

SÉCURISEZ VOS CONNEXIONS  
AVEC

okta



Capsule d'apprentissage

Mercredi 9 décembre 2020

Christian Boulet, Architecte technologique  
Accrédité OKTA Presales Proficient

# ESI, votre partenaire informatique au Québec

En affaires depuis 1994!

- Environ 200 spécialistes de différents créneaux (réseau, stockage, sécurité, données, virtualisation, informatique, gestion de projet, architecture d'affaires, etc.)
- Bureaux à Montréal, Québec et Toronto
- Partenaire de plusieurs manufacturiers de solutions technologiques
- Partenaire de plusieurs fournisseurs de solutions informatiques et d'hébergement
- Entreprises affiliées :



# ESI et Okta

Toujours à la recherche de solutions pour nos clients

- Résultat d'analyses et de recommandations de nos consultants
- En lien avec nos priorités et notre mission :
  - > Protéger les données et aider nos clients à le faire
  - > Gérer les identités efficacement
  - > Recommander les solutions de haut calibre
- ESI est partenaire ELITE d'Okta



# Ce que nous voyons chez nos clients

La transformation numérique est incontournable  
Les risques sont omniprésents



Les entreprises subissent le fardeau  
d'infrastructures vieillissantes



AD/LDAP

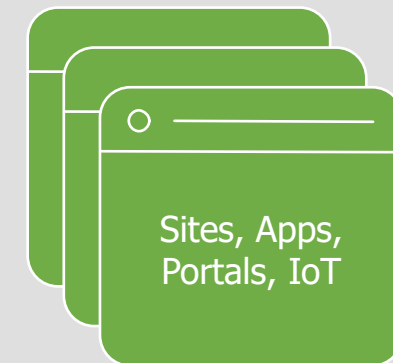
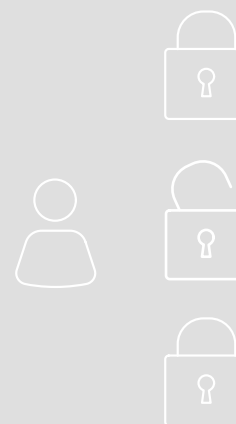
RADIUS

Provisioning

ADFS

WAM

L'identité des consommateurs  
est fragmentée



Sites, Apps,  
Portals, IoT

# La situation actuelle est ... tendue...



## Près de 50 000 comptes piratés à l'Agence du revenu du Canada cet été

Beaucoup plus de personnes qu'on le croyait à l'origine ont été victime de cette intrusion informatique.

🕒 17 septembre | [Cybercriminalité](#)



## L'Ordre des infirmières de l'Ontario victime d'une cyberattaque

L'instance dirigeante des infirmières en Ontario a suspendu certains services en ligne après une cyberattaque.

🕒 17 septembre | [Santé](#)



## Une attaque informatique cible des hôpitaux canadiens et américains

Le ministère de la Santé du Québec fait partie des victimes de cette campagne de demande de rançon.

🕒 29 octobre | [Santé](#) | [Cybercriminalité](#) | [Informatique](#) | [Coronavirus](#)



## Vol de données massif à la Sûreté du Québec

Un ancien sous-traitant informatique a été victime d'une attaque par rançongiciel.

🕒 28 octobre | [Cybercriminalité](#)



## la cyberattaque

Saint-Jean a beaucoup de travail à faire pour rétablir ses systèmes informatiques, selon un expert.

🕒 16 novembre | [Cybercriminalité](#) | [Cybersécurité](#) | [Affaires municipales](#)



## cyberattaque

Les systèmes informatiques ont dû être débranchés et de nombreux services en ligne interrompus.

🕒 16 novembre | [Technologies et médias](#) | [Politique municipale](#)

# Les attaques ciblent l'identité



81%

Des brèches de données ont impliqué des identifiants volés ou faciles à deviner



91%

Des attaques d'hameçonnage ont ciblé des identifiants



73%

Des mots de passes ne sont pas uniques...

