DIGITAL TRANSFORMATION WEBCAST SERIES

Secure and Stable Technology

August 6, 2020

RSM

Your presenters

Karen Wiltgen

Principal

Karen.Wiltgen@rsmus.com

- Strategy & Management Consulting
- National consulting leader for Professional Services and Business Services
- National leader for Digital Strategy

Mike Reiring

Director

Mike.Reiring@rsmus.com

- Southeast Region Leader - IT Managed Services and Infrastructure
- Florida Leader – Technology Consulting

Maria Phillips

Manager

Maria.Phillips@rsmus.com

- Risk Consulting – Security and Privacy
- National Center for Excellence for Professional Services and Business Services

Agenda

Topic
Digital Strategy Overview
What does secure and stable mean?
Application delivery
Identity
Secure endpoints
Privacy
Educated and suspicious workforce
Wrap-up and Q&A

Learning objectives

By the end of this session, you will:

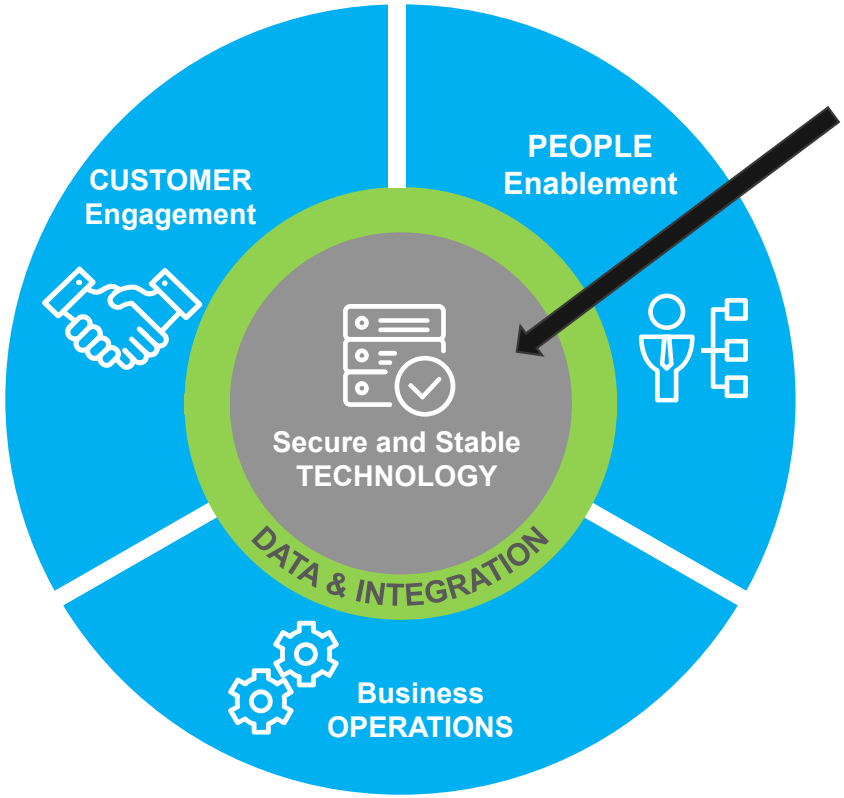
- Gain an understanding of a Digital Strategy framework
- Understand technology trends in the professional and business services industry
- Be able to describe challenges and solution options for security and privacy
- Become familiar with infrastructure solutions to drive digital transformation

DIGITAL STRATEGY: OVERVIEW

Setting the stage for transformation

How We View Digital Transformation

Digital is not just about technology – its about how an organization can use technology to enable and reach their goals.



Secure and Stable Technology

All of the people, processes and systems necessary to maintain the systems, infrastructure and security.

Customer Engagement

How you leverage technology to engage your customers and external stakeholders.

Business Operations

Using the right technologies and systems to transform how you operate, creating higher levels of efficiency and accuracy in day-to-day activities.

