SECURE YOUR CONNECTIONS WITH okta

ESi TECHNOLOGIES

Learning Capsule

Wednesday December 9 2020

Emmanuel Latour, Senior Solutions Consultant

ESI, our cloud partner based in Canada

Founded in 1994!

Partnerships with many technology manufacturers and cloud providers

- About 200 specialists in different areas:
  - Networking
  - Storage
  - Security
  - Data
  - Virtualization
  - Cloud
  - Project Management
  - Business Management Consulting
- Offices in Toronto, Montréal and Québec City
- Affiliated companies:

OCTOPUS

sais Interconnexion inc.

Civatree

ESI & Okta

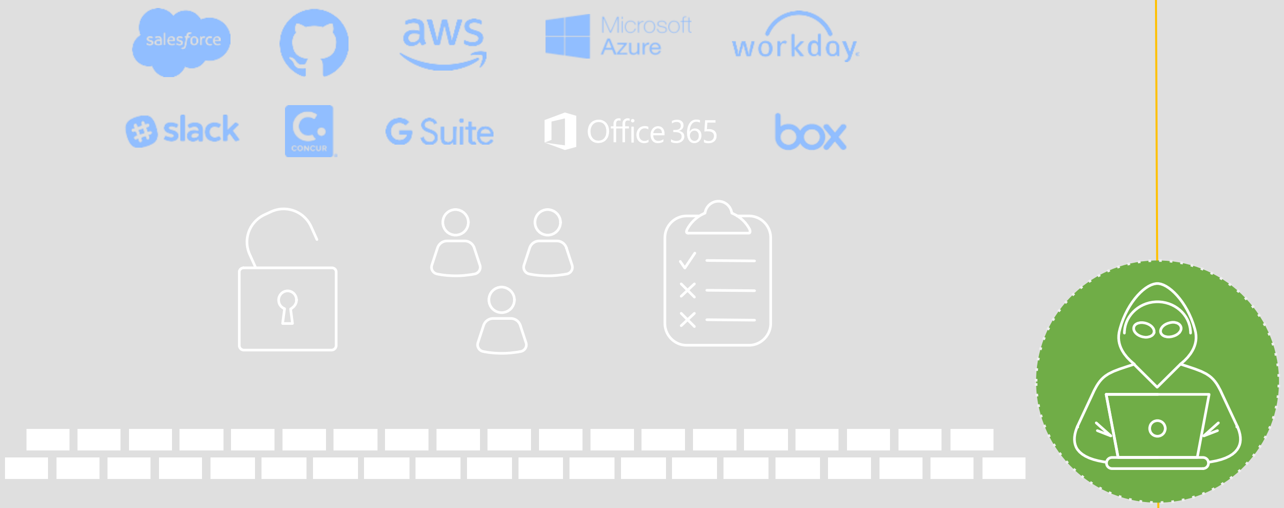
Always providing solutions for our clients

- Results from analysis and recommendations by our consultants
- In line with our corporate priorities
  - Help our clients protect their data
  - Efficiently manage identities
  - Recommend effective & high quality solutions
- ESI Technologies is an Okta ELITE Level Partner

