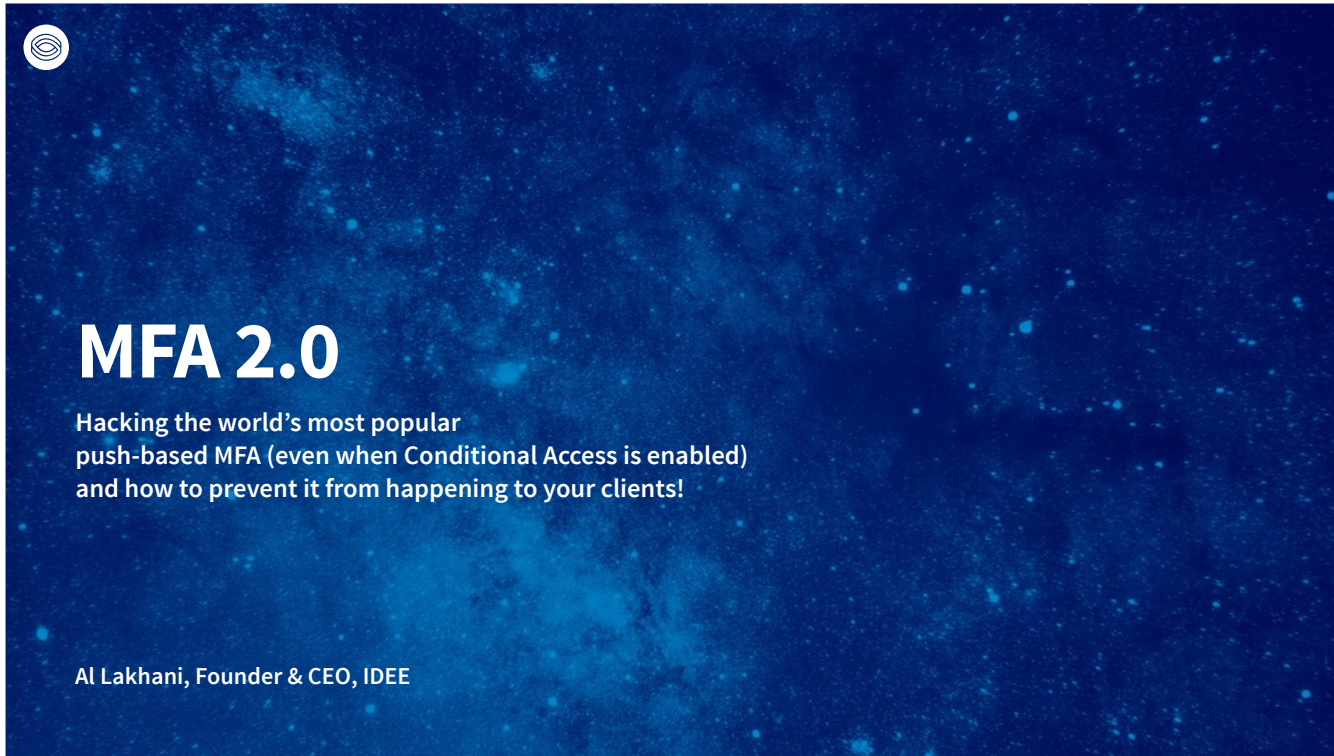
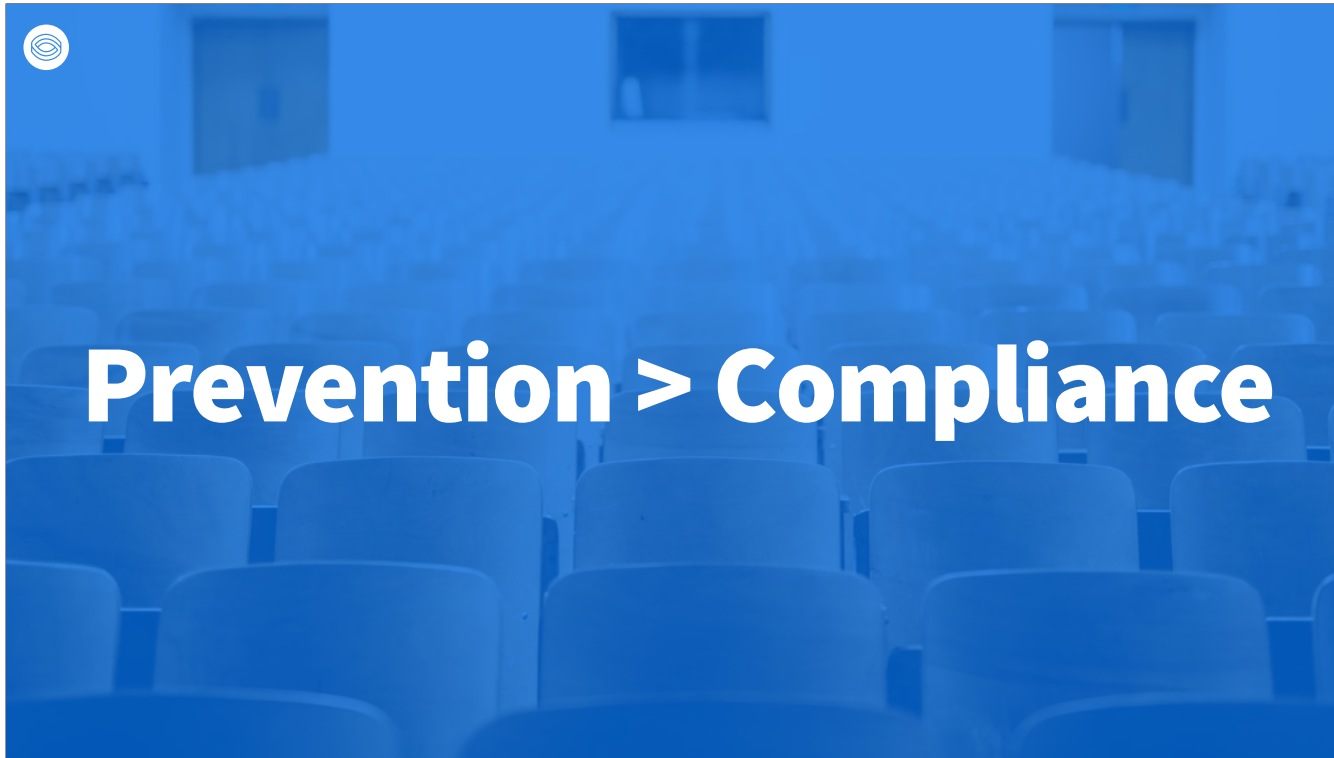




