CYBERSECURITY IN THE NEW NORMAL

CYBER SECURITY CONFERENCE 2020 VIRTUAL EDITION

KEVIN PEUHKURINEN
Principal Research Director – Security, Risk & Compliance

INFO-TECH RESEARCH GROUP

ASIA PACIFIC / SCIENCE & HEALTH

Outbreak of SARS-like pneumonia being investigated in China

AFP-JIJI

 Dec 31, 2019

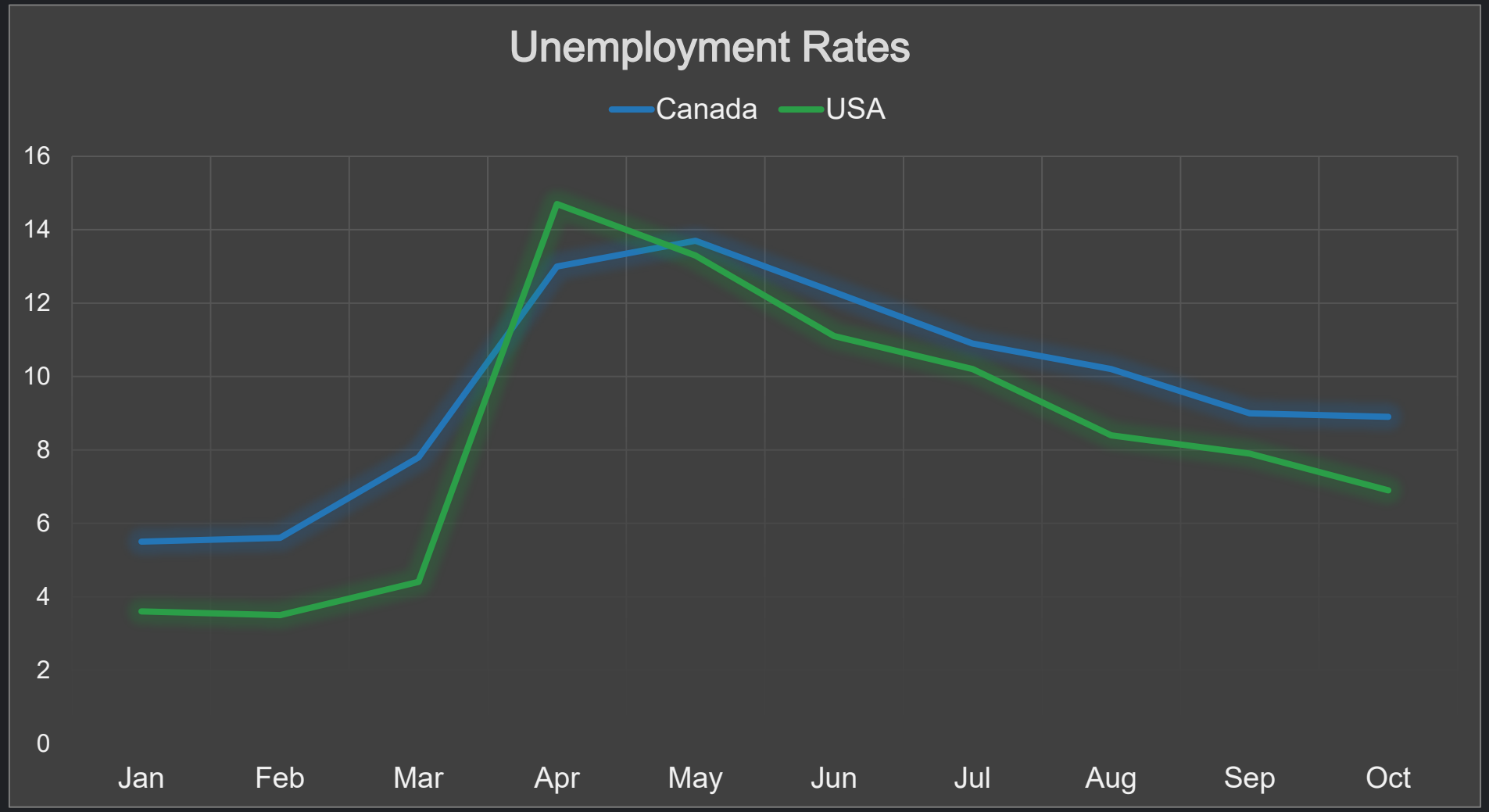
BEIJING – China is investigating an outbreak of atypical pneumonia that is suspected of being linked to severe acute respiratory syndrome (SARS), the flu-like virus that killed hundreds of people in the early 2000s, state media reported Tuesday.

