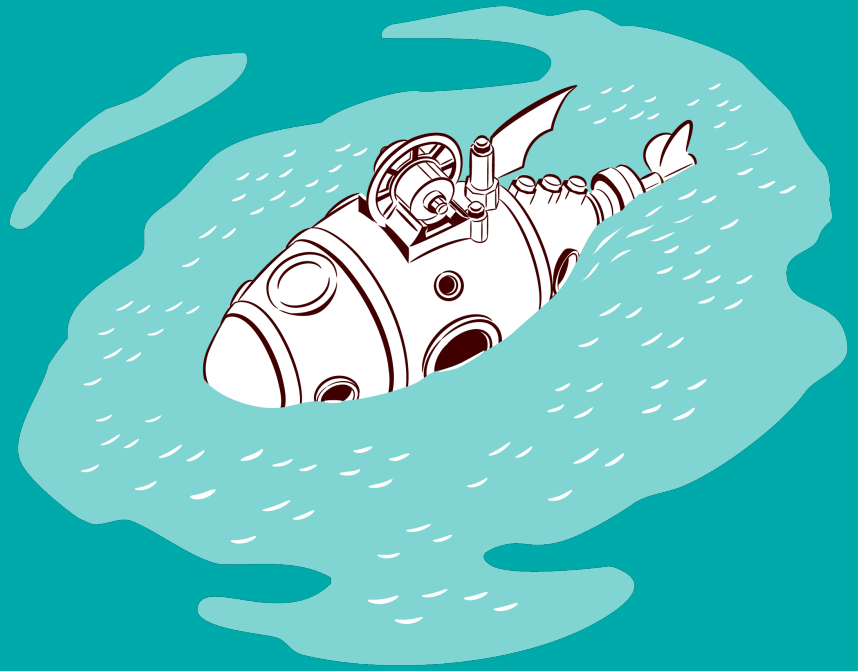
ALEF

Moderní způsob autentizace

Secure Access with Cisco DUO

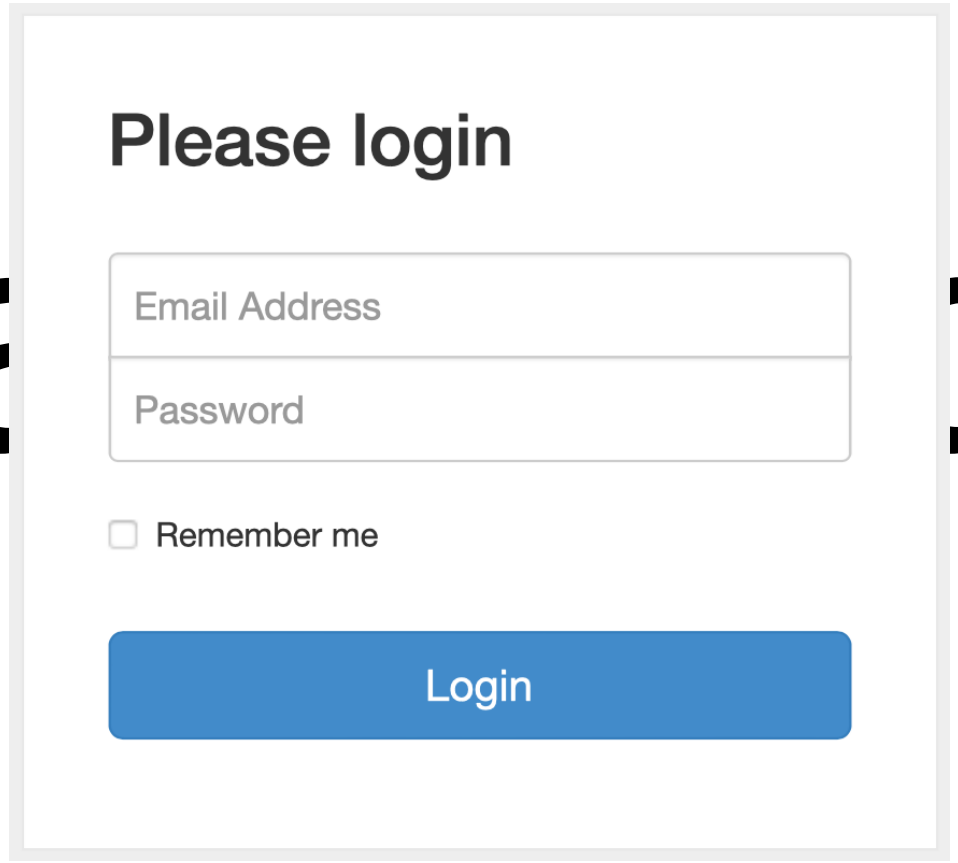


Jan Šimůnek

Systems Engineer, Network Security

jan.simunek@alef.com

Pa ds



ALEF

Password123!

