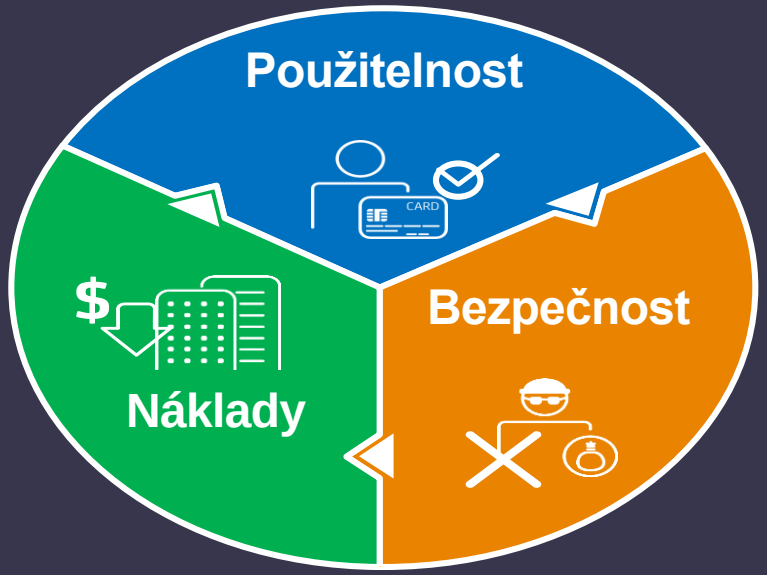
Silná autentizace a detekce fraudu (nejen) ve finančním sektoru – jak to udělat správně ☺

David Matějů
Senior Security Consultant

CA Expo 2018

Vývoj autentizace uživatelů (nejen) v bankovnictví

Uměním je vyvážit použitelnost, bezpečnost a náklady

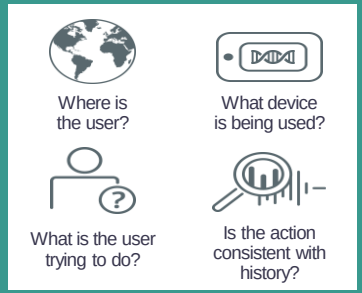


CA Advanced Authentication / CA Payment Security – 2 v 1

CA STRONG AUTHENTICATION

Identifikace uživatele použitím široké škály autentizačních metod

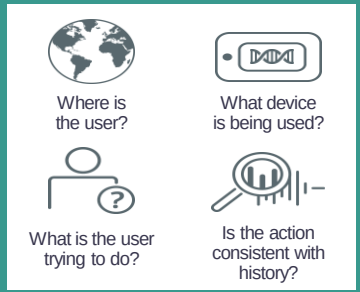
CA RISK AUTHENTICATION



Autentizace v reálném čase založená na analýze rizika dané operace / transakce

CA Risk Authentication / CA Risk Analytics

CA RISK AUTH / ANALYTICS



Autentizace v reálném čase založená na analýze rizika dané operace / transakce

Přínosy obě strany

- Neviditelné pro uživatele
- Behaviorální analýza na pozadí
- Adaptivní skóring rizika
- Dynamická pravidla
- DeviceDNA™ identifikace zařízení
- Významné snížení podvodných přihlášení a transakcí

CA Risk Authentication / CA Risk Analytics

CA RISK AUTH / ANALYTICS

OBSERVED

- Operating System
- System Language
- Time Zone Offset
- Monitor Details (11 characteristics)
- Browser Details (5 Characteristics)
- Plug-ins
- IE Plug-ins
- Camera/Microphone Presence
- Fonts
- Network IP Address
- Connection Type (LAN, Dial-up, etc.)
- CPU Model and Clock Speed
- Volume of Boot Partitions
- True IP Address of End-User System