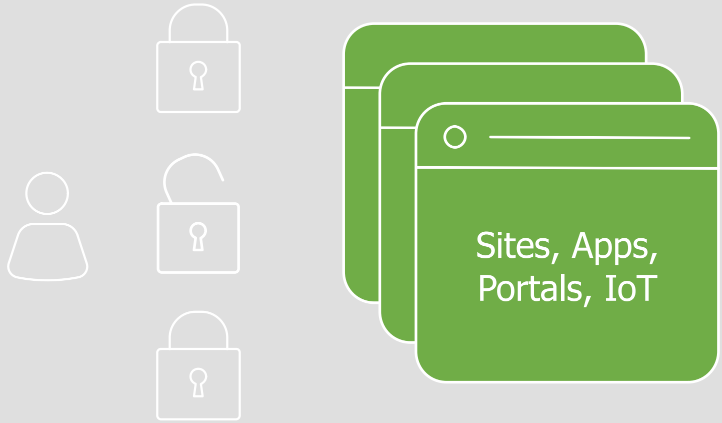
okta ELITE SOLUTION PROVIDER

What we’re seeing with our clients

Digital transformation is unavoidable
Risks are pervasive



User identities are fragmented



Entreprises carry the burden of their legacy infrastructure baggage

AD/LDAP

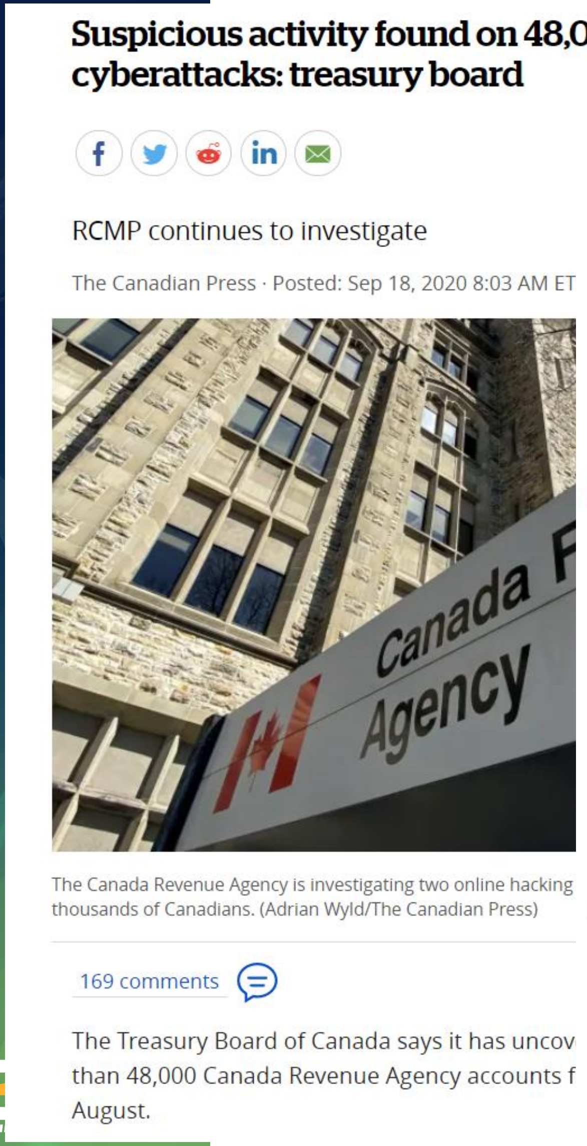
RADIUS

Provisioning

ADFS

WAM

Security is top of mind



Suspicious activity found on 48,000 CRA accounts after cyberattacks: treasury board