Hi. Today we are going to talk about next-generation MFA or MFA 2.0. I am Al Lakhani, founder & CEO of IDEE. Let's get started. You know I started with this title. But then I realized compliance is boring. So I changed it...



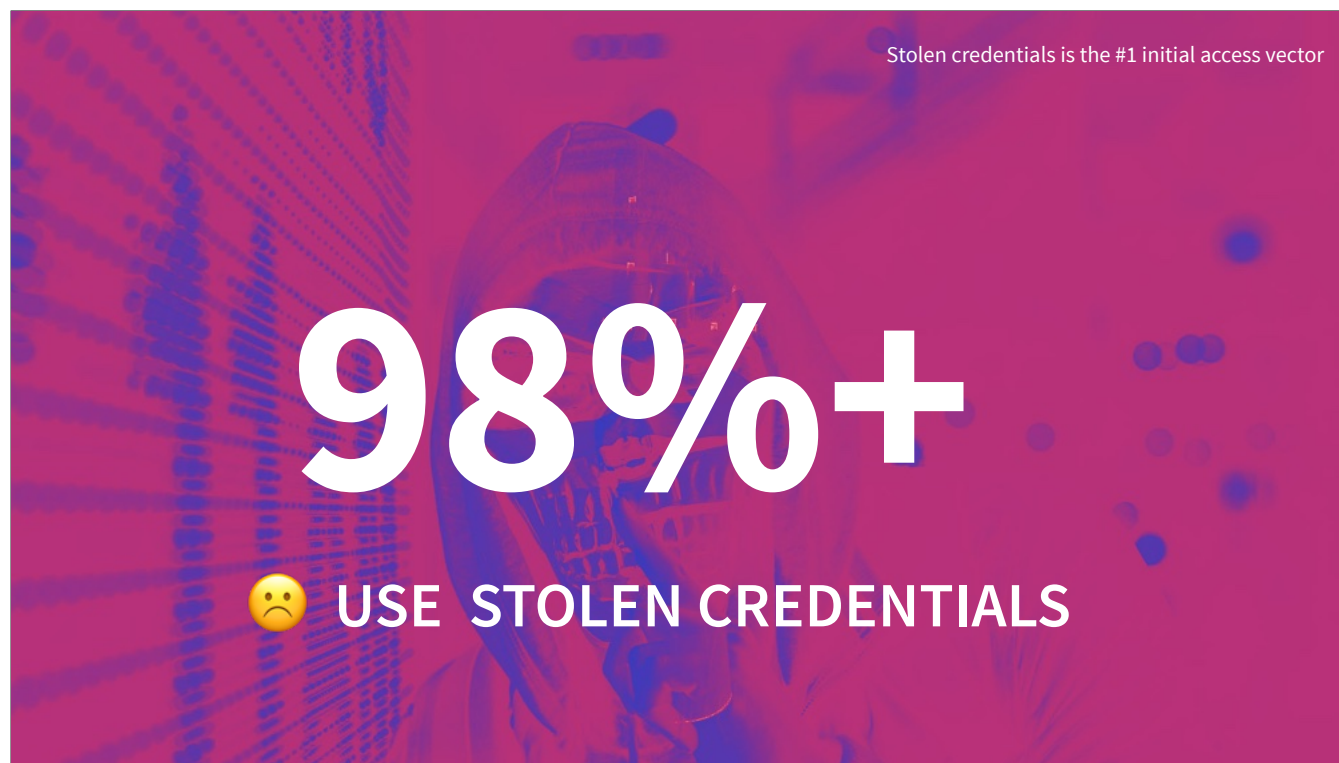
To hacking Microsoft Authenticator with features like Defender and Conditional Access enabled. My CISO is not a fan of me doing these live demos. So I hope that for the sake of my bet with him, the demo will work without any issues! And all kidding aside, I will say that...



Prevention is critical. And compliance is important. So while today I will tie a lot back to compliance, I want to be clear, I am very clearly focused on prevention. So let's get started.