People Enablement

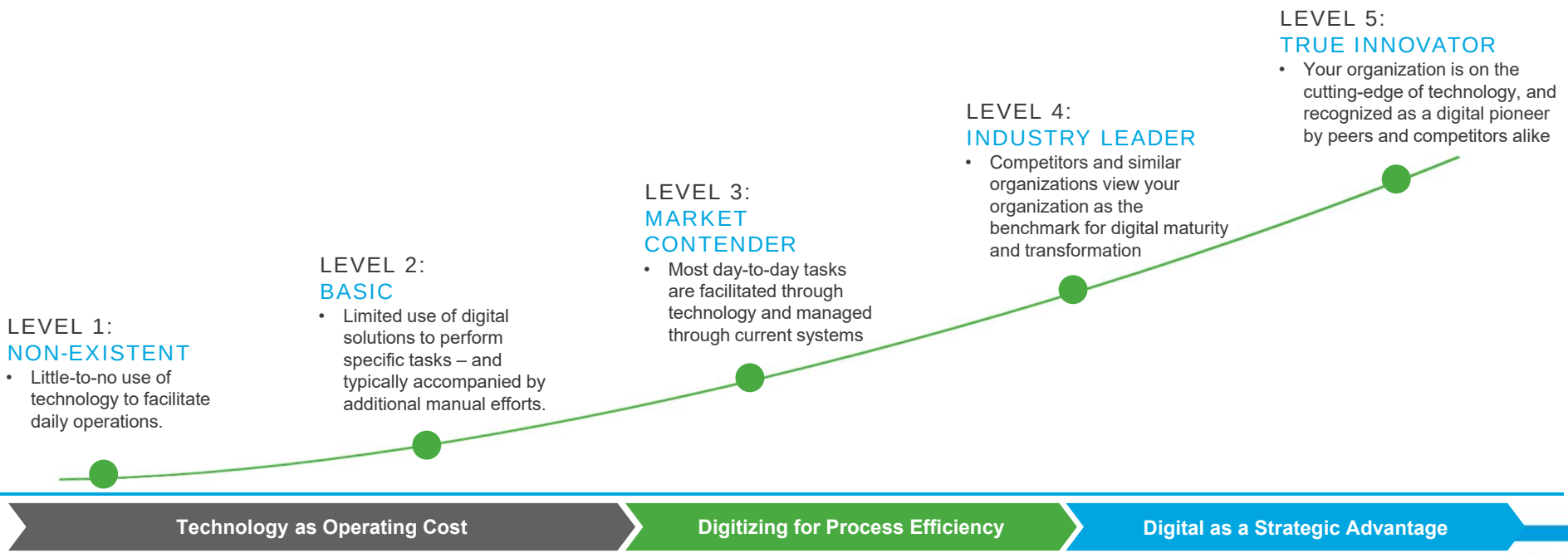
Giving your teams the digital tools, capabilities and culture to be more effective and increase value contribution on a regular basis.

Data & Integration

Capturing and using data to create better insights, deliver more personalized experiences and improve decision making .

The Digital Journey - Where are you & where do you need to be?

A key output of the Digital Strategy Roadmap is determining the target level of maturity for each domain that is needed to support your business strategy



Digital Capabilities – Executive Survey

As part of the executive survey, RSM asked middle market executives to identify the key digital technologies being discussed at their firms

Digital Transformation Priorities

Primary Responses:

- **Enterprise Mobility**
- **Mobile Technologies**
- **Artificial Intelligence (AI)**

Other Notable Responses:

- Cloud
- Blockchain
- Data & Analytics
- ERP
- Cyber Security
- Robotic Process Automation (RPA)
- CRM
- Digital Marketing
- Internet of Things (IoT)

Source: RSM Digital Transformation 2 (DT2) Study, November 2019

WHAT DOES SECURE AND STABLE MEAN?

2020 table stakes

Apps Delivered Where and When Needed

- Always On VPN
- Application Proxy
- Cloud App Delivery
- Virtual Desktops / Remote Apps

Identity Management

- Single Sign On
- Conditional Access
- Multifactor Authentication
- Identity Governance
- Self Service Password Resets

Secure Endpoints

- Comprehensive Patching
- Vulnerability Management
- Endpoint Detection and Response
- Data Loss Prevention

Privacy

- Privacy Training
- Understand your Responsibilities
- Regular Monitoring / Assessments
- Contractual Obligations