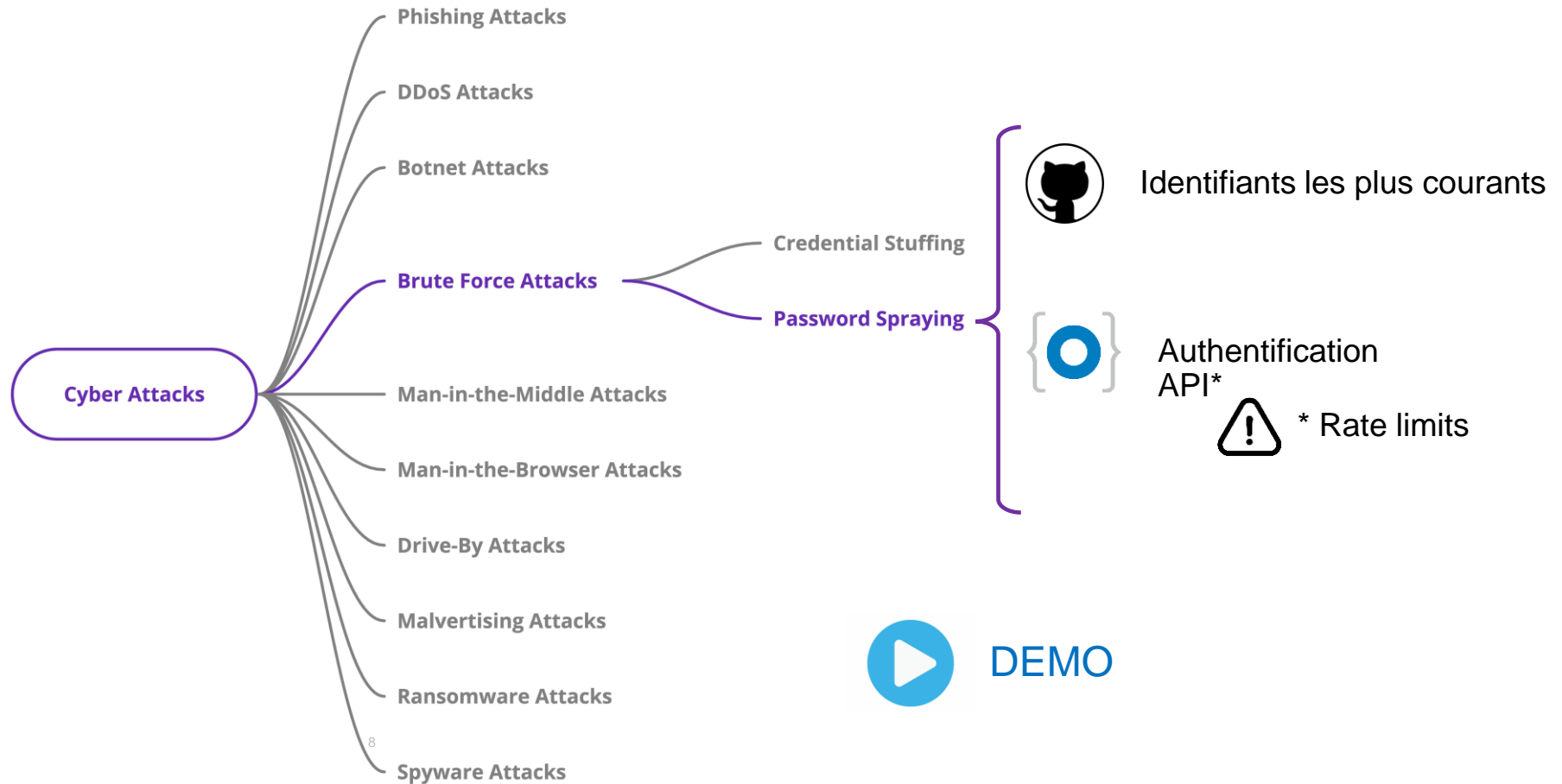
La collecte d'identifiants est la tactique la plus profitable pour les groupes de menaces

*Source: 2017 Verizon Data Breach Investigations Report*

*Source: 2016 Verizon Data Breach Investigations Report*

*Source: TeleSign 2016 Consumer Account Security Report*

# Les cyberattaques les plus communes



# Combien de temps pour trouver un mot de passe?

Length of Password (Characters)	Numbers Only	Mixed Lower and Upper Case Alphabets	Mixed Numbers, Lower and Upper Case Alphabets	Mixed Numbers, Lower and Upper Case Alphabet, and Symbols
3	Instant	Instant	Instant	Instant
4	Instant	Instant	Instant	Instant
5	Instant	Instant	3 secs	10 secs
6	Instant	8 secs	3 mins	13 mins
7	Instant	5 mins	3 hours	17 hours
8	Instant	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hours	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36 bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years