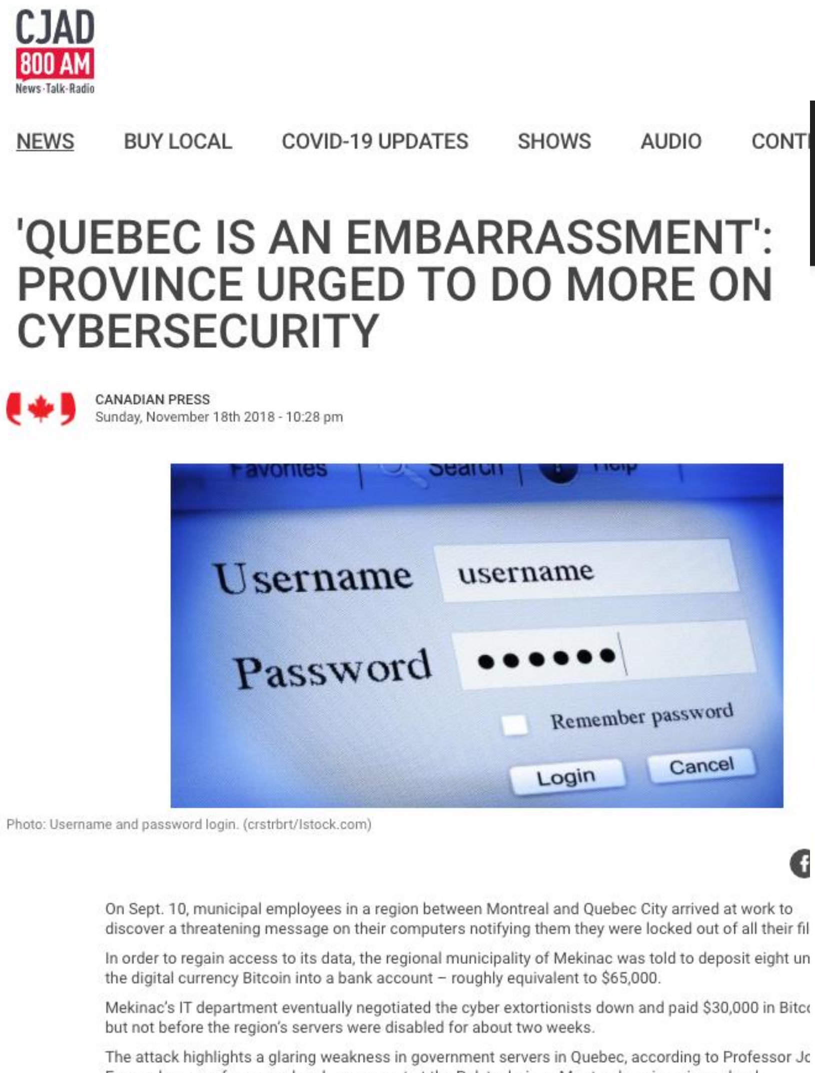
RCMP continues to investigate

The Canadian Press · Posted: Sep 18, 2020 8:03 AM ET

The Canada Revenue Agency is investigating two online hacking thousands of Canadians. (Adrian Wyld/The Canadian Press)

169 comments

The Treasury Board of Canada says it has uncov than 48,000 Canada Revenue Agency accounts f August.



CJAD 800 AM News·Talk·Radio

NEWS BUY LOCAL COVID-19 UPDATES SHOWS AUDIO CONT

'QUEBEC IS AN EMBARRASSMENT': PROVINCE URGED TO DO MORE ON CYBERSECURITY

CANADIAN PRESS
Sunday, November 18th 2018 - 10:28 pm

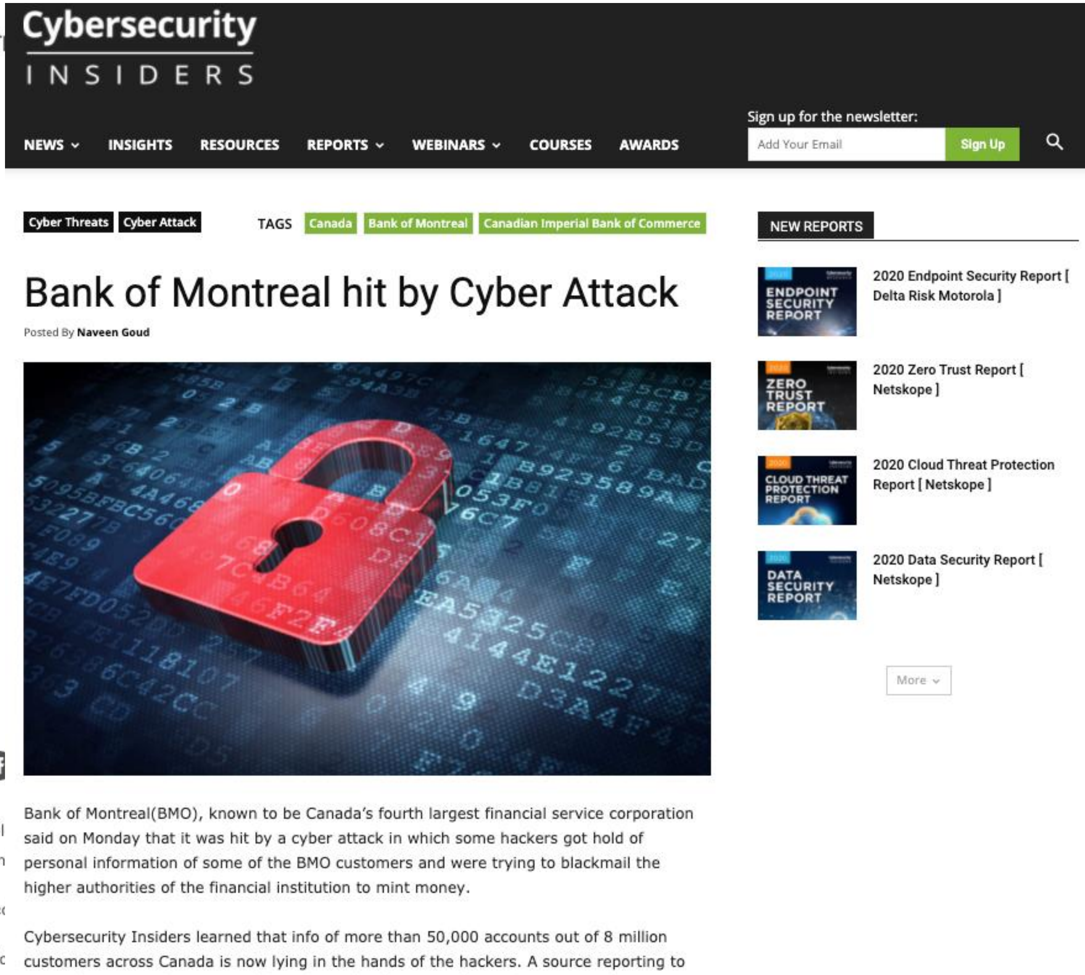
Photo: Username and password login. (crstrbrt/Istock.com)

