

iStores



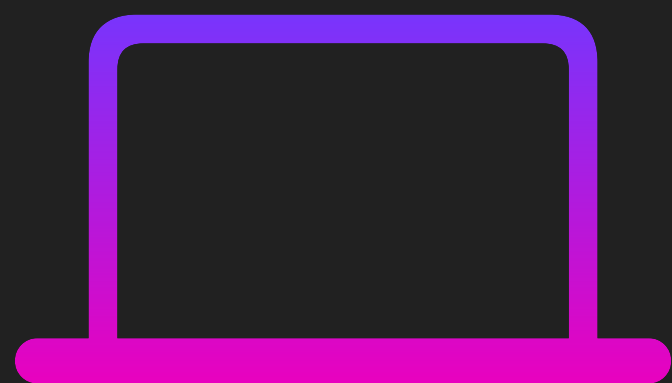
Premium
Partner

Jak řešení Apple posilují firemní bezpečnost a odolnost

Ivan Malík BA (Hons)
Head of Professional Services

18. 3. 2026

Experti v nasazení a správě Apple zařízení ve firmách



**Téměř 25 let
v ICT oboru**



**Certifikovaný
tým**



**Výborné
reference**

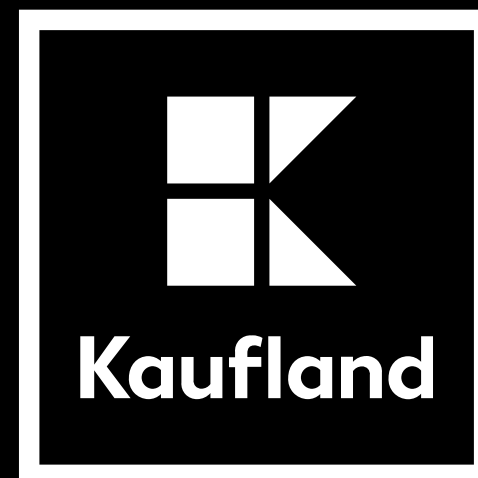


**Komplexní
řešení**

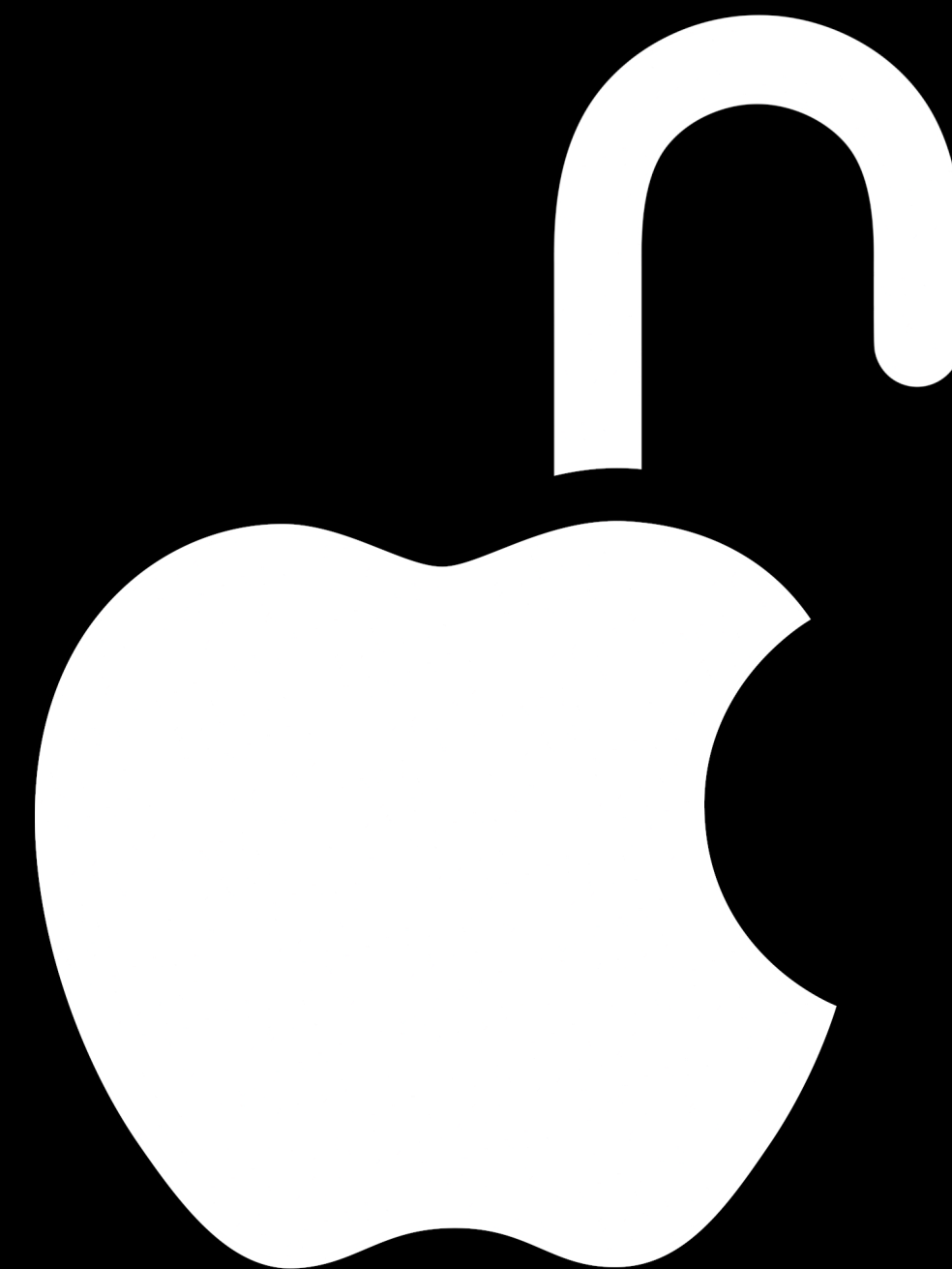


**Prodejny a
servisy**

REFERENCE



**Vícevrstvý bezpečnostní
model připravený pro NIS2**



Bezpečnost vestavěná v každé vrstvě



Služby



Síťové zabezpečení



Bezpečnost aplikací



Šifrování a ochrana dat



OS zabezpečení

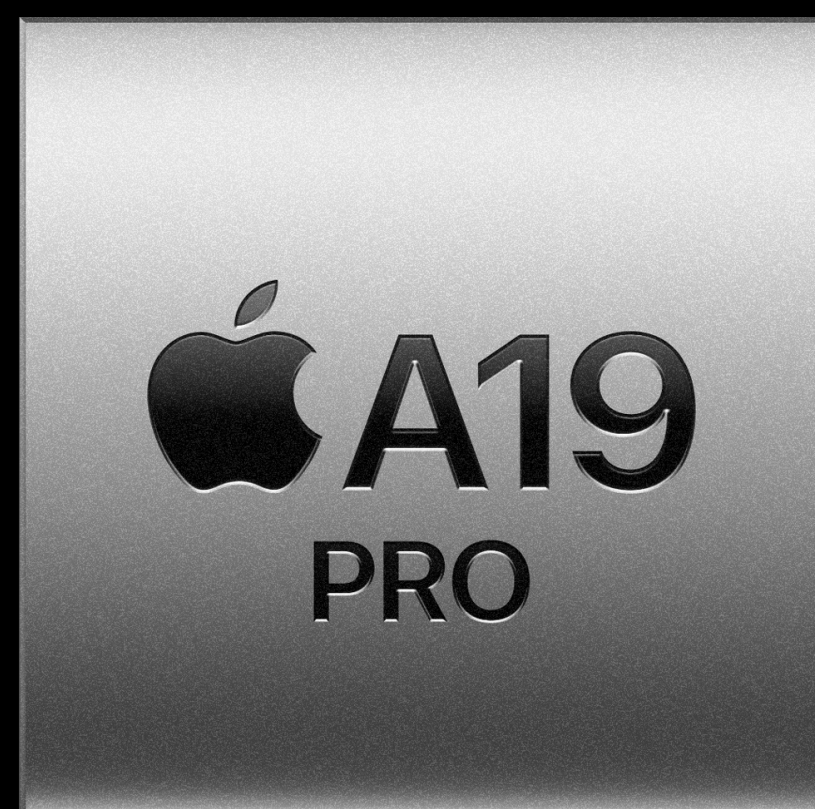