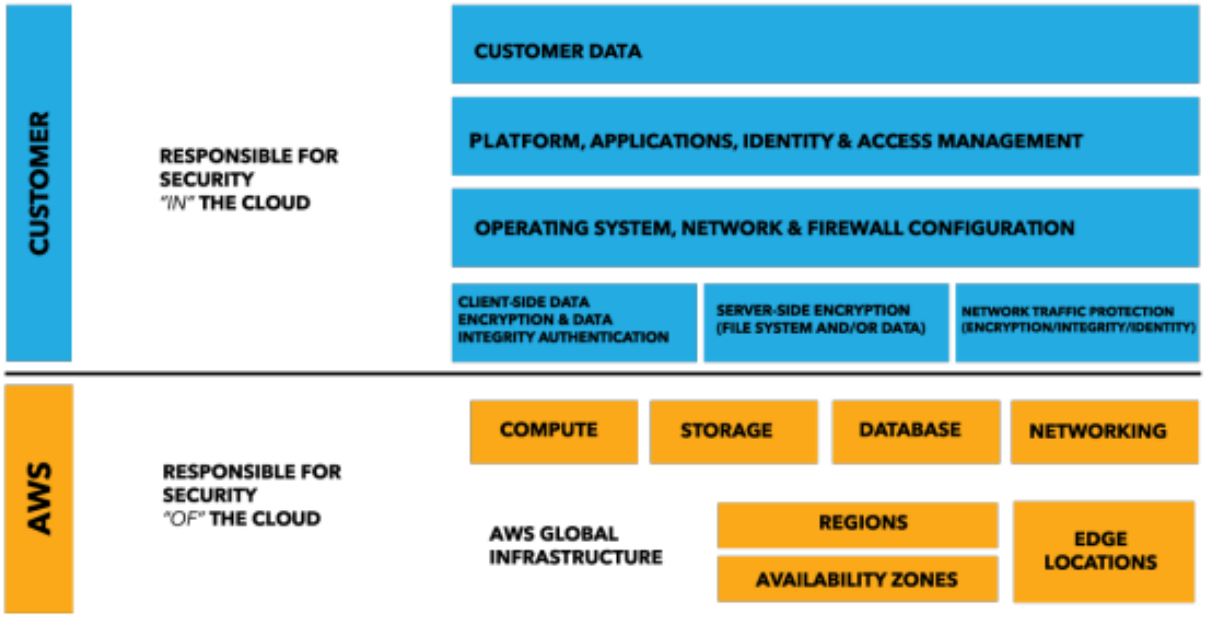
Educated and Suspicious Workforce

- Security and Awareness Training
- Measure Effectiveness
- Culture of Awareness
- Manage Shadow IT

APPLICATION DELIVERY

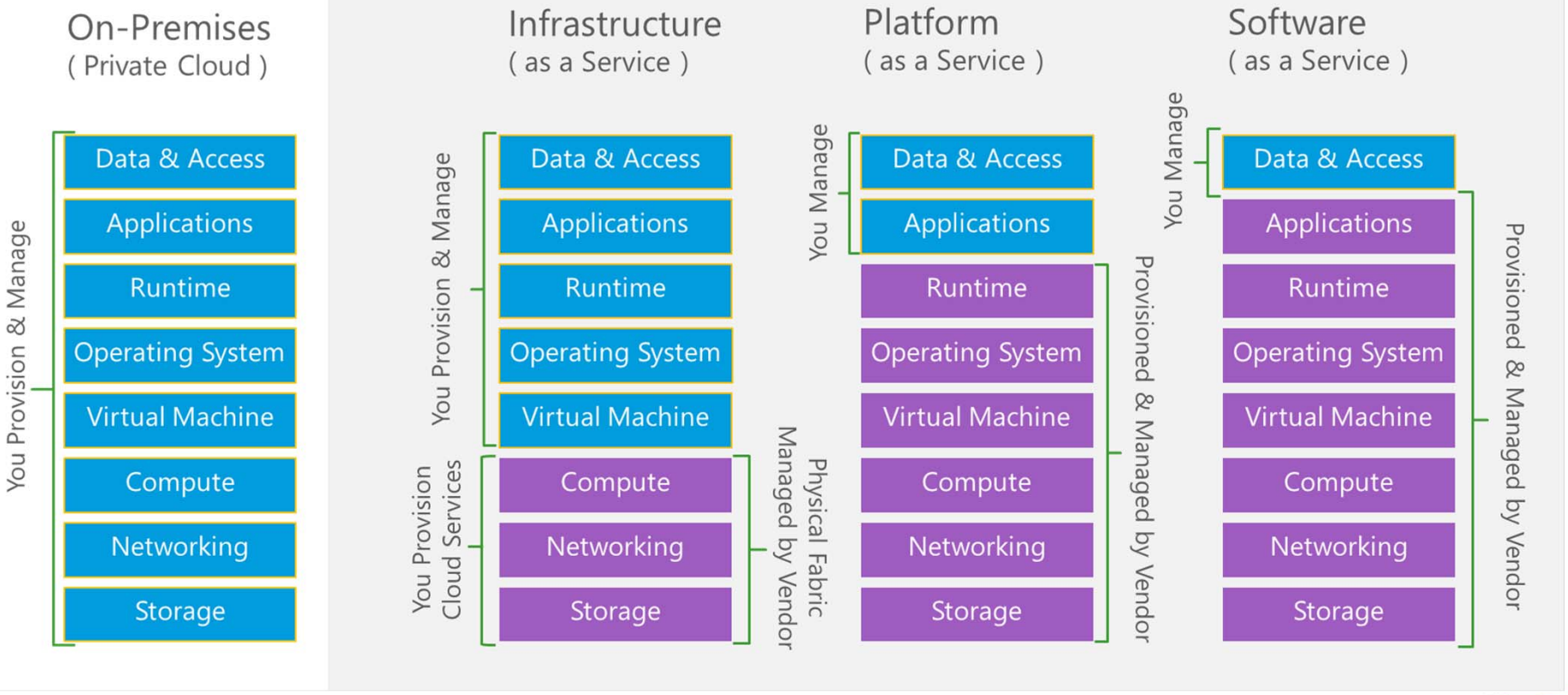
Increased secure access in a mobile and remote environment