On Sept. 10, municipal employees in a region between Montreal and Quebec City arrived at work to discover a threatening message on their computers notifying them they were locked out of all their fil

In order to regain access to its data, the regional municipality of Mekinac was told to deposit eight un the digital currency Bitcoin into a bank account – roughly equivalent to $65,000.

Mekinac's IT department eventually negotiated the cyber extortionists down and paid $30,000 in Bitc but not before the region's servers were disabled for about two weeks.

The attack highlights a glaring weakness in government servers in Quebec, according to Professor Jc



Cybersecurity INSIDERS

NEWS INSIGHTS RESOURCES REPORTS WEBINARS COURSES AWARDS

Sign up for the newsletter: Add Your Email Sign Up

Cyber Threats Cyber Attack TAGS Canada Bank of Montreal Canadian Imperial Bank of Commerce

Bank of Montreal hit by Cyber Attack

Posted By Naveen Goud

Bank of Montreal(BMO), known to be Canada's fourth largest financial service corporation said on Monday that it was hit by a cyber attack in which some hackers got hold of personal information of some of the BMO customers and were trying to blackmail the higher authorities of the financial institution to mint money.

Cybersecurity Insiders learned that info of more than 50,000 accounts out of 8 million customers across Canada is now lying in the hands of the hackers. A source reporting to