HASH

2c103f2c4ed1e59c0b
4e2e01821770fa

Take the Password Test

AcmeCo

Email	Cracked
...	...
jim@mail.com	R0cky!17
...	...

1 guess is enough!

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
...	...

Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus

Have I Been Pwned: Check if your email has been compromised in a data breach

Správa přístupu pomocí **Cisco DUO**

vytvoření důvěry

Autentizace uživatele

- Vícefaktorová autentizace
- Passwordless
- Nezávislost na zdroji identity

Důvěryhodnost zařízení

- Device Trust
- Device health & compliance
- Mac, Win, Linux, iOS, Android, BYOD

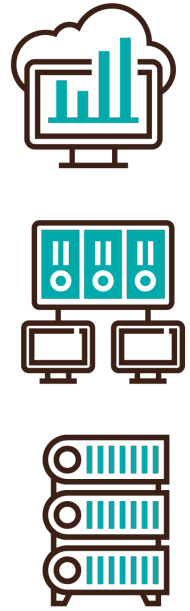
Zpřístupnění aplikace

- Single Sign-On (SSO)
- VPN-less remote access
- All apps – cloud, on-prem and private

Průběžný monitoring a vyhodnocení risk-based metrik

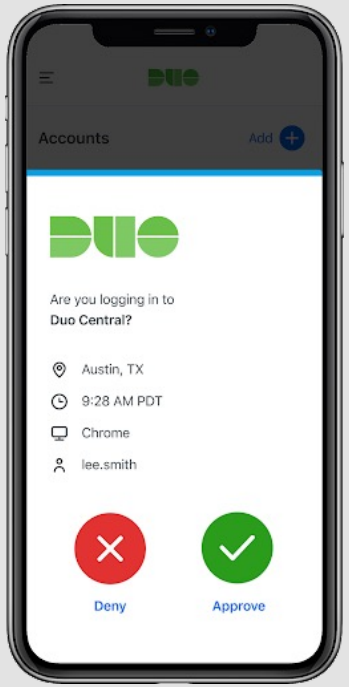
Korporátní aktiva