- 
- 😞 **USE STOLEN CREDENTIALS**
 - 😓 **EXPLOIT A VULNERABILITY**
 - 😡 **GO THROUGH THE BACKDOOR**

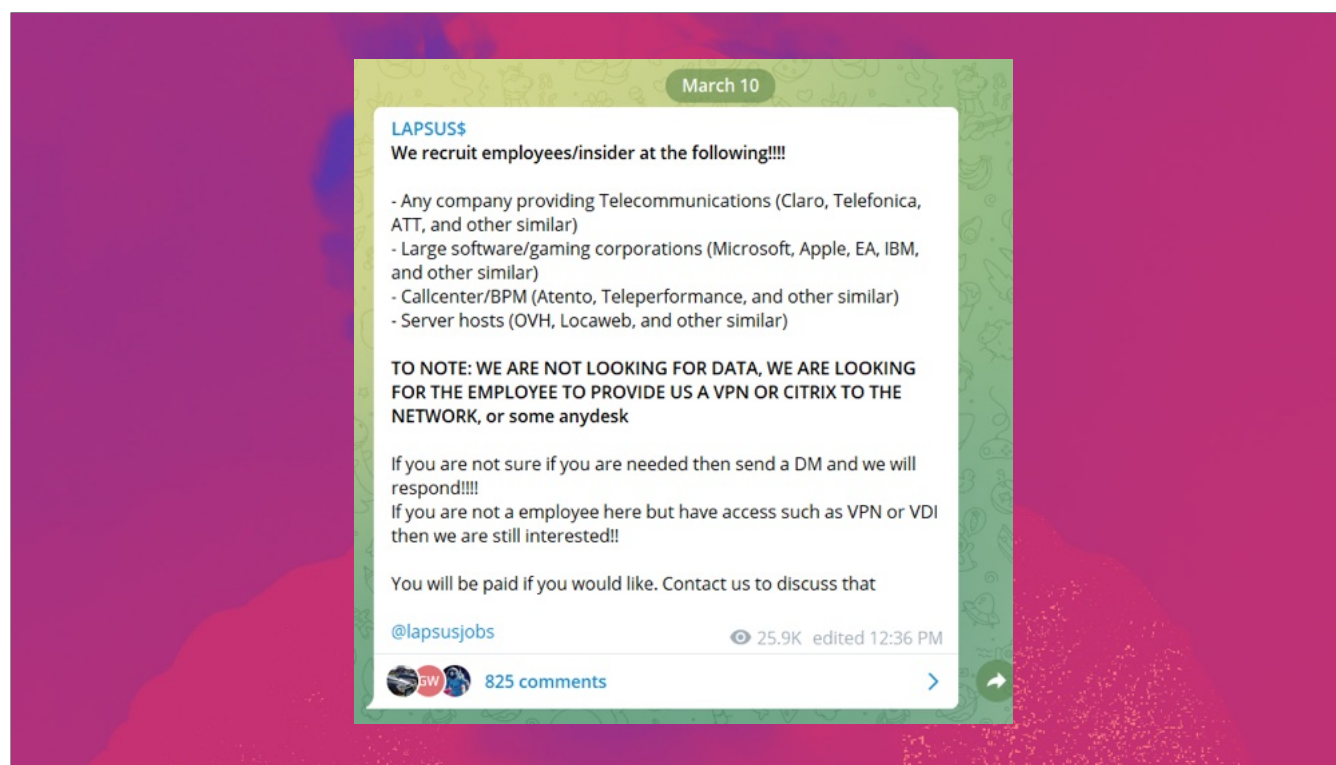
Stealing your digital identity or taking over your account is now big business. For this prezi I will refer to it as account takeover. There are only 3 ways this is possible.



Stolen credentials are responsible for 98% of breaches



In fact it is so easy that the number one attack vector for initial access in Ransomware are stolen or compromised credentials.



And account takeover is so easy that cyber criminal groups like LAPSUS\$ are advertising on Telegram to find disgruntled employees. Did you know that if I steal your credentials or you give me your credentials, there is no way for your boss to know until it is too late? When you think about this, it is super scary for MSPs. And I want to make it real for you all. So let's...



...hack Microsoft Authenticator live with Defender and Conditional Access enabled.



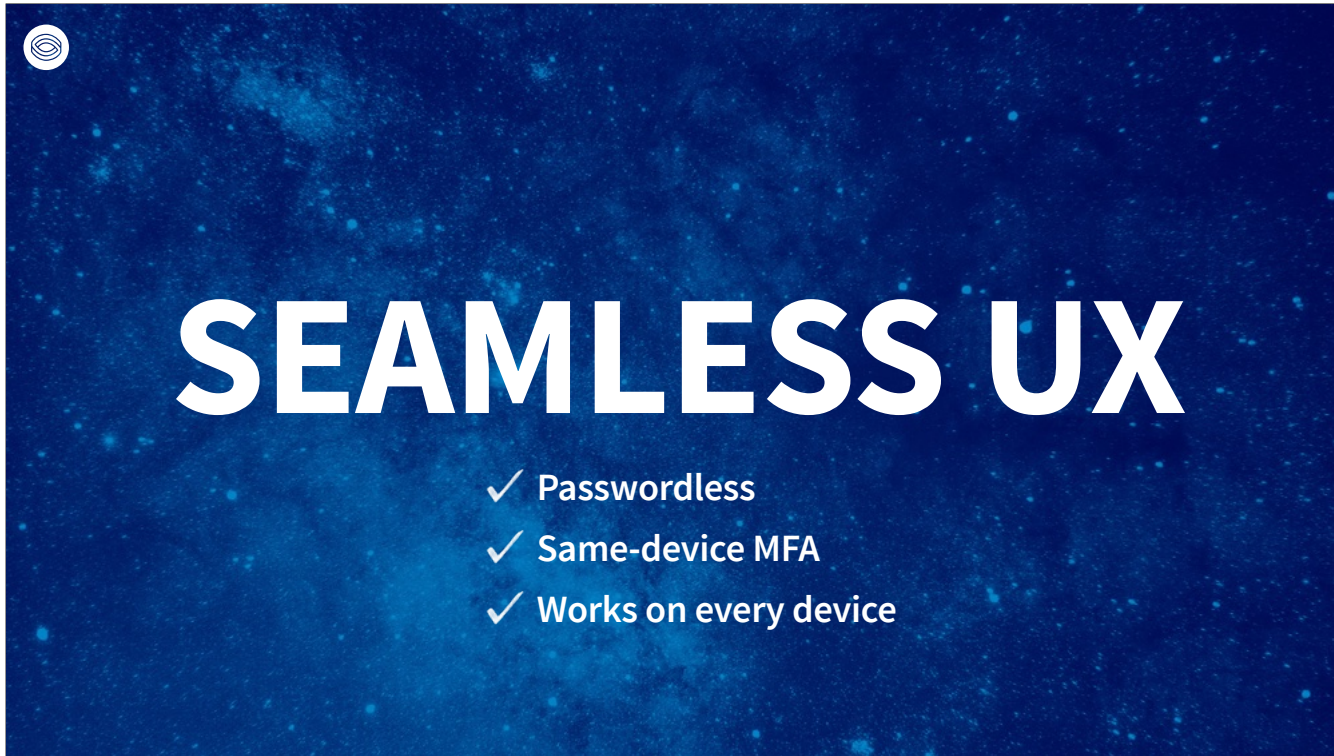
That is MFA 1.0. The fact is that it cannot protect businesses from credential phishing and MFA bypass.