A team of experts from the National Health Commission were dispatched Tuesday to Wuhan, in central China's Hubei province, and are "currently conducting relevant inspection and verification work," state broadcaster CCTV reported.

An emergency notification issued Monday by the Wuhan Municipal Health Committee said hospitals

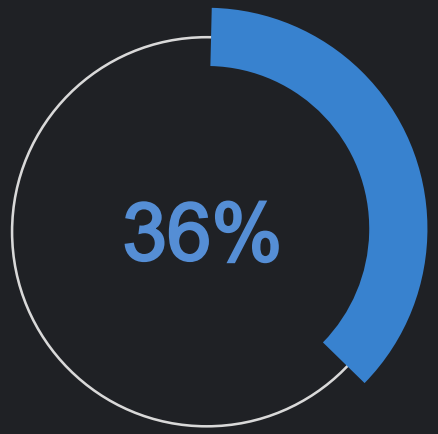
The New Insider Threat

The New Unemployed

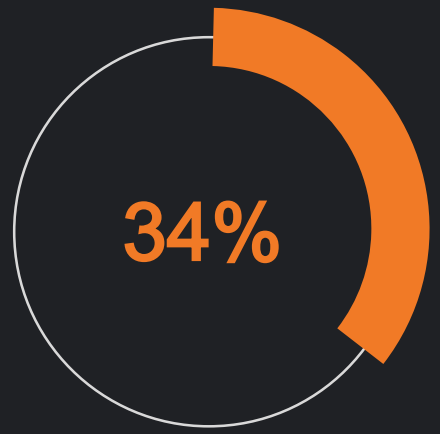


Source: Statistics Canada, Trading Econom

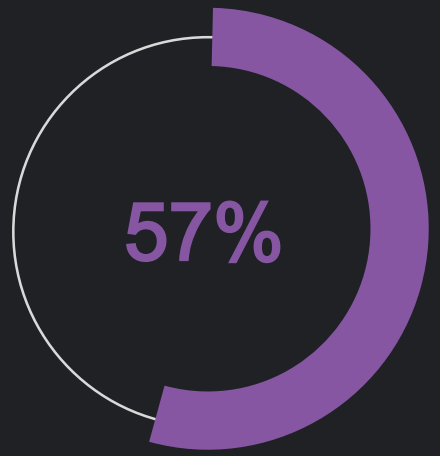
The New Freelancers



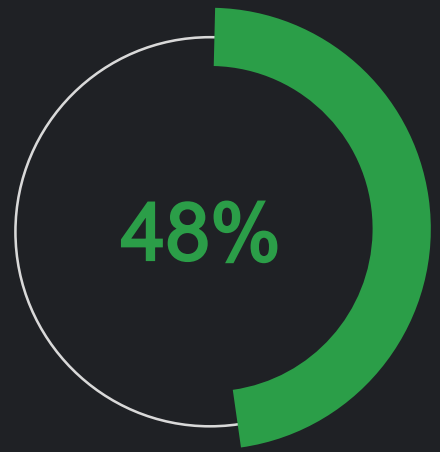
% of US Workers freelancing



% of freelancers who started due to pandemic



% of new freelancers providing skilled services

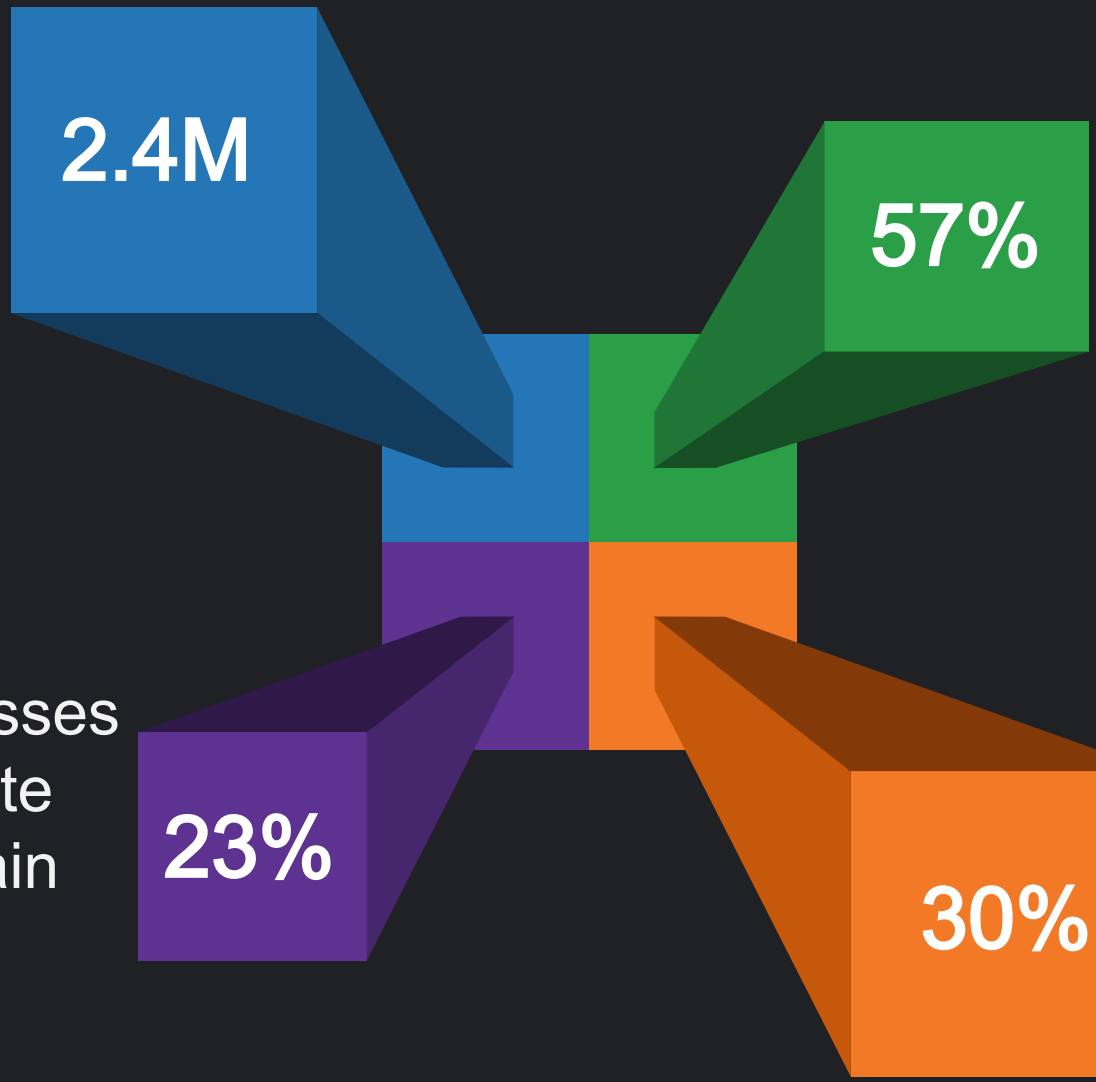


% of new freelancers who see freelancing as a long-term solution

Source: Upwork

The New Remote Work Normal

More Canadians working from home in October 2020 vs 2019



Businesses that do not include remote work risks in their security awareness program

Canadian businesses that expect remote working will remain normal post - pandemic

Security incidents caused by insider threats

Source: Statistics Canada, Ponemon, Verizon

The New Insider Threat

Economic Downturn

Resulting in layoffs and inability to hire new full-time staff.

Remote Workforce

Resulting in staff who are no longer within the security perimeter.

Corporate Gig Economy

Resulting in influx of new, untrusted freelancers to corporate workforce.

Ineffective Awareness

Resulting in a need to re-think security awareness for a remote workforce.