Cloud, On-premise,
Public, Private, Hybrid

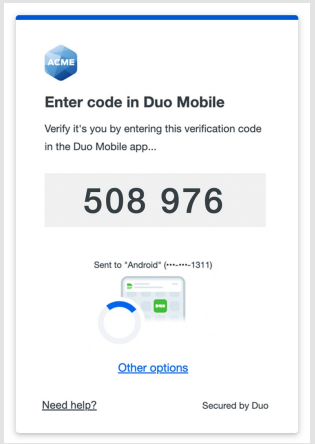


ALEF

Autentizace uživatelů



Push notifikace



Push notifikace s number matching

Napojení na libovolný zdroj identity

Kompatibilita s širokou škálou zdroje identity
LDAP, RADIUS, SAML

Microsoft Active Directory

amazon web services

Multifaktorová autentizace

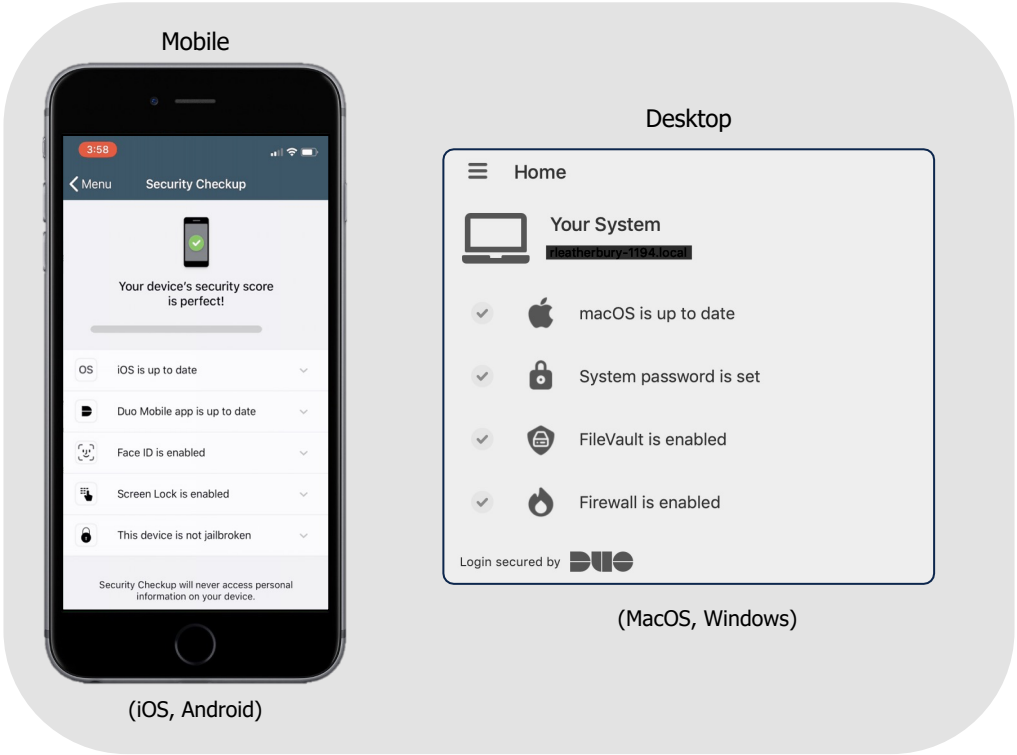
Ochrana pomocí vícefaktorové autentizace:
SMS, TOTP, Hardware tokeny, Push notifikace, Biometrie

Ochrana před phishing útoky

Automatická detekce podezřelých aktivit

ALEF

Ověření přístupového zařízení



Kontrola stavu zařízení

Zpřístupnění služby na základě splnění předem definovaných podmínek

- software up-to-date?
- passcode ochrana?
- zapnuté šifrování disku?
- ochrana endpointu zapnuta?

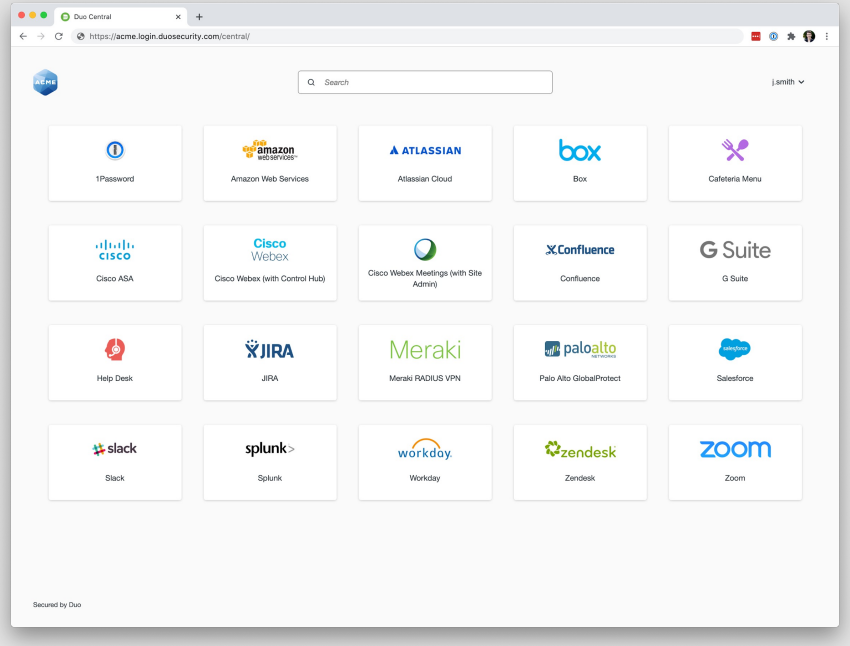
Je zařízení důvěryhodné?