We need MFA which is better.



We need MFA which can be deployed in minutes.



We need MFA where the UX is seamless.



That is why we created AuthN by IDEE. It is MFA 2.0. And rather than talk about what MFA 2.0 looks like, let's see it in action. I will do two additional demos today. 1st...



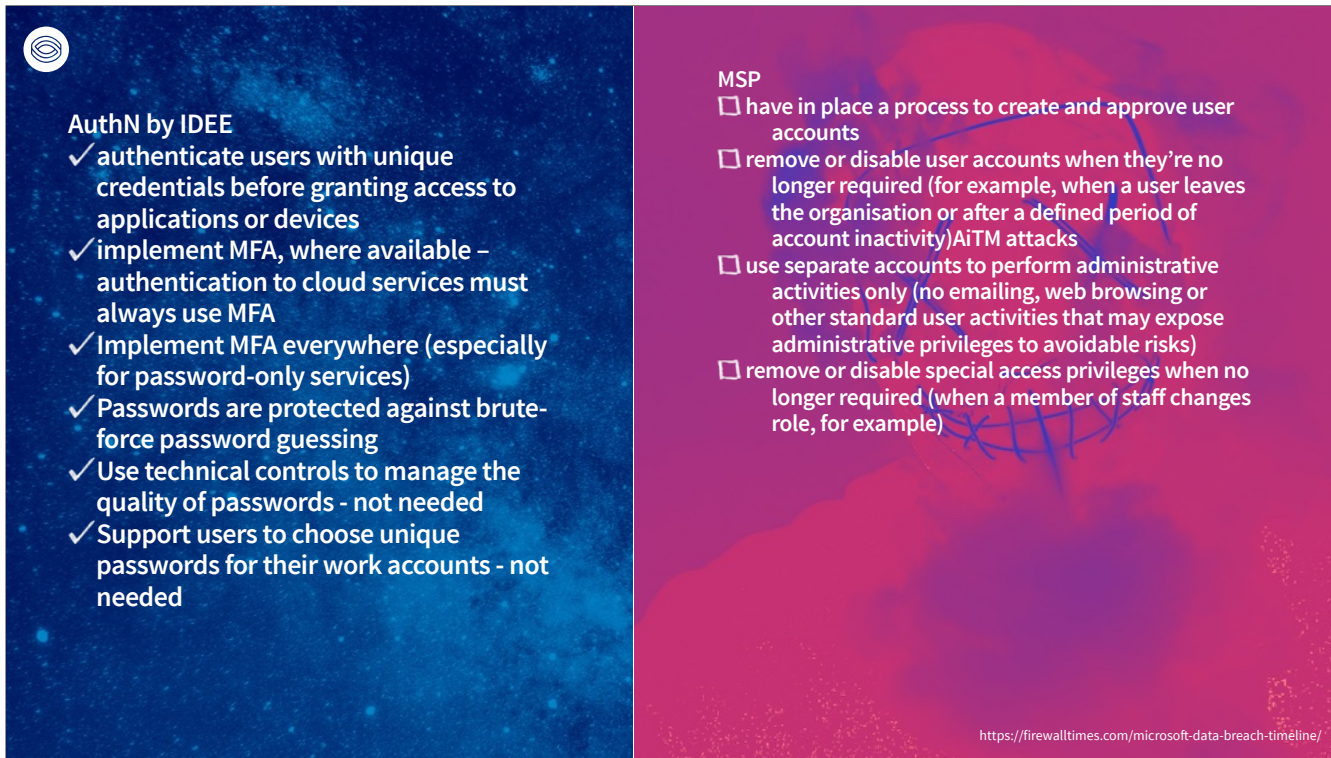
How easy it is to integrate with M365. So fast integration. And..




Second, the seamless UX.



That was MFA 2.0. And the best part it complies with requirements for Cyber Essentials v3.1 and v3.2. And the devil is in the details so let's dive in.



 AuthN by IDEE

- ✓ authenticate users with unique credentials before granting access to applications or devices
- ✓ implement MFA, where available – authentication to cloud services must always use MFA
- ✓ Implement MFA everywhere (especially for password-only services)
- ✓ Passwords are protected against brute-force password guessing
- ✓ Use technical controls to manage the quality of passwords - not needed
- ✓ Support users to choose unique passwords for their work accounts - not needed

MSP

- ☐ have in place a process to create and approve user accounts
- ☐ remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)
- ☐ use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)
- ☐ remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

<https://firewalltimes.com/microsoft-data-breach-timeline/>

And this list of MSFT breaches are only for the last 10 years.