NEW REPORTS

2020 Endpoint Security Report [Delta Risk Motorola]

2020 Zero Trust Report [Netskope]

2020 Cloud Threat Protection Report [Netskope]

2020 Data Security Report [Netskope]

More

Cyber attacks target credentials

81%

of data breaches involve stolen/weak credentials

91%

of phishing attacks target credentials

73%

of passwords are duplicates

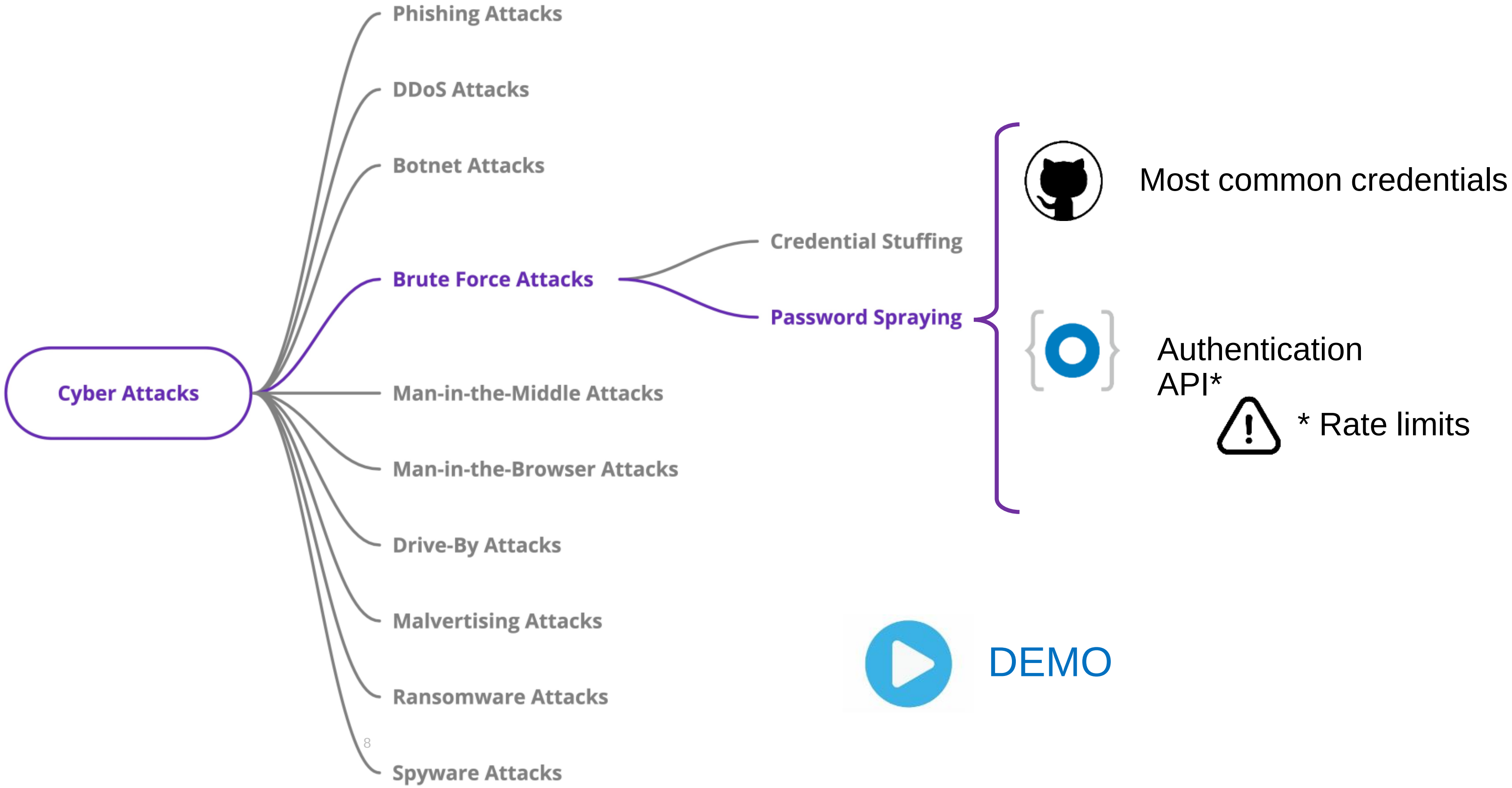
Credential harvesting is the most fruitful tactic for today's threat actors