The End of Endpoint Protection

The Old Normal

- MALICIOUS CODE PROTECTION
- USER BEHAVIOR MONITORING
- DATA LOSS PREVENTION
- MANAGED RESPONSE

- HOST-BASED IDS/IPS
- PATCH MANAGEMENT
- APPLICATION CONTROL
- CONFIGURATION MANAGEMENT

The Old Normal

$12 Billion USD

Global endpoint protection market in 2019

Source: Fortune Business Insight

Endpoints in the New Normal

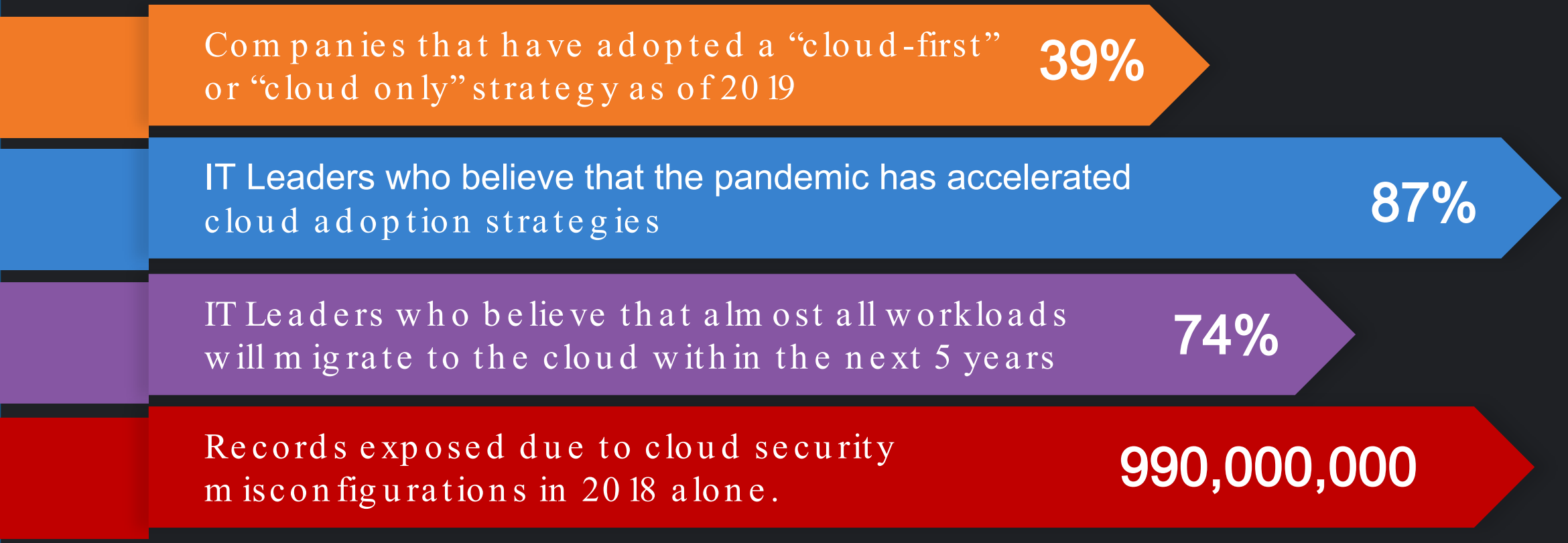
Rush to enable work-from-home forced many organizations to accept BYOD

Adoption of permanent remote workforce likely to also make BYOD permanent

Slow death of VPN removes ability to enforce even basic endpoint security controls