Cyber Essentials

4. User Access Controls (Requirements)

- Authenticate users with unique credentials before granting access to applications or devices
- Authentication to cloud services must always use MFA
- Implement MFA, where available
- Implement MFA everywhere (especially for password-only services)

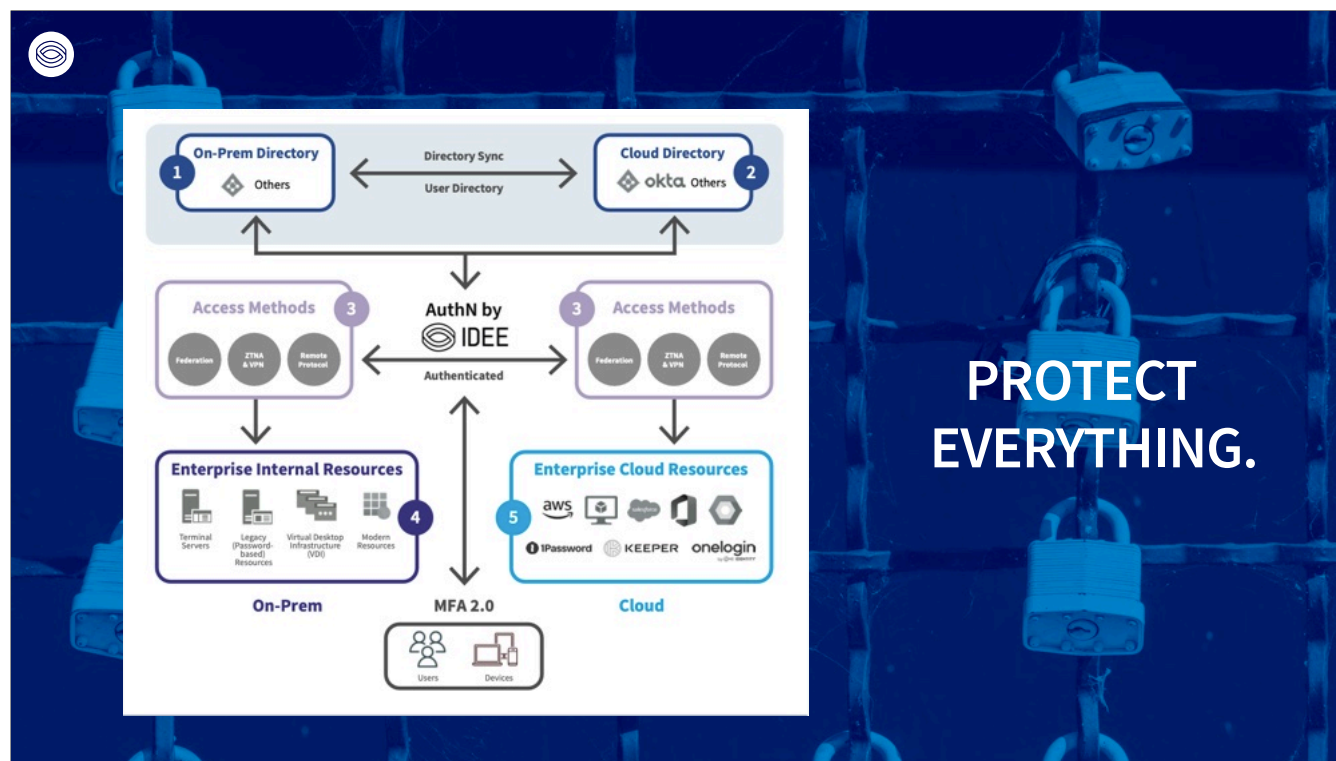


Cyber Essentials

4. User Access Controls (Passwords)

- Passwords are protected against brute-force password guessing
- Use technical controls to manage the quality of passwords - not needed
- Support users to choose unique passwords for their work accounts





This is why we created MFA 2.0.



This is why we created MFA 2.0.



What do our customers say...



“...just buy it. You will thank me later. Since we introduced the solution we have not had a single account takeover. [It] let's me sleep peacefully.”

Head of Cloud Services
Joel Knecht



..DekaBank

“IDEE GmbH offers a new way of thinking for securing and leveraging digital identities with best-in-class security, privacy and usability. This was instrumental in enabling the digital transformation of the Capital Markets’ new products and meeting the stringent regulatory expectations.”

Stephan Hachmeister
Managing Director

“AuthN is an essential part of our security concept for safeguarding the will of the customer in our crypto business.”