Source: 2017 Verizon Data Breach Investigations Report

Source: 2016 Verizon Data Breach Investigations Report

Source: TeleSign 2016 Consumer Account Security Report

Most common types of cyber attacks



Cyber Attacks

Phishing Attacks

DDoS Attacks

Botnet Attacks

Brute Force Attacks

Credential Stuffing

Password Spraying

Most common credentials

Authentication API*

* Rate limits

Man-in-the-Middle Attacks

Man-in-the-Browser Attacks

Drive-By Attacks

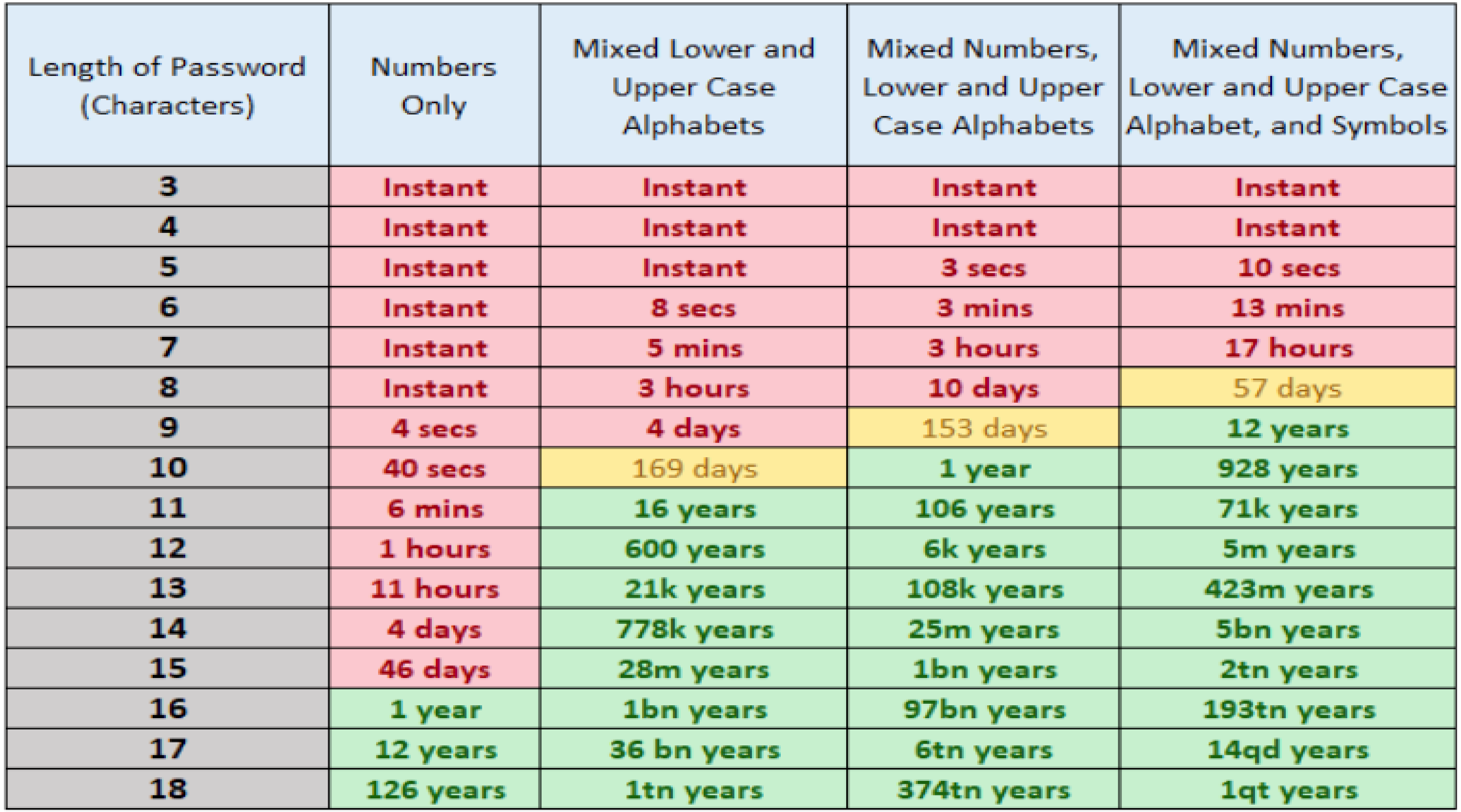
Malvertising Attacks

Ransomware Attacks

Spyware Attacks

DEMO

How long it would take to crack your password ?