Data Centers without Data

The Dark Cloud Around the Silver Lining



Source: LogicMonitor, IBM

Data in the New Normal

Accelerated Cloud Adoption

Data not protected by IT Security

Accelerated BYOD

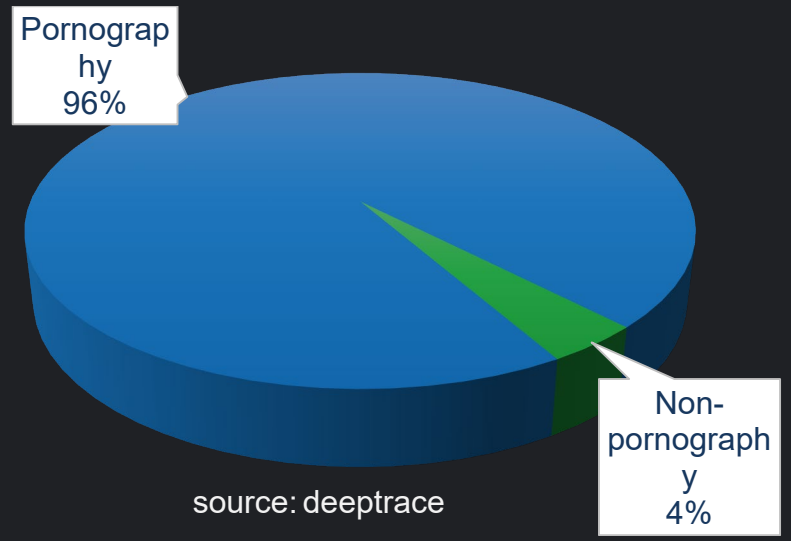
Data accessed by untrusted devices

Accelerated Remote Work

Data accessed by untrusted people

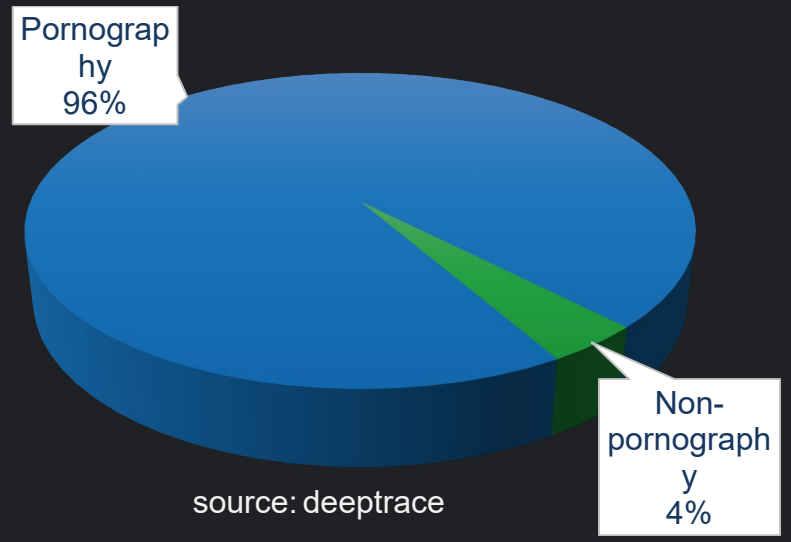
Wildcard Threat: Deepfake and Video Conferencing

96% of all online deepfake videos are pornographic in nature



source: deeptrace

96% of all online deepfake videos are pornographic in nature



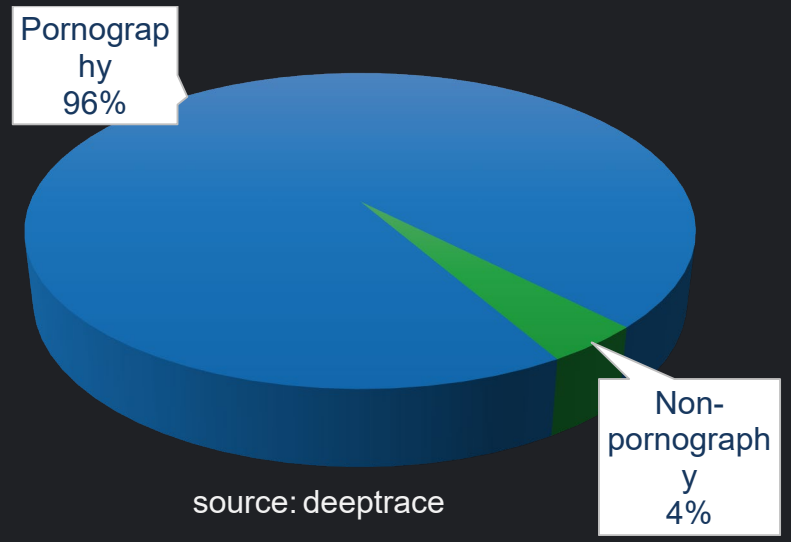
source: deeptrace

$243,000

amount stolen using synthetic voice audio in one 2019 incident

source deeptrace

96% of all online deepfake videos are pornographic in nature



source: deeptrace

$243,000

amount stolen using synthetic voice audio in one 2019 incident

source deeptrace

$68,000,000

spent by US defense on deepfake detection technology in 2018

source futurism.com

$10,000,000

contributed by Facebook for the 'Deepfake Detection Challenge'