Sascha Bach
IT Manager



4.8/5

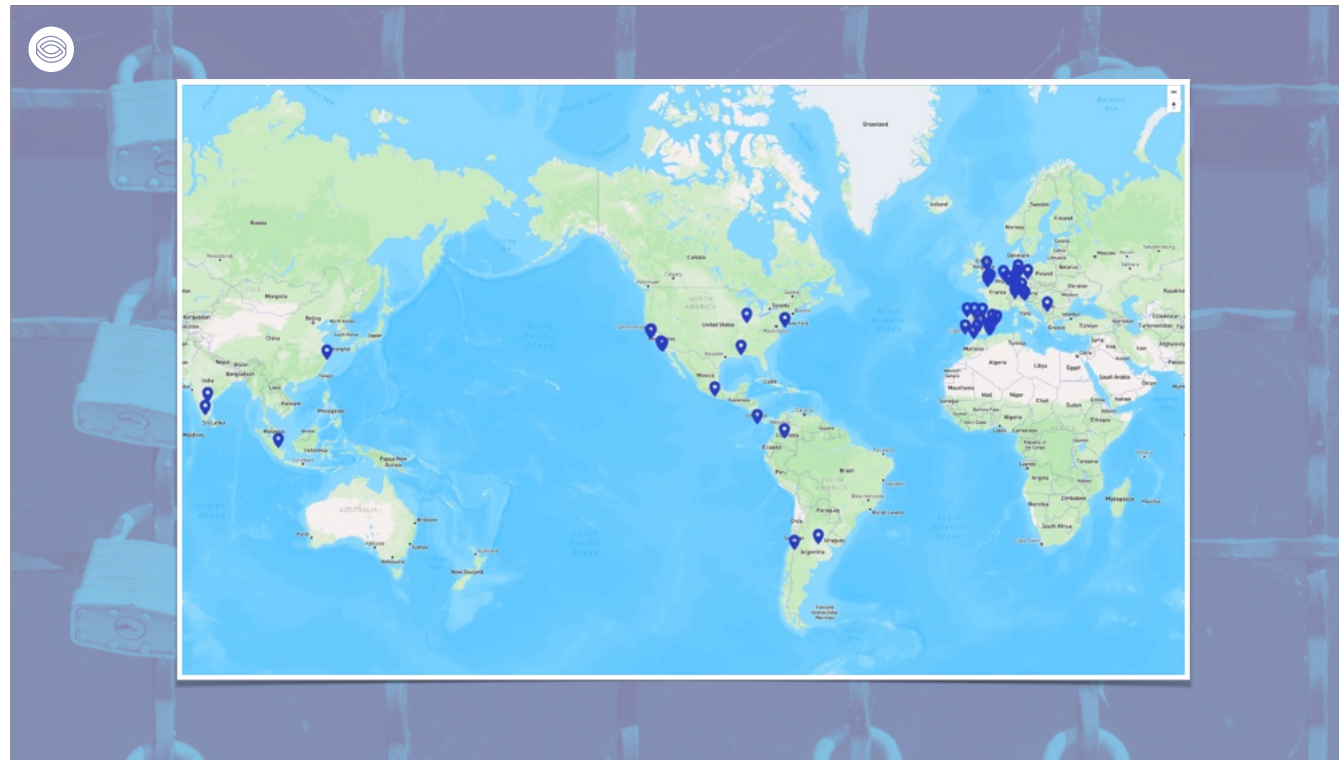




We are a channel first company.



We have lots of great partners. And we are super excited to have Brigantia as our newest partner in the UK. Our partners love us because we have 3 USPs which are not available from any other MFA provider in the market today.



We are already selling it in Germany, Austria, and Switzerland.

Who are we?





**Our mission is to render account
takeover a relic of the past...**



... securely navigate the online
world with absolute confidence.



That was MFA 2.0. And the best part it complies with requirements for Cyber Essentials v3.1 and v3.2. And the devil is in the details so let's dive in.



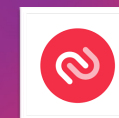
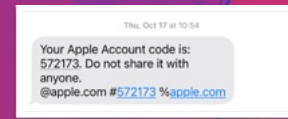
FAST INTEGRATION



Deployed in mins.