CA RISK AUTH / ANALYTICS

DERIVED

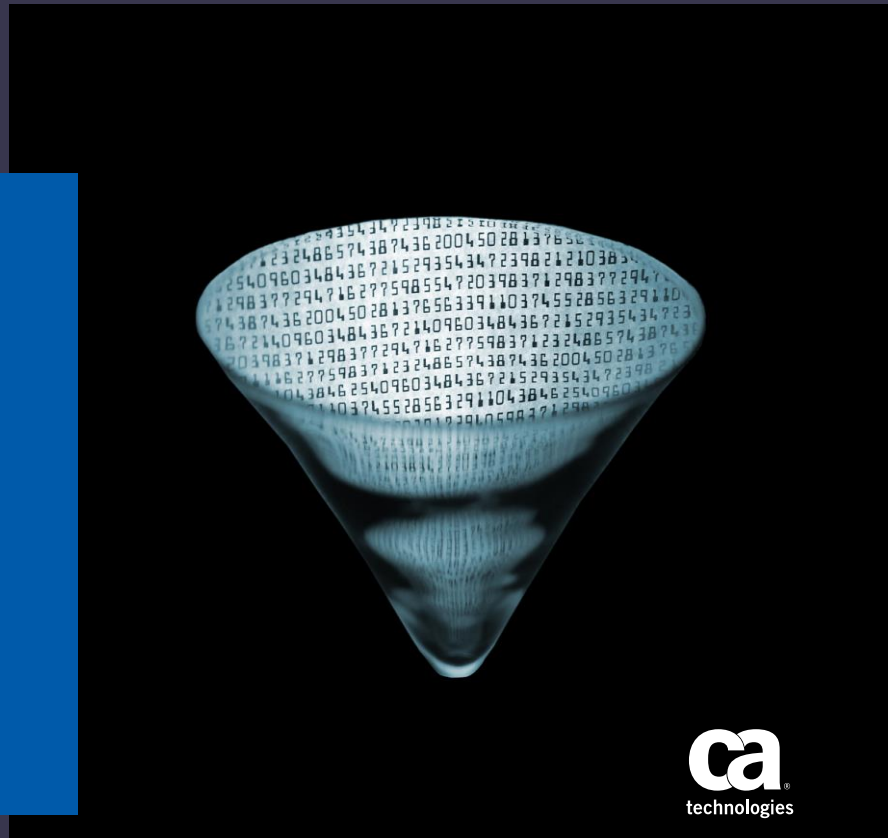
- Zone Hopping
- User Velocity
- Device Velocity
- User Previously Associated with Device
- New User or New Device
- Device Known, But New User at Device
- Negative IP
- Negative Device
- Trusted IP
- Trusted Device
- End-user geo location
- Anonymizing Proxy Check

CA Risk Auth / CA Payment Security – Neuronová síť

- Založeno na ***„Advanced machine learning techniques“***
- **Rozezná** legitimní od fraudulentního chování v kontextu každého uživatele
- Učí se v **reálném-čase**
- Vysoká **přesnost**, minimum tzv. „false-positives“
- Výsledkem je srozumitelné rizikové **skóre**

CA Risk Auth / CA Payment Security – Behaviorální model

- CA Model vybírá z tisíců komplexních proměnných a
  - detekuje v nich trendy,
  - podle historických dat na ně aplikuje další operace typu „dobře/špatně“,
- Pak vybere cca. 100 nejvlivnějších a ty použije pro oddělení legitimního a fradulentního chování.