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 over brute force attacks

→ Password policy

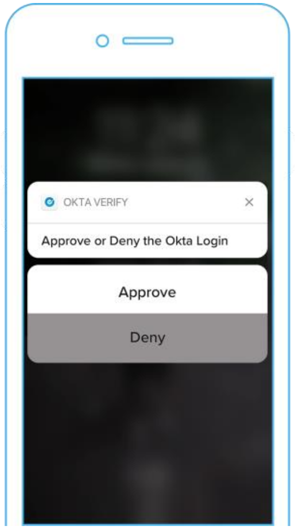
- Account lockouts
- Complexity requirements

→ Blacklisting malicious IP

- Network action
- Automation with ThreatInsight

→ Multi-factor authentication

- Add multi-factor policy
- Adopt passwordless authentication



OKTA VERIFY

Approve or Deny the Okta Login

The key is MFA everywhere

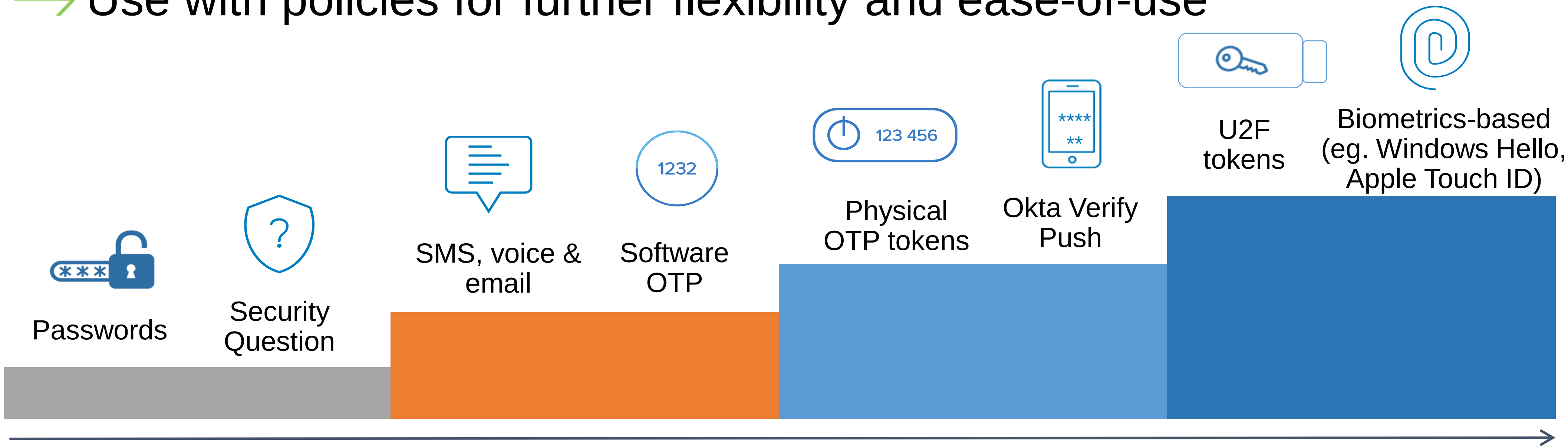
Secure authentication

Simple to use

Extensible

Organizations must also balance security with usability

- Comprehensive set of factors with full range of assurance levels
- Allows for customization to fit different use cases
- Ensures compliance with regulations
- Use with policies for further flexibility and ease-of-use