AuthN by
 IDEE

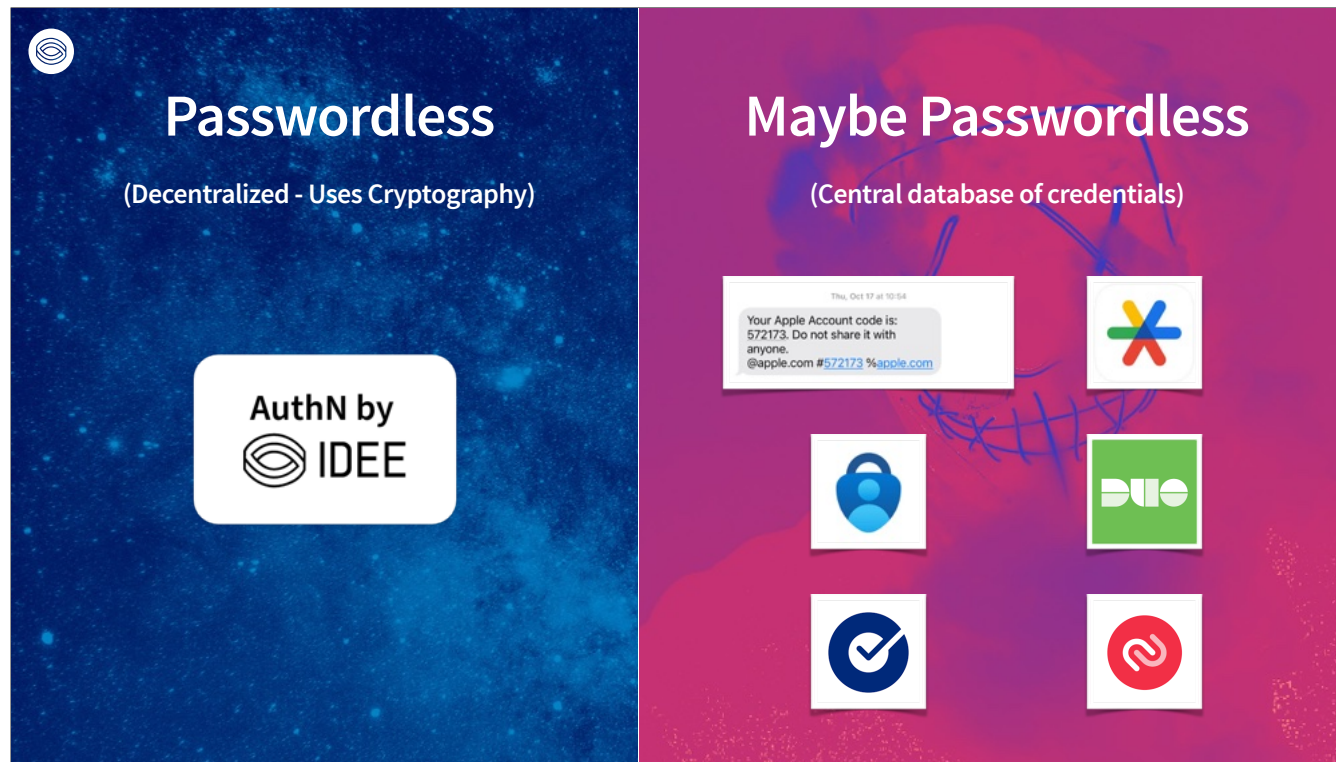
Needs a project plan



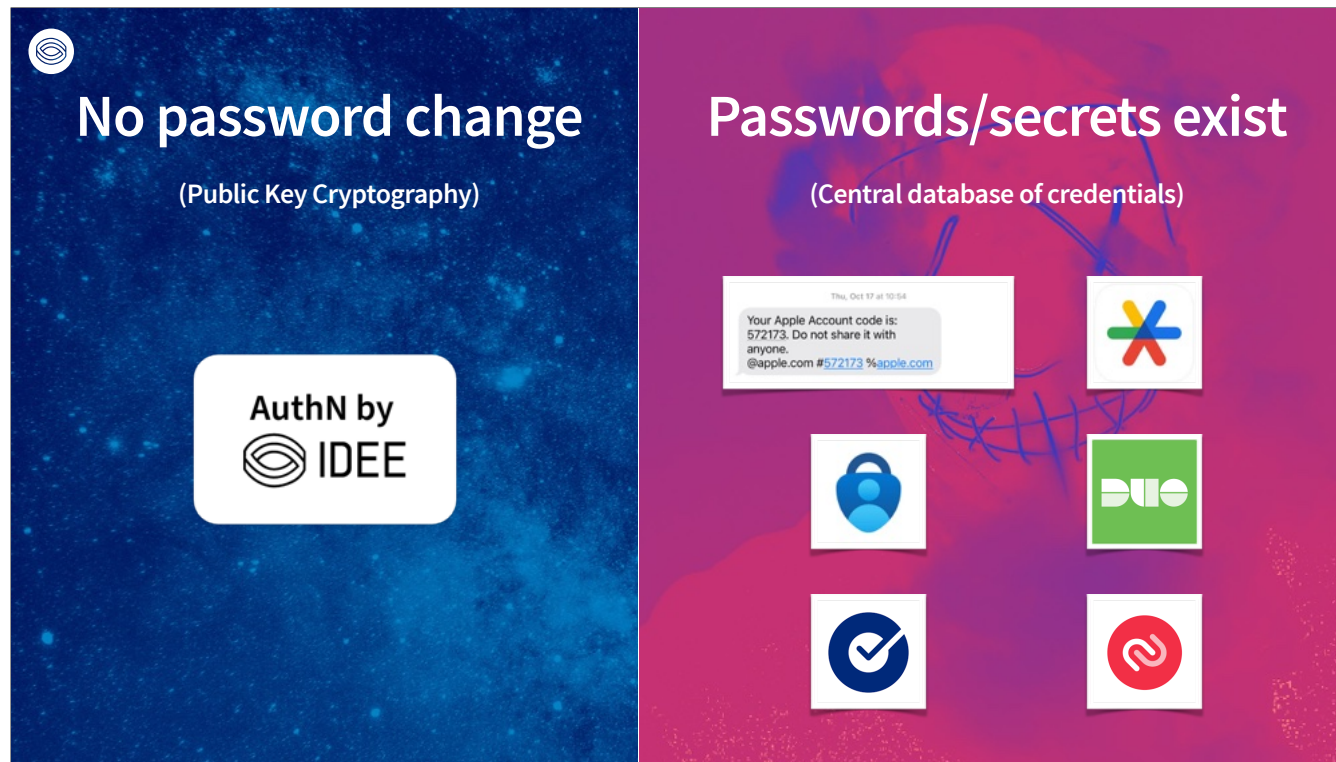


USP #3

SEAMLESS UX



You can put a gun to my head or threaten the life of my kids to get Robert's credentials, I still cannot help you. I just do not have them. They exist on Robert's devices.



We have no passwords. So stealing them is out of the question. We do not have a central credentials database. Which means you also do not have a central credentials database of all the passwords of your customers.