CA Risk Auth / CA Payment Security – Pravidla

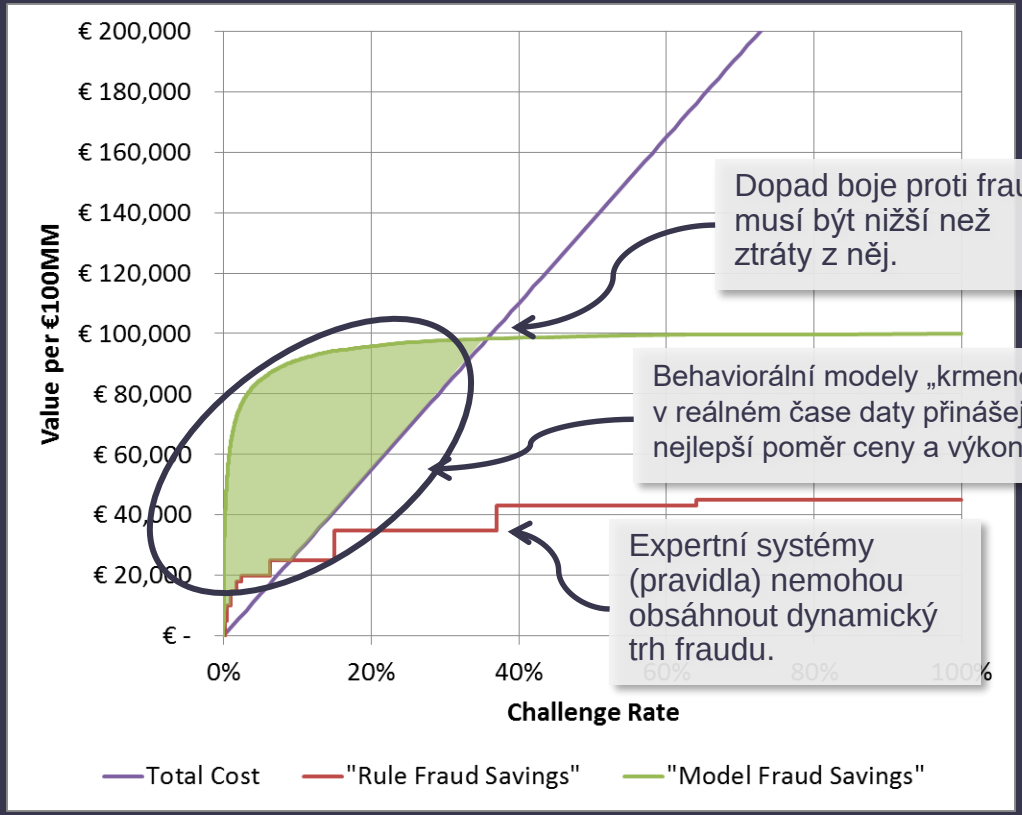
Cílí na známé typy útoku

Kritická pro vyhodnocení rizikového skóre

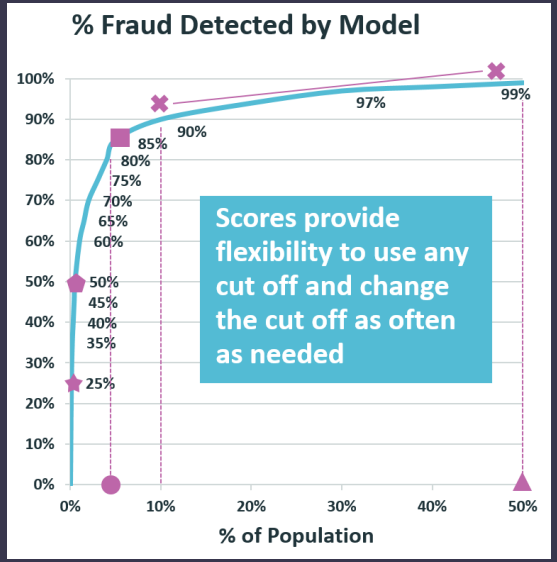
Okamžitá akce při vysokém riziku

Definice vlastních pravidel
Např. VIP, web, iOS / Android, externí / interní, …

Maximální detekce fraudu, minimální vliv na uživatele



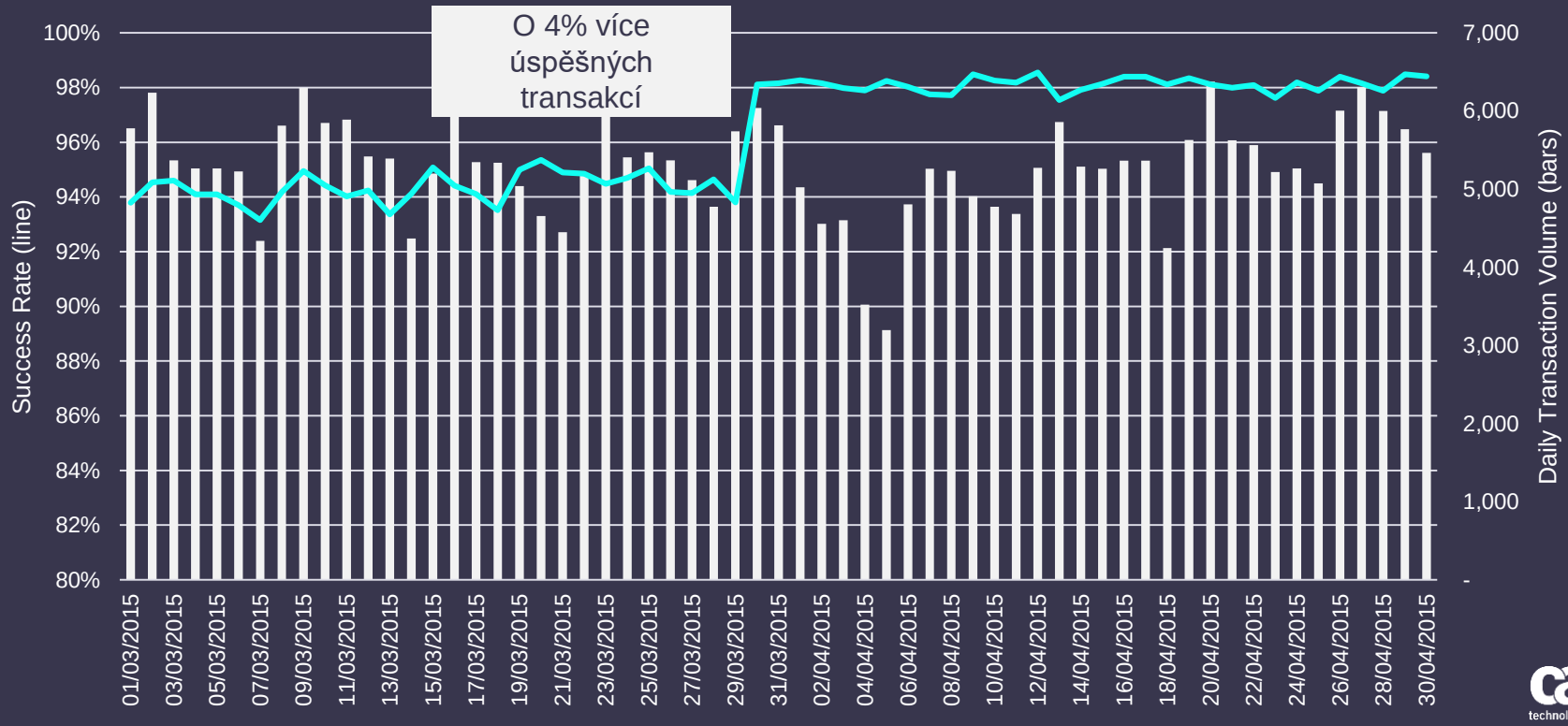
Výsledky behaviorálního modelu na potřebu sekundární autentizace



- **85%** podvodů je detekováno při sekundárním ověření pouhých **5%** uživatelů / klientů
- Další zvyšování **nad 5%** už přináší jen marginální výsledky
- Téměř 100% detekce podvodů již kolem **30%** sekundárním ověřování
- Při sekundárním ověřování pouhé **0.1%** uživatelů / klientů již detekujete kolem **25%** podvodů
- Při sekundárním ověřování pouhého **0.5%** uživatelů / klientů již detekujete kolem **50%** podvodů
- Zvýšením sekundárního ověření z **10%** na **50%** uživatelů / klientů detekujete jen o 9% více podvodů.