source: facebook

Recommendations

Identify Internal Strategies

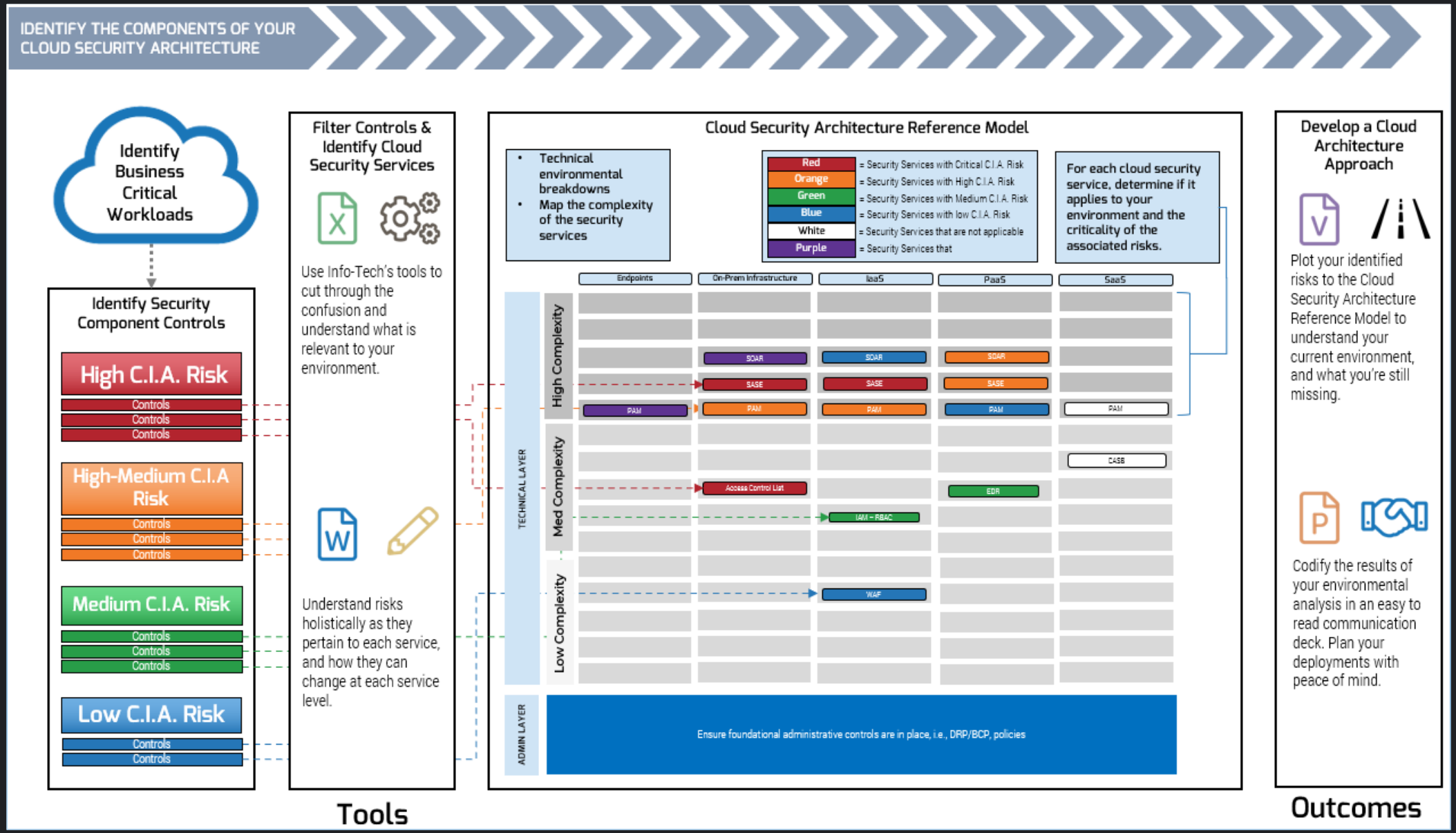
PLANS FOR USE OF FREELANCERS

REMOTE WORK STRATEGIES

BYOD STRATEGIES

CLOUD ADOPTION PLANS

Build a Cloud Security Architecture



Create a Data-Centric Security Strategy

Update Your Security Awareness Program

- FOCUS ON DATA SECURITY
- REMOTE WORK RISK TRAINING
- DEEPFAKE AWARENESS

Thank you!

Questions?

kpeuhkurinen@infotech.com