Hardwarové zabezpečení





Secure Boot
Ochrana integrity systému



Secure Enclave
Touch ID
FileVault
Ochrana osobních údajů

Zero-touch a MDM: **Správa, která nestojí čas**





Správa bezpečnosti pomocí MDM

Vynucení bezpečnostních standardů

Ochrana dat a šifrování

Řízení toku dat

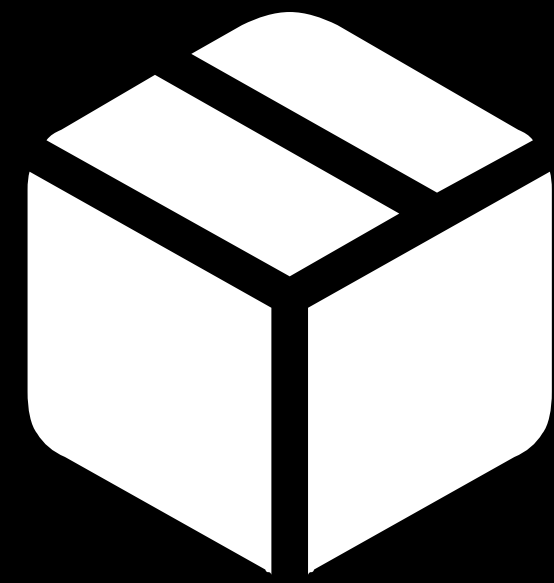
Správa zámku aktivace

Režim ztráty a vzdálené smazání

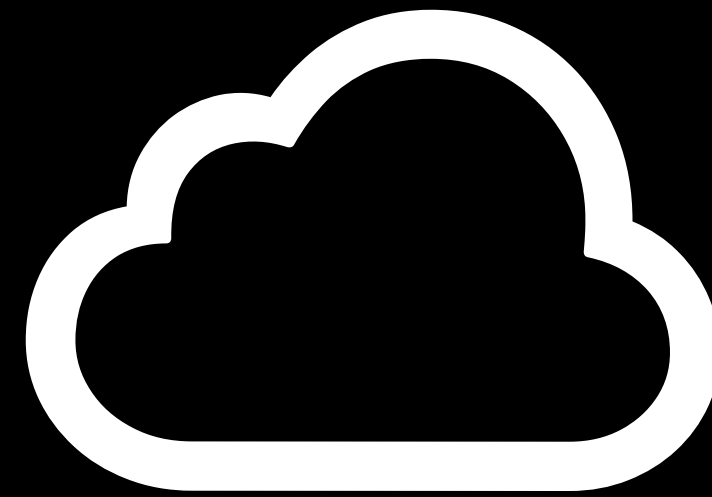




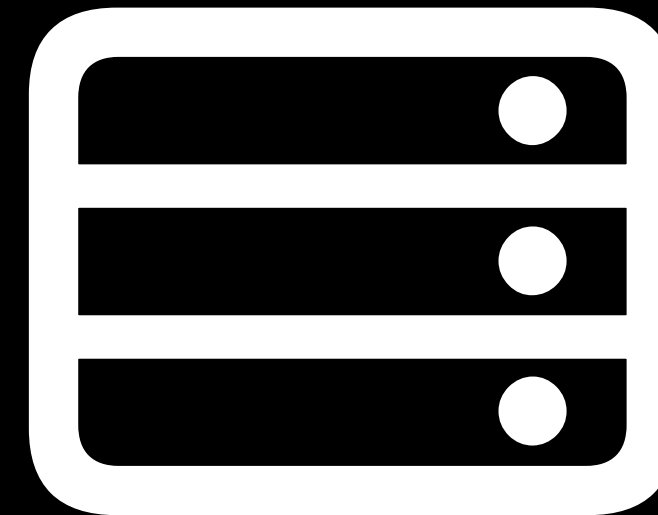
Jak Zero-touch nasazení funguje



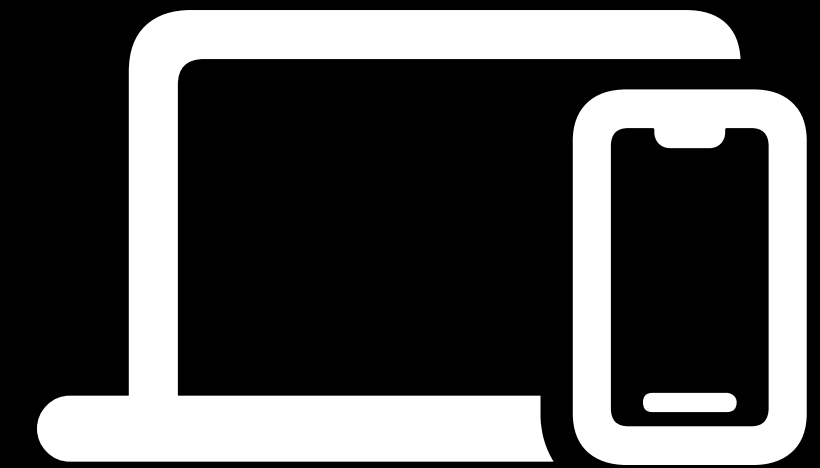
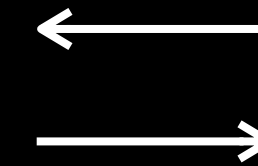
Nákup



Apple Business
Manager



MDM Server



Zařízení

Ochrana **soukromí** a **zabezpečení dat**

11001110001111011100000110000000110001110