Přístup pouze z povolených zařízení

- spravované zařízení pomocí MDM?
- registrované zařízení BYOD vyhovující bezpečnostním parametrům

ALEF

Zpřístupnění aplikací



Zvýšení bezpečnosti pro on-premise aplikace

Implementace MFA pro aplikace a služby hostované on-premise

Single Sign-on (SSO)

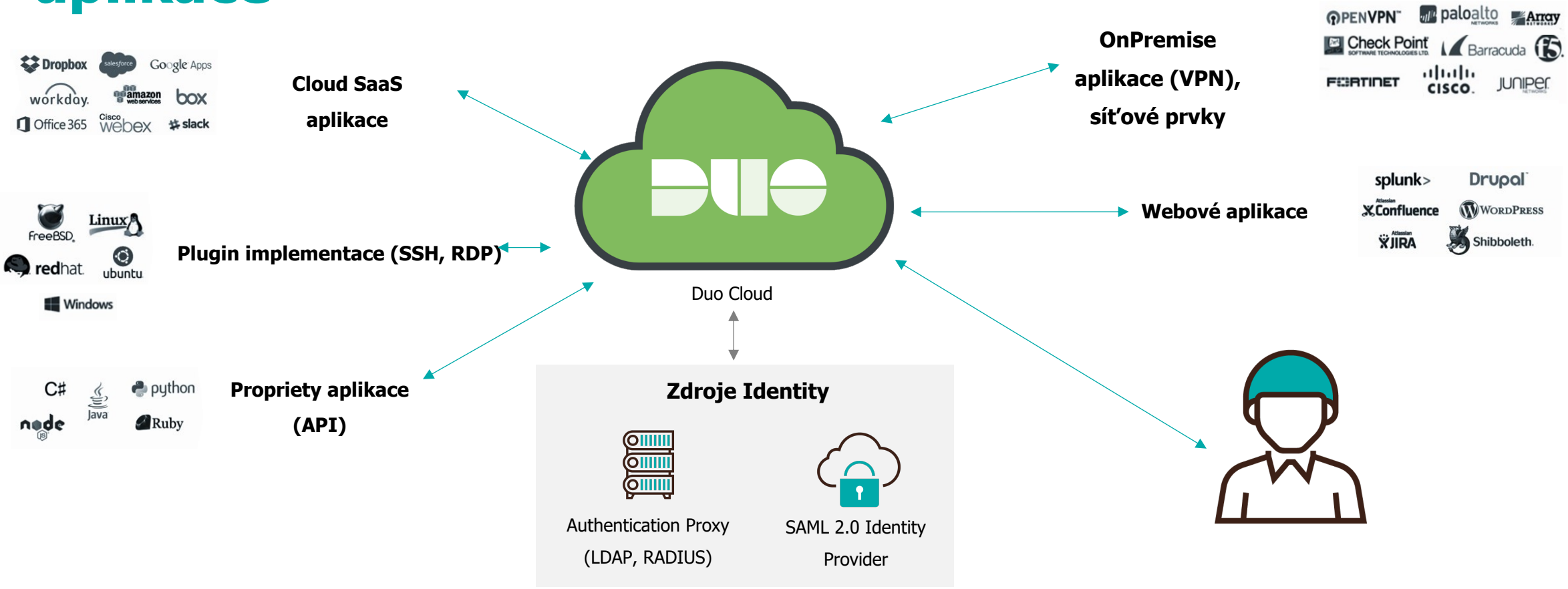
Unifikuje autentizaci a poskytuje uživatelům přístup k množství aplikací

