The post-mortem shows the attacker never even saw your MFA prompt.

Not bypassed. Not phished. Never encountered it.

• THE TWIST

They came in on a service account, an API key, a session token that was already minted — **the credentials MFA doesn't touch.**

“We support MFA” stopped being enough in 2023. Here's the gap most vendors are still selling around.

AUTHENTICATION COMES IN TWO SHAPES

SHAPE 1 · THE COMMON ONE

Standing credentials, with MFA.

Password + a TOTP code or push. But the credential itself is *permanent* — it lives in your IdP, in browser sessions, in API keys, in service accounts, in the support engineer's password vault. MFA is a gate at login time, and that's it.

Protects against: someone who has *only* the password.

WHAT MFA-AT-LOGIN DOES NOT STOP

- → Stolen session tokens — the Okta HAR-file playbook, replayed at Cloudflare, 1Password, BeyondTrust
- → AitM phishing kits (EvilProxy, Tycoon, NakedPages) that capture live sessions straight through the MFA prompt
- → API keys that outlive the engineer who created them
- → Service accounts nobody has rotated since 2022
- → A stolen laptop with cached SSO and a logged-in browser

SHAPE 2 · THE ONE THAT MATTERS

Ephemeral, identity-bound credentials.

Issued on demand, bound to a specific piece of hardware (Secure Enclave, YubiKey, TPM), and expired in minutes. **There is no standing credential to steal.** A stolen token is useless five minutes later. A stolen laptop is useless without the hardware key. A compromised API call can't be replayed.

Protects against: every attack on the previous slide — including the AitM kits bypassing MFA in production today.

THE CLEANEST PUBLIC EXAMPLE

Okta, 2023.

Attackers walked off with HAR files containing live session tokens, then logged in to the Okta environments of Cloudflare, 1Password, and BeyondTrust as authenticated users. The MFA prompts had already been answered — by the real user, hours earlier.

Standing sessions made the breach portable.

> Okta support-system breach, Sept–Oct 2023: HAR-file session tokens used to hijack 5 customers' sessions.
>
> Okta root-cause analysis; BeyondTrust, Cloudflare & 1Password disclosures

• TWO QUESTIONS FOR ANY VENDOR

1. How long does a valid credential live — *minutes*, or *until someone manually rotates it?*

2. Is the credential bound to a *hardware key or secure element*, or just to a *password + a push or OTP?*

If the answer to #1 is “until rotated,” or the answer to #2 is “a push or OTP” — **you're not authenticated against the threat model shipping breaches in 2026.**

THE PATTERN

Quick check: if an attacker stole one of your team's session tokens right now — how long would it stay valid?

Preventing bad days is the whole job.

MNEMOSHARE

Part 2 of the bad-day series