00111111000001000111000111111100110000011
10001110010100110110001100001111000110001
11001001100011001111011000110100011100010
100000111010010001000111111100100101
1111100000010001000111000000011
11011000001000111100000100001000010
0001000110001001111111100111111
111011011000000100110100011111101111
11110111001000010010010011100110001
001100001111111100100100110110011110
0111011111011011110010011111111100
00001001000100010010010001110010000
00011101100000011100000100110100000001010
00011001111001111110001000111101100010110
01111011001011000111001111100001001111001
10001110011000110111110000001100000100111



Ochrana soukromí a zabezpečení dat

Zpracování přímo v zařízení (On-device Processing)

Private Cloud Compute

Prevence sledování a šifrování

Transparentnost a kontrola uživatele



Přístup k soukromým datům pomocí MDM

- | | |
|--|---|
| ✓ Konfigurace firemního účtu | ✗ Přístup k osobním údajům |
| ✓ Konfigurace Per-App VPN | ✗ Přístup k aplikacím vlastněným uživatelem |
| ✓ Instalace a konfigurace firemních aplikací | ✗ Možnost odstranění osobních dat |
| ✓ Vynucení kódu zařízení | ✗ Sběr logů BYOD zařízení |
| ✓ Vynucení firemních politik | ✗ Převzetí aplikací vlastněných uživatelm |
| ✓ Přístup k firemním aplikacím | ✗ Přístup k poloze zařízení |
| ✓ Odstanění pouze pracovních dat | |

Spolkový úřad pro bezpečnost informační techniky

Umožňuje zaměstnancům německé státní správy zpracovávat citlivá data na zařízeních