Poskytnutí VPN-less vzdáleného přístupu

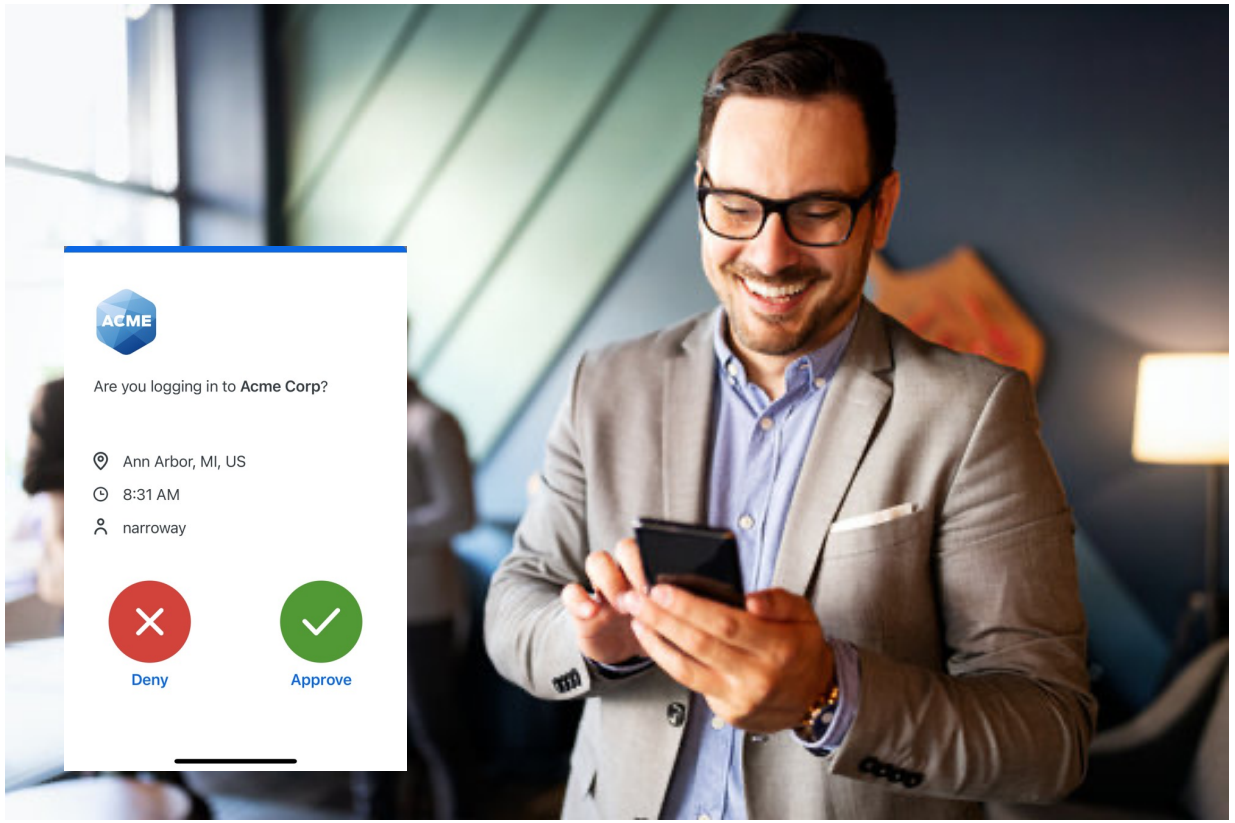
Přístup k privátním aplikacím skrze Duo Network Gateway (DNG) bez nutnosti VPN klienta

ALEF

Řešení přístupu do kterékoliv aplikace



Nasazením MFA to nekončí



Úspěšné překonání MFA (2022)

Uber data breach

Cisco unprivileged access to internal network

Microsoft user account hijacking

Social Engineering strategie

MFA fatigue nebo Push harassment

Uber data breach

Session cookie theft

Racoon Stealer

Machine-In-The-Middle Attacks

Social Engineering a ochrana po technické stránce

Push notification limitace a monitoring – 10 pokusů defaultně nastaveno v DUO

Risk based authentication – automatická detekce a funkce dostupná v DUO

Vyhodnotit možnosti 2FA: Vypnutí push notifikace a zapnutí push notifikace s number matching ověřením (MS nebo DUO)

FIDO2 (klíčenka Yubikey, Microsoft Windows Hello, Apple Face ID, passkeys)