Cloud and security



All cloud providers utilize a shared responsibility model

On Prem vs Cloud Responsibilities



 |

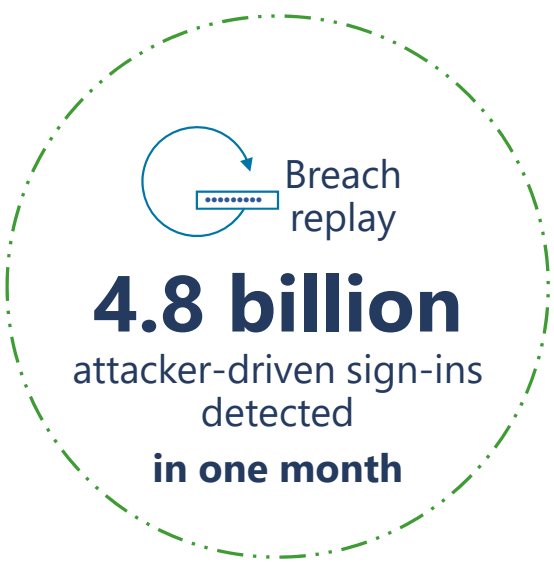
IDENTITY

Strengthening stable environment

FM1

Why identity matters

Data tells us the frequency and intensity of attacks is rising



81% of network intrusions are due to compromised user credentials!

Slide 15

FM1 What is the source of this slide?
Franko, Matt, 7/28/2020

Authentication…something you KNOW

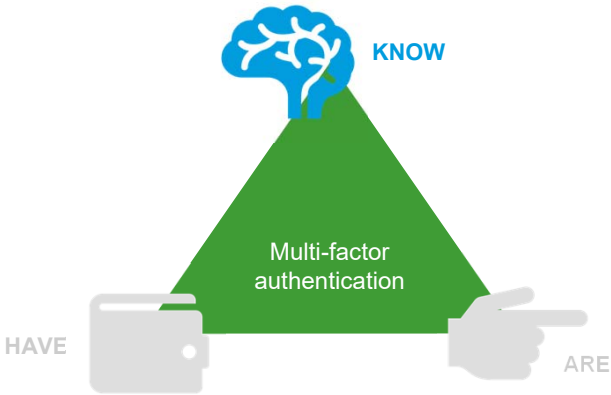
Username and Password

Pros:

- Simple
- Built into various solutions

Cons:

- Can be shared
- Can be compromised
  - Breach
  - Brute force
  - Social engineering
  - Phishing



Authentication…something you ARE

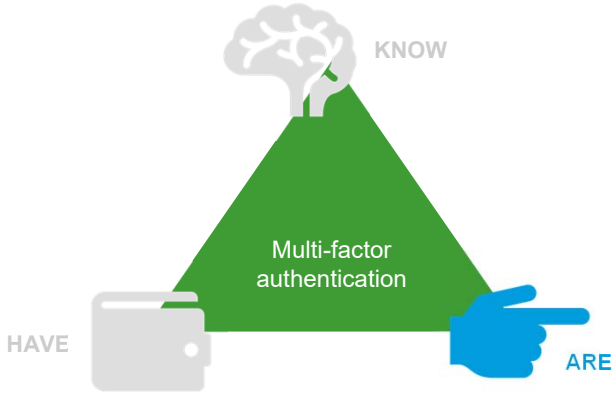
Biometric – Fingerprint or facial recognition

Pros:

- Simple for users
- Built in to newer platforms (Windows, Mobile)

Cons:

- Limited to newer platforms
- Can be compromised: simple implementations can give a false sense of security.