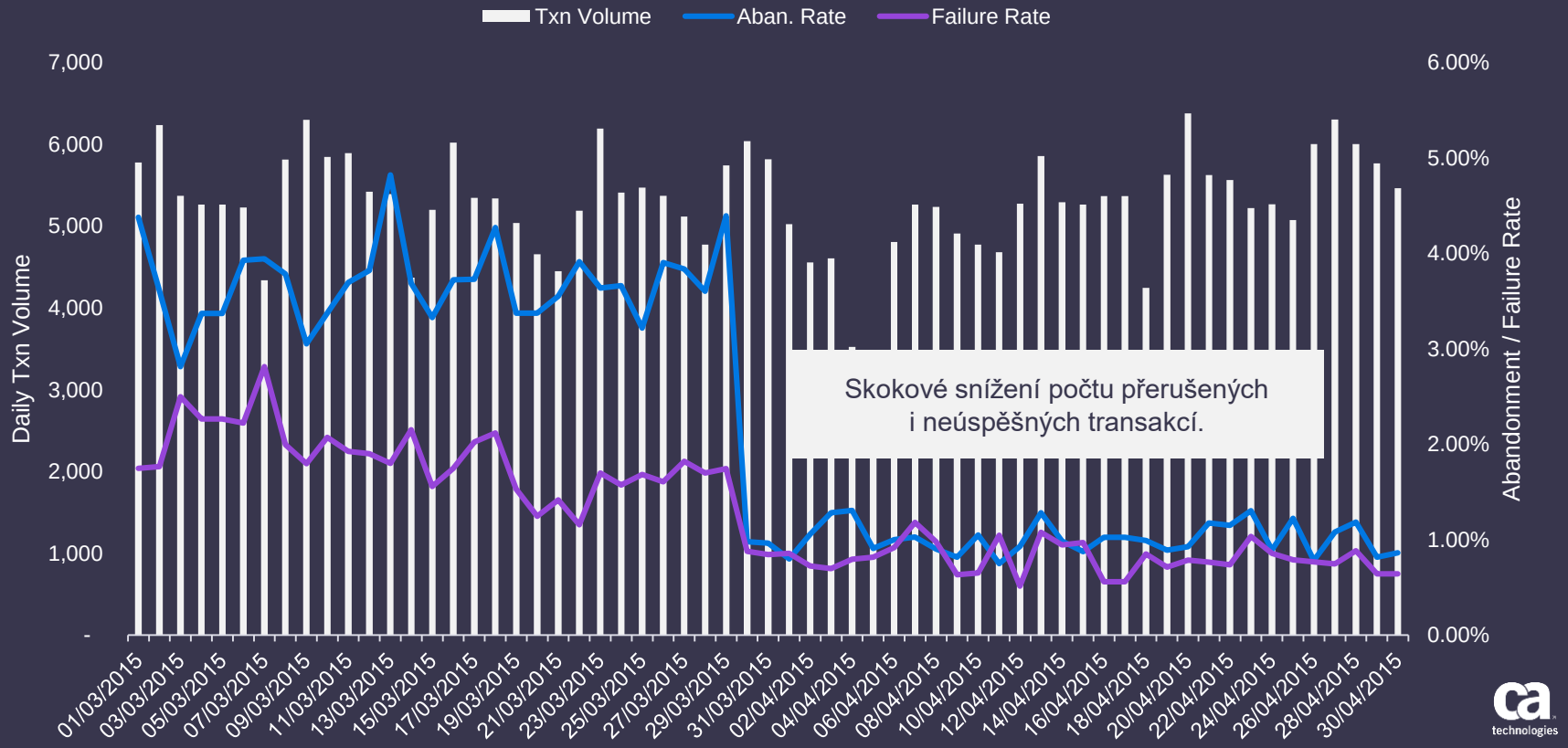
Reálná data – transakce CNP (card not present)