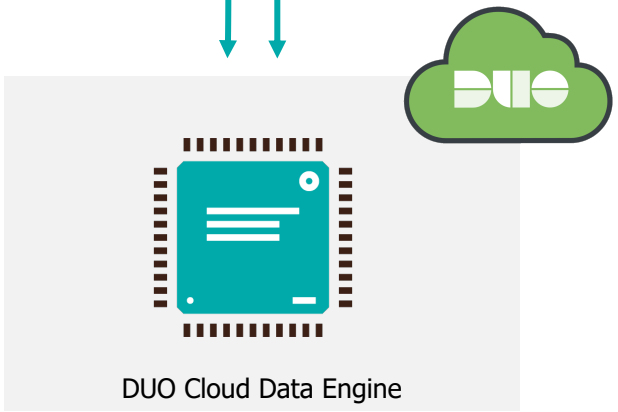
Risk Based Authentication

Zprocesování historických dat

Wi-Fi fingerprint, device IP, time of day, Browser Agent

Detekuje známé attack patterny

Push harassment, Push fatigue, Push spray, high risk location

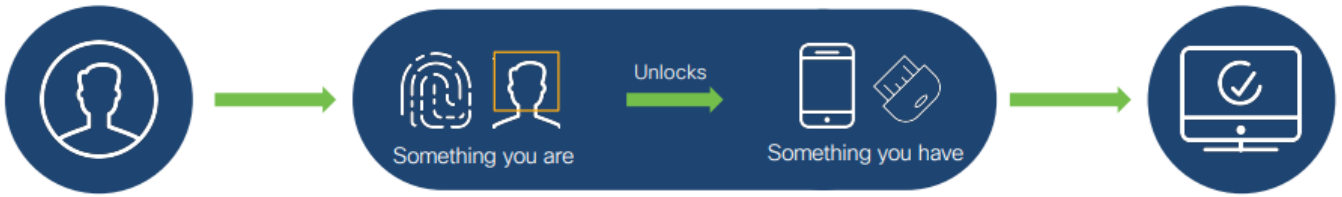


Risk Based Authentication

ALEF

FIDO2 - Passwordless Autentizace

- Není zapotřebí uchovávat něco co známe – “something you know”, místo toho použít veřejný klíč
- Uživatelsky přívětivé, technicky komplexní a bezpečné řešení
- FIDO2 nejsou jen klíčenky! Podporuje Windows Hello, Apple Touch ID/Face ID



