 유출로 이어질 가능성이 높기 때문에 일반 사용자 계정보다 강한 인증 체계가 필요하다.

2. . 단일 인증 구조를 제거한다

ID와 비밀번호만으로 접근 가능한 시스템을 점검하고, 외부 접속과 관리자 접근부터 MFA를 필수화해야 한다. AWS의 FortiGate 사례에서 단일 인증 구조와 약한 자격증명이 공격 성공의 주요 원인으로 확인된 만큼, 고위험 계정부터 단일 인증 구조를 제거해야 한다 (Moses, 2026).

3. 관리자·VPN 계정에 MFA를 우선 적용한다

관리자 계정과 VPN 계정은 외부에서 내부 시스템으로 접근하는 주요 통로가 될 수 있다. 따라서 이 영역에는 MFA를 우선 적용해야 한다. Microsoft는 MFA가 무단 접근 시도의 99% 이상을 차단하는 핵심 보안 조치라고 설명하며, Mandiant 역시 탈취된 자격증명의 위험을 줄이기 위해 MFA 적용이 중요하다고 제시한다 (Microsoft Threat Intelligence, 2025, p. 8; Mandiant, 2025, p. 9).

4. 생체인증 기반 MFA를 단계적으로 확대한다

얼굴, 지문, 홍채 등 생체인증을 단말 기반 인증, 공개키 기반 구조, 추가 인증 요소와 결합해야 한다. 이를 통해 탈취된 비밀번호만으로는 접근을 완료할 수 없도록 하고, 실제 사용자가 접근을 시도하고 있는지 검증할 수 있다. 생체인증과 단말 기반 인증, 다중인증, 공개키 기반 구조의 결합은 차세대 인증체계의 중요한 방향으로 언급되고 있다 (박정수, 2026).

5. phishing-resistant MFA를 강화한다

SMS, 이메일 OTP, 단순 푸시 인증 중심의 MFA에서 벗어나 phishing-resistant MFA를 우선 검토해야 한다. Microsoft는 phishing-resistant MFA가 더 높은 보안 수준을 제공한다고 설명하며, Mandiant도 infostealer 위험 완화를 위해 AiTM-resistant MFA 방식의 활용을 권고한다 (Microsoft Threat Intelligence, 2025, p. 8; Mandiant, 2025, p. 49).

6. 인증 로그 기반 모니터링을 강화한다

탈취 계정을 활용한 공격은 정상 로그인처럼 보일 수 있다. 따라서 로그인 성공 여부만 확인하는 방식으로는 충분하지 않다. 인증 로그, 접속 위치, 단말 정보, 비정상 로그인 패턴, 권한 상승 시도, VPN 접속 이력 등을 지속적으로 분석해야 한다. Mandiant는 infostealer로 탈취된 계정 정보가 장기간 공격자에게 활용될 수 있다고 설명하며, 접근 정책과 MFA, 탐지 체계의 중요성을 강조한다 (Mandiant, 2025, pp. 48–49).

06 Expected Benefits

생체인증 기반 MFA 도입을 통해 기업은 다음과 같은 효과를 기대할 수 있다.

- 계정 탈취 기반 공격 차단력 강화
- 관리자 계정 보호 강화
- 계정 공유 및 대리 로그인 위험 감소
- 사용자 편의성 개선
- AI 기반 자동화 공격 대응력 향상
- 인증 중심 보안 체계 전환

07 Conclusion: 결과

AI 시대의 사이버보안은 더 이상 네트워크 장비를 보호하는 문제만으로 설명할 수 없다. AI는 공격자의 기술적 한계를 낮추고, 기존 취약점을 더 빠르게 탐색하며, 공격을 대규모로 자동화할 수 있게 만든다. AWS의 FortiGate 사례는 새로운 취약점이 아니라 노출된 관리 포트, 약한 자격증명, 단일 인증 구조와 같은 기본적인 보안 허점이 AI에 의해 대규모로 악용될 수 있음을 보여준다 (Moses, 2026).

또한 Mandiant는 infostealer malware와 탈취된 자격증명이 기업 침해의 중요한 원인으로 활용되고 있다고 분석했다 (Mandiant, 2025, pp. 47–48). 이는 기업 보안의 핵심이 네트워크 경계 방어를 넘어 사용자 인증과 접근 통제 강화로 이동해야 함을 의미한다.

결국 AI 기반 사이버 위협에 대응하기 위한 핵심 전략은 인증 구조의 고도화다. 생체인증 기반 MFA는 탈취된 비밀번호만으로는 접근을 완료할 수 없게 만들고, 실제 사용자의 존재와 인증 의도를 함께 확인할 수 있는 강력한 수단이다. 따라서 기업은 비밀번호 중심 보안에서 벗어나 생체인증, 단말 기반 인증, phishing-resistant MFA를 결합한 차세대 인증 보안 체계로 전환해야 한다.

AI 시대의 사이버보안은 네트워크 경계 방어만으로는 충분하지 않다. 공격자가 AI를 활용해 탈취 계정과 기본 보안 허점을 더 빠르고 대규모로 악용하는 환경에서는, “누가 접근하고 있는가”를 정확히 검증하는 인증 체계가 보안의 출발점이 되어야 한다. 생체인증 기반 MFA는 계정 기반 공격을 차단하고 실제 사용자의 접근을 검증하기 위한 핵심적인 차세대 인증 보안 전략이다.

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

Address

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

Contact
Email: onlinemarketing
@unionbiometrics.com