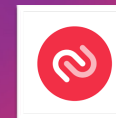


Same Device

AuthN by
 IDEE

2nd device needed

Thu, Oct 17 at 10:54
Your Apple Account code is:
572173. Do not share it with
anyone.
[@apple.com #572173 %apple.com](#)

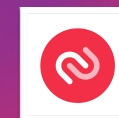
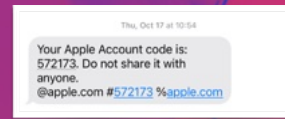




Anyone can use it

AuthN by
 IDEE

Digital native needed





100%

- ✓ Stop all password-based attacks
- ✓ Stop all credential phishing attacks
- ✓ Stop all AiTM attacks



Stops ALL

- ✓ Password-based attacks
- ✓ Credential-phishing attacks
- ✓ AiTM attacks

AuthN by
 **IDEE**



| | |
|----------------|---|
| January 2024 | Microsoft breached by Russian hacker group |
| September 2023 | 60k State Department Emails Stolen in Microsoft Breach |
| July 2023 | Chinese Hackers Breach U.S. Agencies Via Microsoft Cloud |
| July 2023 | Microsoft Denies Purported Data Breach |
| October 2022 | 548,000+ Users Exposed in BlueBleed Data Leak |
| March 2022 | Lapsus\$ Group Breaches Microsoft |
| August 2021 | Organizations Expose 38 Million Records Due to Power Apps |
| August 2021 | Thousands of Microsoft Azure Customer Accounts and |
| January 2021 | Microsoft Exchange Server Vulnerability Leads to 60,000+ |
| December 2020 | Microsoft and 18,000 Other SolarWinds Customers Targeted |
| December 2019 | Over 250 Million Microsoft Customer Records Exposed |
| April 2019 | Compromised Support Agent Credentials Give Hackers |
| November 2016 | Hundreds of Skype Accounts Hacked to Send Spam |
| May 2016 | 33 Million Stolen Hotmail Credentials Discovered for Sale |
| October 2013 | Internal Microsoft Bug Tracking Database Compromised |

<https://firewalltimes.com/microsoft-data-breach-timeline/>

And this list of MSFT breaches are only for the last 10 years.



December 2024 - Chinese hackers breach Janet Yellen's computer via remote access using a token from Beyond Trust a leader in PAM solution.



TRANSITIVE-TRUST

(Protects the entire identity lifecycle)

AuthN by
 IDEE



-TRUST

(Relies on the human firewall of admins)



Hackers Stole Access Tokens
from Okta's Support Unit



<https://krebsonsecurity.com/2023/10/hackers-stole-access-tokens-from-oktas-support-unit/>



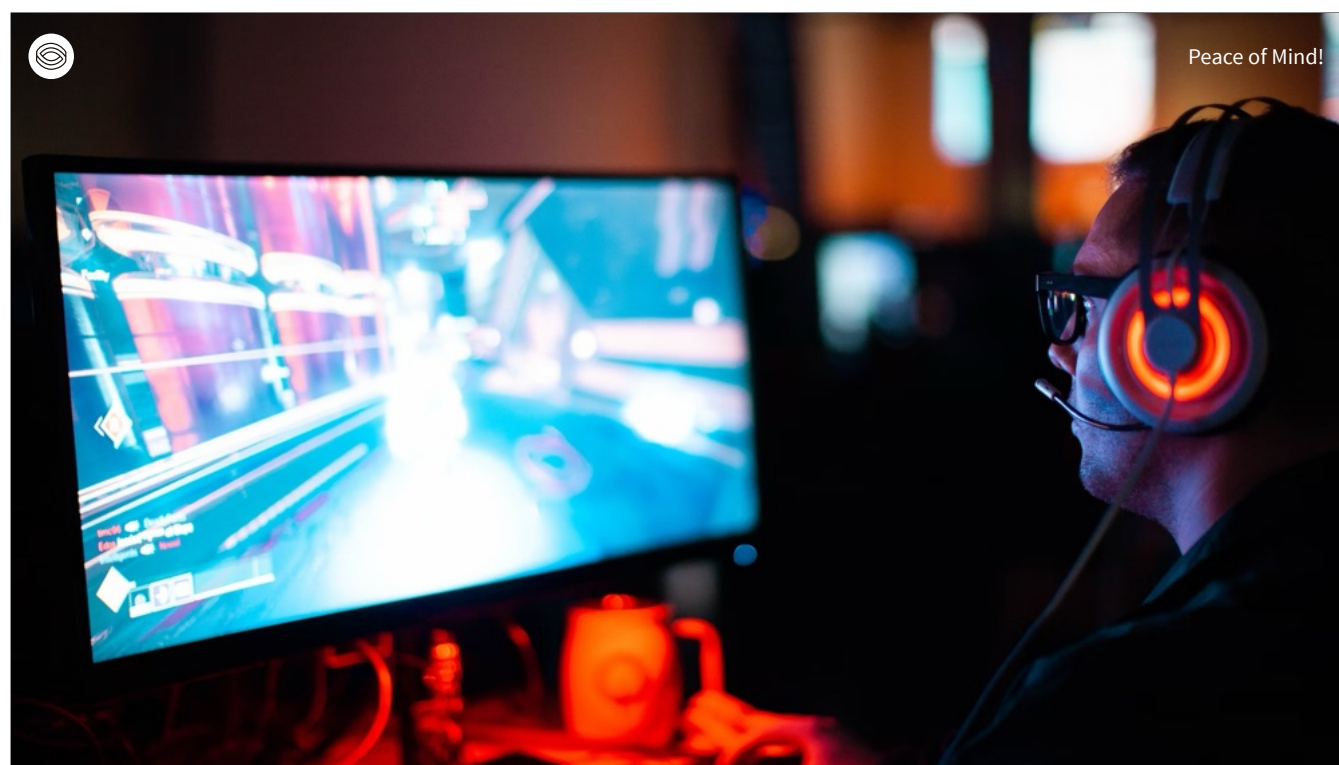
The problem with a credential provider is that it can be bypassed. Duo lists 10 reasons why this can happen. Don't believe me, just scan this QR-code. This is the headline from their knowledge base article from the Duo website.



The result...



Peace of Mind!





Peace of Mind!

 **Al Lakhani**
Founder & CEO

Thank You!





Your questions...