Two Factor

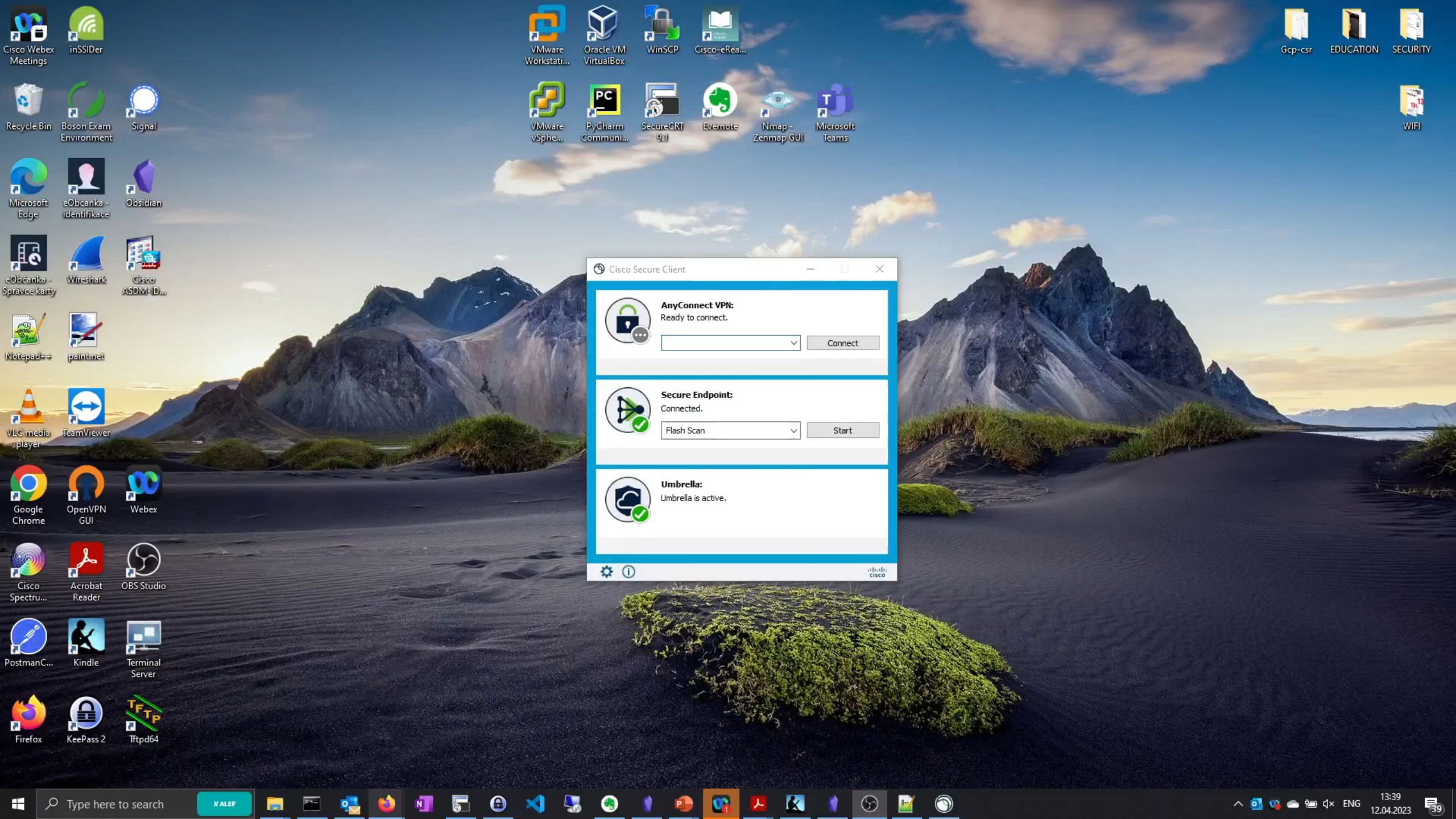
No Shared Secret

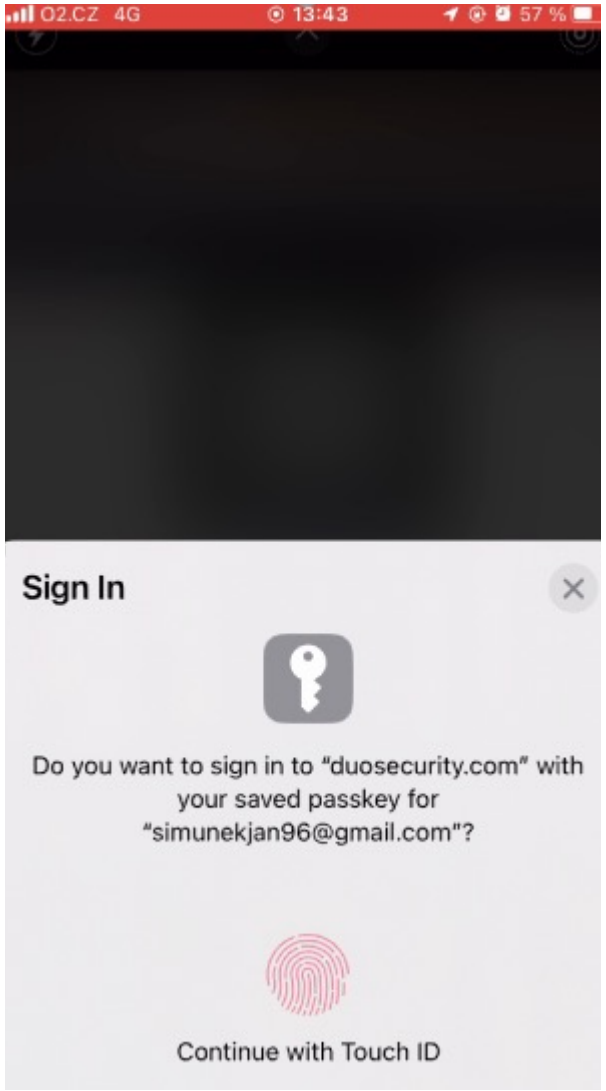
One Step

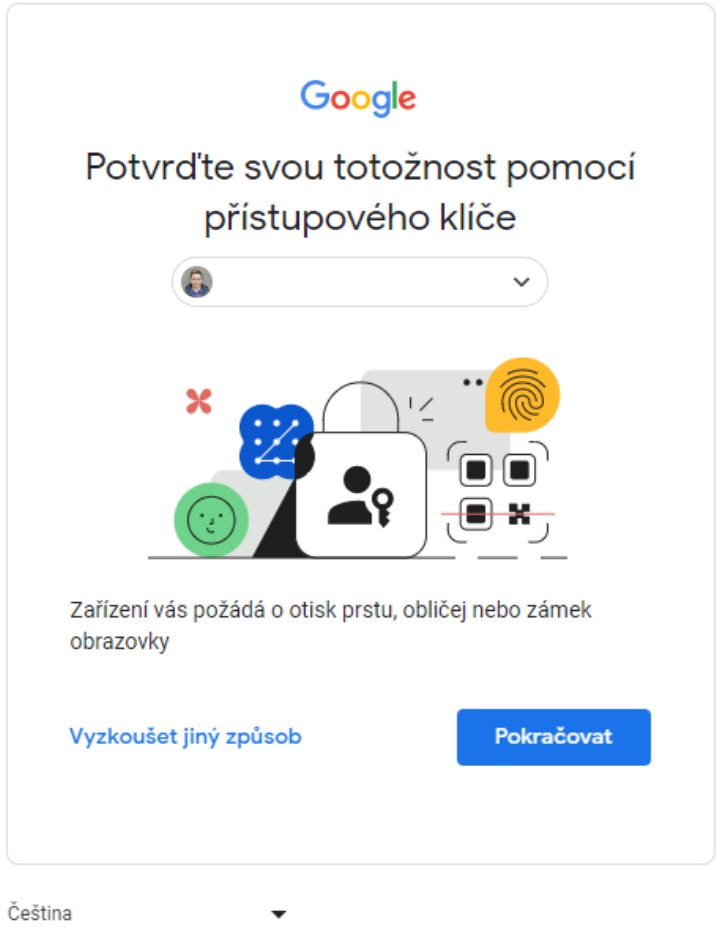
Biometrická data

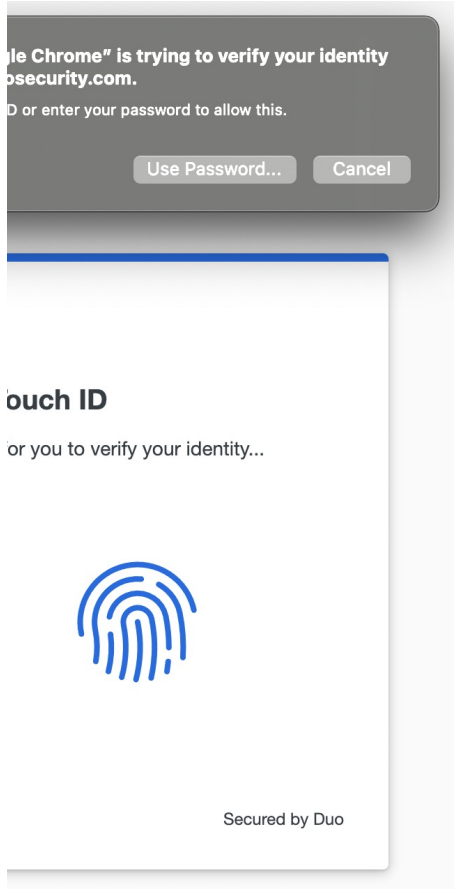
Privátní klíč uložený na zařízení

ALEF


Cisco Webex Meetings
inSSIDer
VMware Workstati...
Oracle VM VirtualBox
WinSCP
Cisco-eRea...
Gcp-csr
EDUCATION
SECURITY
Recycle Bin
Boson Exam Environment
Signal
VMware vSphe...
PyCharm Communi...
SecureCRT 9.1
Evernote
Nmap - Zenmap GUI
Microsoft Teams
WIFI
Microsoft Edge
eOčanka - identifikace
Obsidian
eOčanka - Správce karty
Wireshark
Cisco ASDM-ID...
Notepad++
paint.net
VLC media player
TeamViewer
Google Chrome
OpenVPN GUI
Webex
Cisco Spectru...
Acrobat Reader
OBS Studio
PostmanC...
Kindle
Terminal Server
Firefox
KeePass 2
Tftpd64
Cisco Secure Client
AnyConnect VPN:
Ready to connect.
Connect
Secure Endpoint:
Connected.
Flash Scan
Start
Umbrella:
Umbrella is active.
Type here to search
ENG
13:39
12.04.2023







FIDO2 v praxi: **WebAuthn.io**

ALEF

Děkuji za pozornost!