Passwords

Security Question

SMS, voice & email

Software OTP

Physical OTP tokens

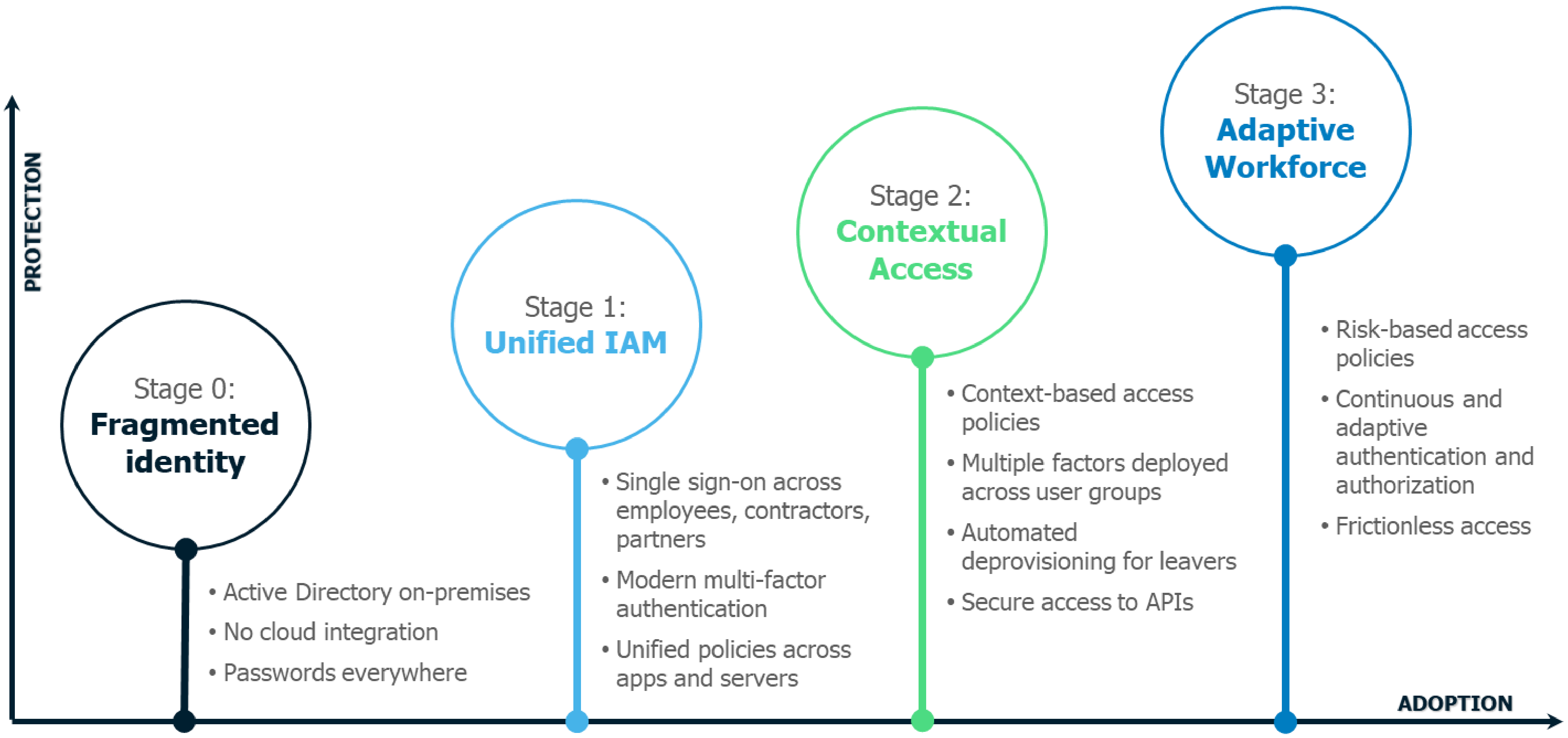
Okta Verify Push

U2F tokens

Biometrics-based (eg. Windows Hello, Apple Touch ID)

Plus de protection

Zero Trust Maturity Curve



Stage 0: **Fragmented identity**

- Active Directory on-premises
- No cloud integration
- Passwords everywhere

Stage 1: **Unified IAM**

- Single sign-on across employees, contractors, partners
- Modern multi-factor authentication
- Unified policies across apps and servers

Stage 2: **Contextual Access**

- Context-based access policies
- Multiple factors deployed across user groups
- Automated deprovisioning for leavers
- Secure access to APIs

Stage 3: **Adaptive Workforce**

- Risk-based access policies
- Continuous and adaptive authentication and authorization
- Frictionless access

Next steps

→ Dare to question the processes and tools in place

→ Look to implement SSO

- Supports most of the tools/apps as possible

→ Ensure that:

- MFA is enabled for everyone and everywhere
- Zero Trust practices are known and that a plan has been developped
- Decision makers are conscious of the current risks and your defenses in place

In conclusion…

→ Okta = Easy and very effective solution

- A market leader as per Gartner & Forrester

→ Follow standards and best practices

- Oauth2 - OpenID
- Zero Trust – SSO

→ Contact ESI

- Your trusted partner!

Question Period