Risk-based autentizace zapnuta 30.3.2015



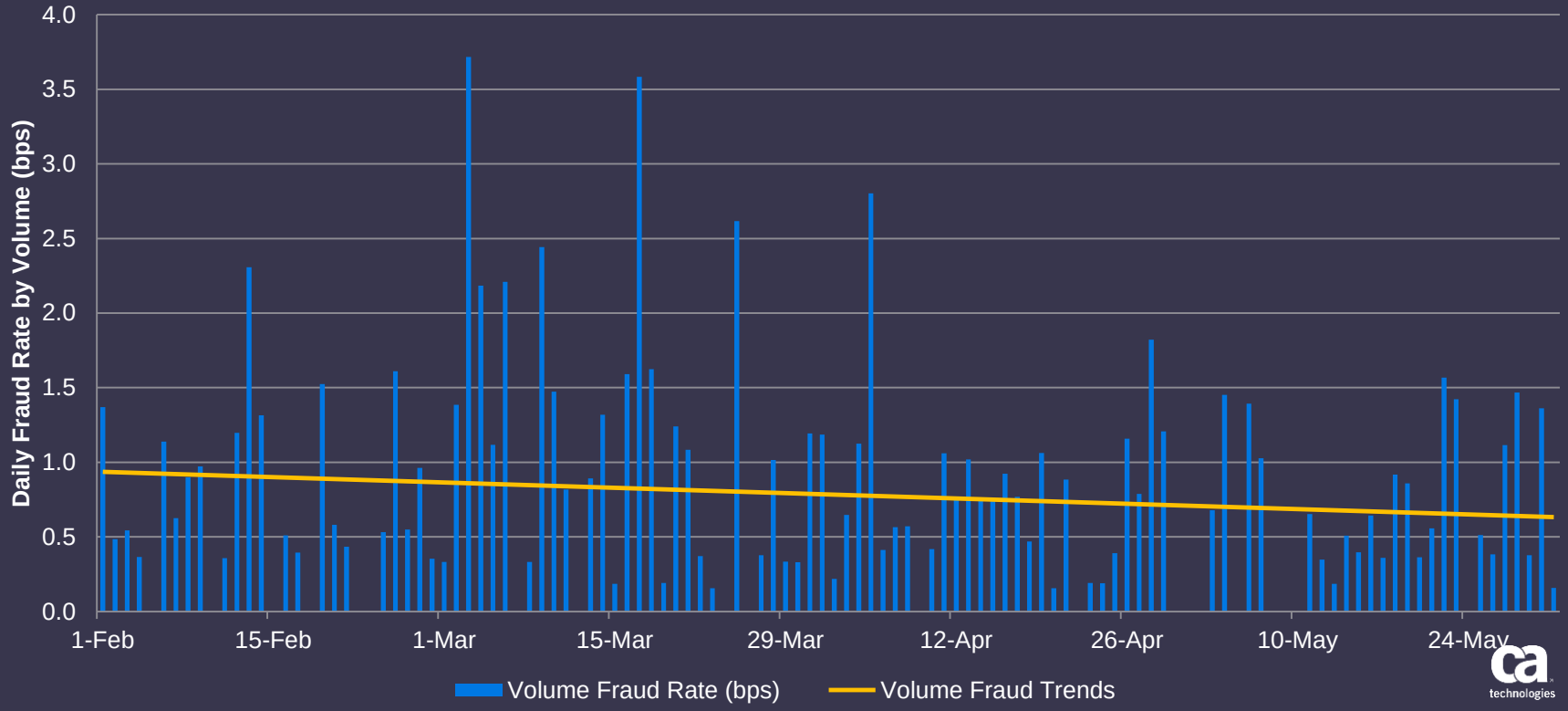
Reálná data – transakce CNP (card not present)

Risk-based autentizace zapnuta 30.3.2015

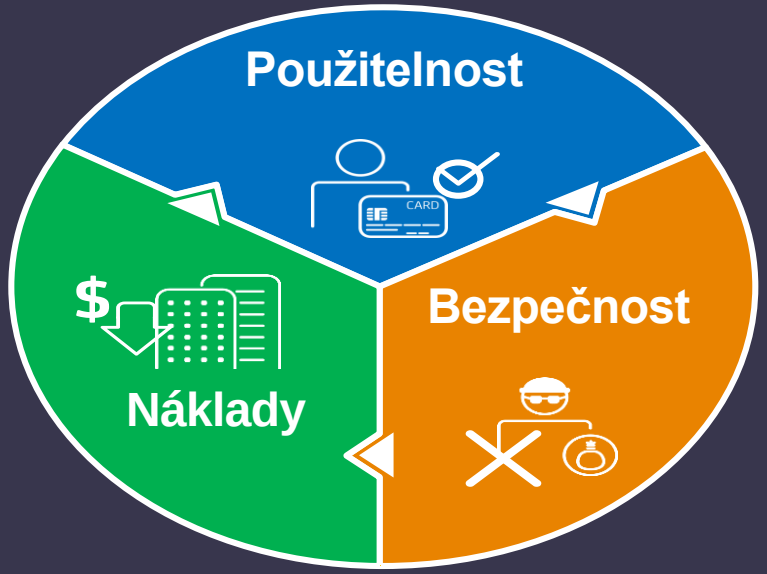


Reálná data – transakce CNP (card not present)

80% snížení sekundárního ověření bez nárůstu fraudu



CA Advanced Authentication – web, mobile, IoT
CA Payment Security – 3D Secure



ca technologies

Děkuji za pozornost!

David Matějů
Senior Security Consultant
david.mateju@contractor.ca.com


@cainc


slideshare.net/CAInc


linkedin.com/company/ca-technologies

ca.com