# Protections offertes contres les attaques par force brute

## → Politique de mot de passe

- > Exigences de complexité
- > Automatismes de verrou



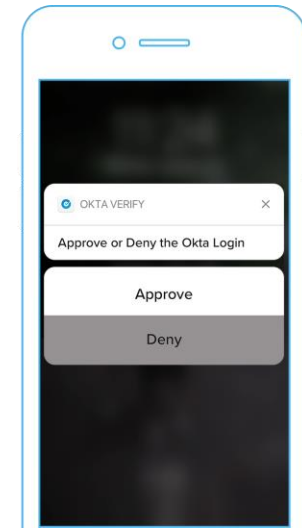
## → Liste noire d'IP malveillantes

- > Verrouillage du réseau par zone
- > Automatisation avec ThreatInsight



## → Authentification multifactorielle (MFA)

- > Ajout des politiques MFA
- > Adoption de l'authentification sans mot de passe



# La clé du succès : MFA partout et en tout temps



Authentification  
sécuritaire



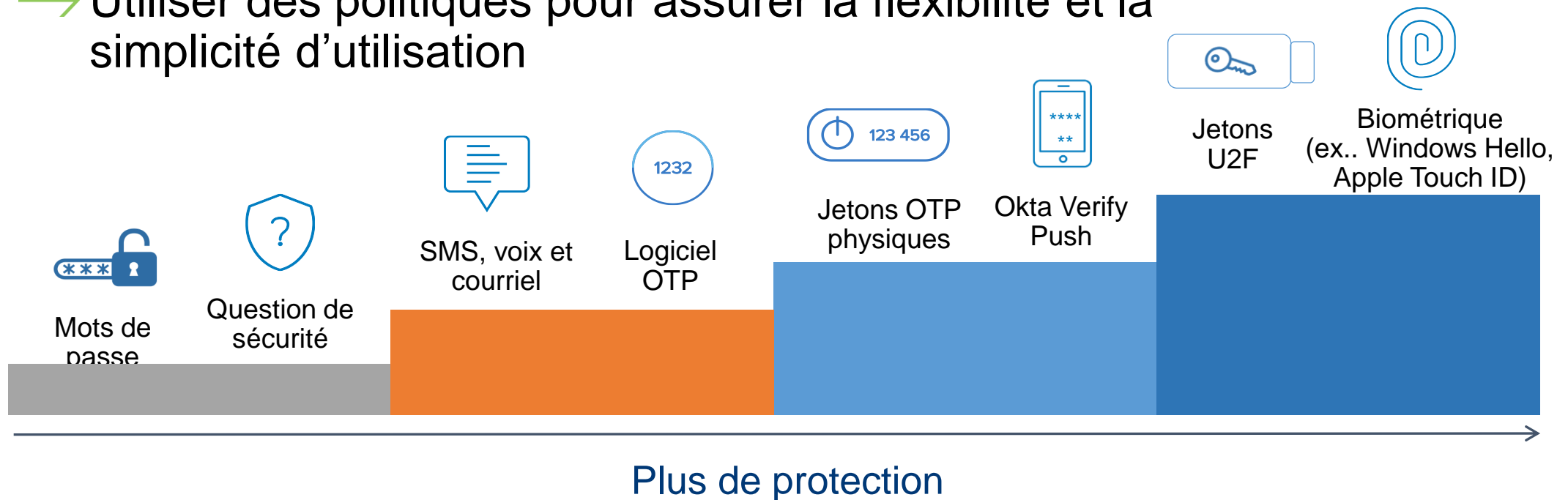
Facile à utiliser



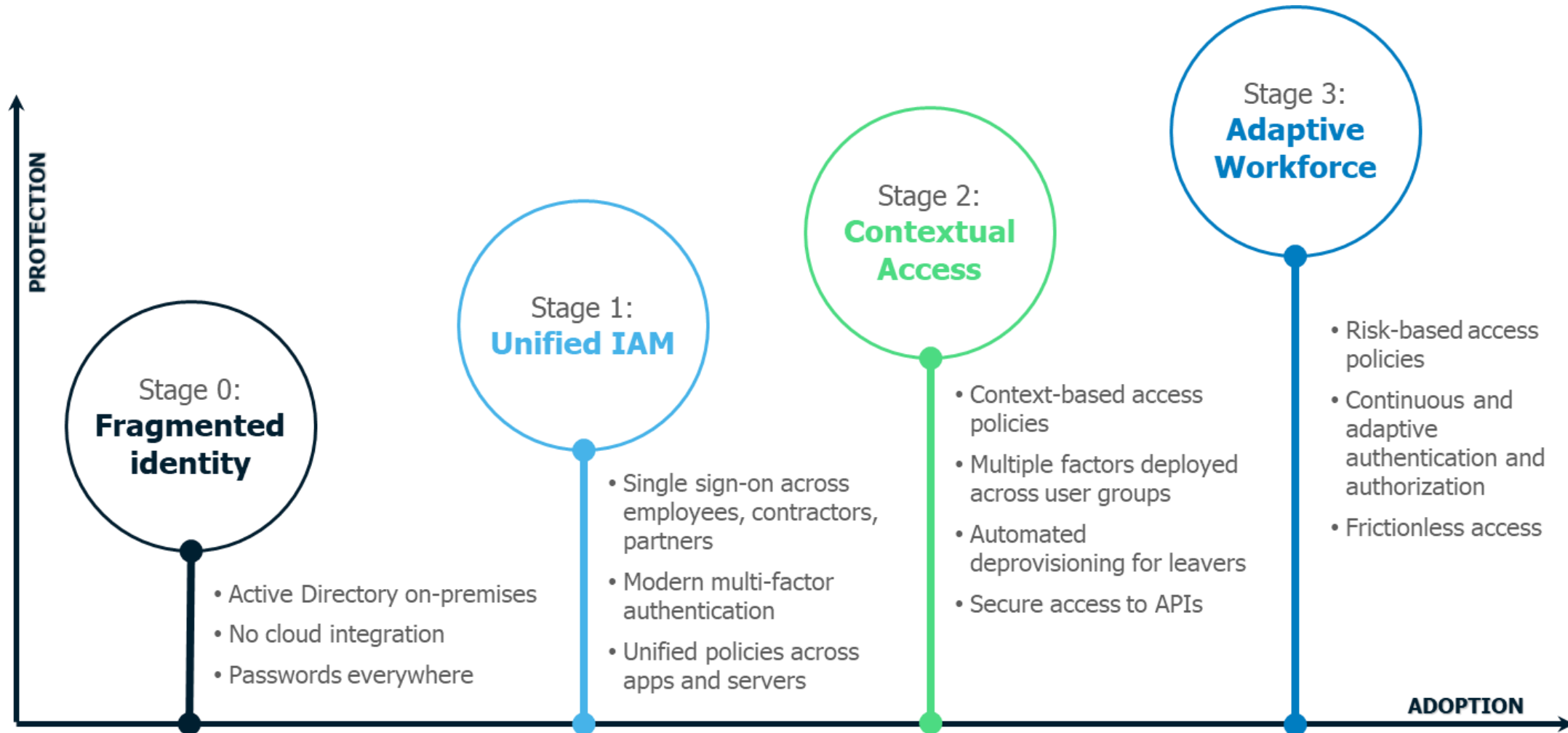
Extensible

# Nos organisations doivent concilier la sécurité avec la simplicité d'utilisation...

- Plusieurs facteurs selon le degré d'assurance requis
- Permettre la paramétrisation selon les cas d'utilisation
- Assurer le respect des règles et des lois
- Utiliser des politiques pour assurer la flexibilité et la simplicité d'utilisation



# Courbe de maturité « Zero Trust »



# Prochaines étapes

- Osez remettre en question les méthodes et outils en place
- Cherchez à mettre en place du SSO
  - > Qui fonctionne sur le plus d'outils possible
- Assurez-vous que :
  - > Le MFA est actif pour tous et partout
  - > Les pratiques « Zero Trust » sont connues et qu'un plan est construit
  - > Les décideurs sont conscients des risques actuels et de vos protections

# Pour terminer...

- Okta = Solution simple et très efficace
  - > Leader selon Gartner et Forrester
- Choisir des standards et les meilleures pratiques
  - > Oauth2 - OpenID
  - > Zero Trust – SSO
- Contactez ESI
  - > Votre partenaire de confiance!

A group of business professionals are gathered around a conference table in a meeting room. A man in a dark suit is pointing at a laptop screen, while others look on attentively. The scene is dimly lit, with a blue and green color cast. The text "Période de questions" is overlaid on the left side of the image.

Période de questions