Nativně pro iOS a iPadOS bez nutnosti řešení doplňků od třetích stran

Schváleno pro Face ID a Touch ID



iPhone a iPad: první zařízení s certifikací NATO

Schváleno pro práci s utajovanými informacemi stupně „NATO Restricted“

Bezpečné použití bez nutnosti instalovat speciální vládní software

Špičkové šifrování a biometrie splňují nejnáročnější mezinárodní standardy



Case Study

Zdravotnická záchranná služba

vybrané kraje České republiky





0

výpadků hardware v průběhu
3 let

80%

snížení provozních požadavků
na IT

50%

snížení provozních nákladů
na energie

Apple Silicon — bezpečný díky
svému designu



Apple Business
Manager

MDM framework



Endpoint Security
framework

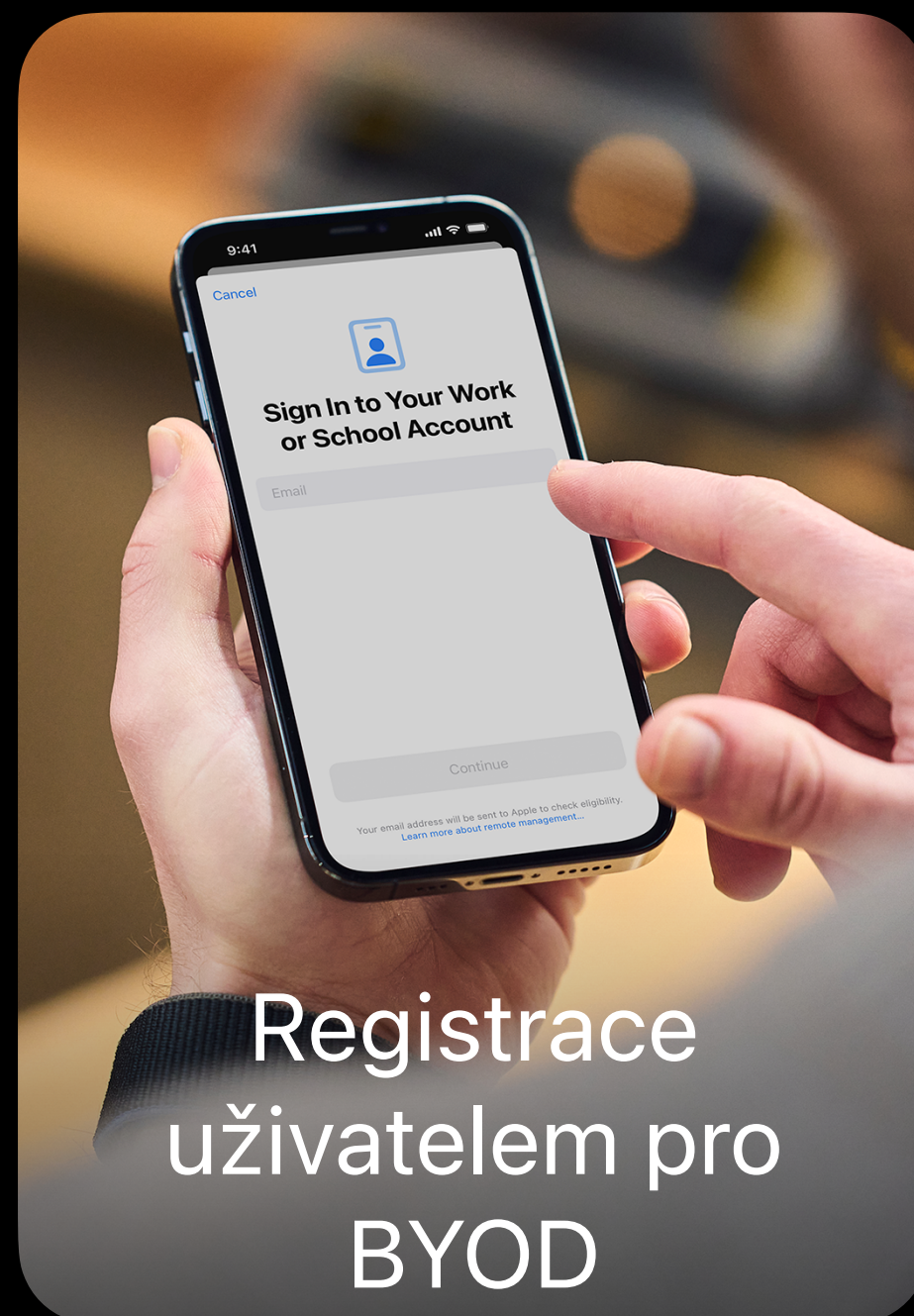


Zero-trust principy

Firemní bezpečnost



Správa aktualizací
systému



Registrace
uživatelů pro
BYOD



Passkeys jako
náhrada hesel



Ověření spravovaného
zařízení



Zero-touch nasazení



Integrace pro
jednotné přihlášení

iStores



Premium
Partner

B2B Enterprise Solutions