Authentication…something you HAVE

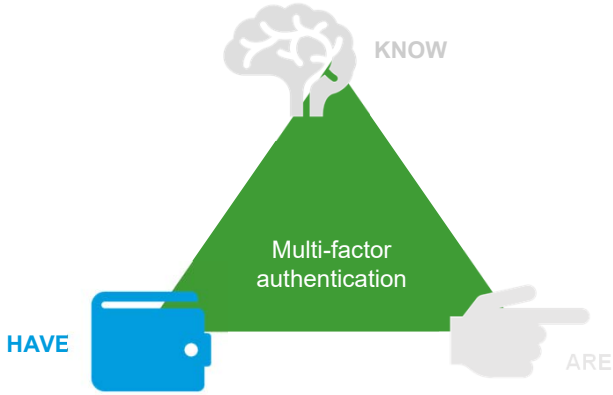
Tokens, SMS Text, or Mobile Apps

Pros:

- Lots of options
- Widespread support

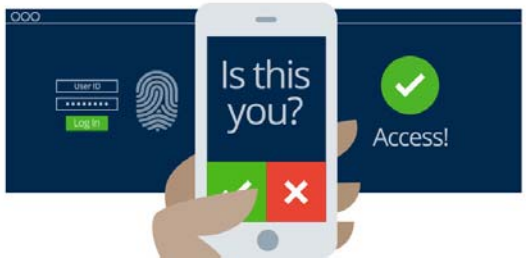
Cons:

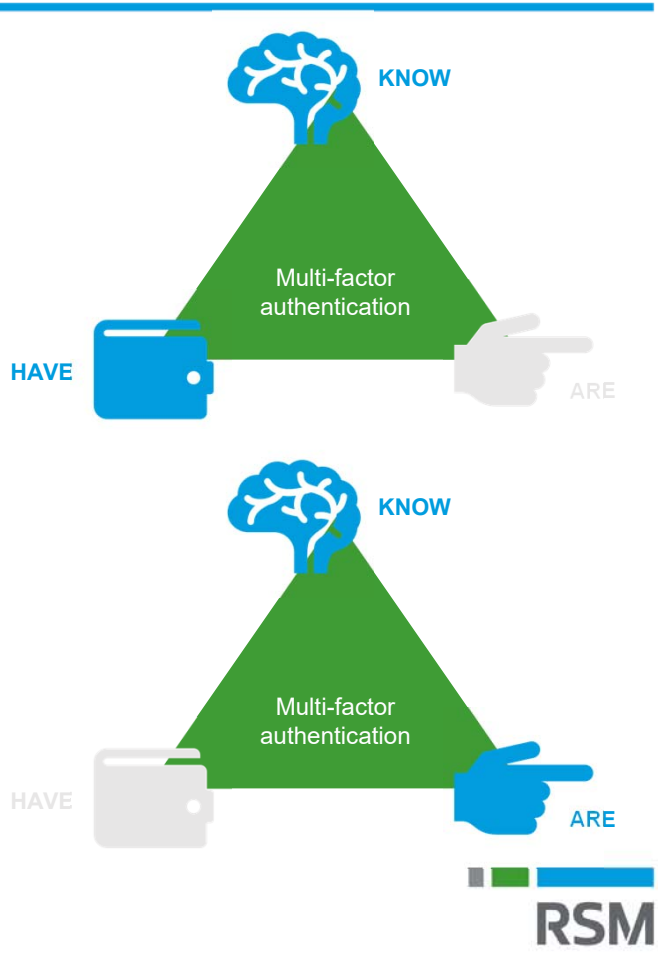
- Tokens can be lost or stolen
- Mobile devices require SMS or data coverage
- Not useful by itself
- Time delay to receive one time code or SMS



Authentication: multifactor

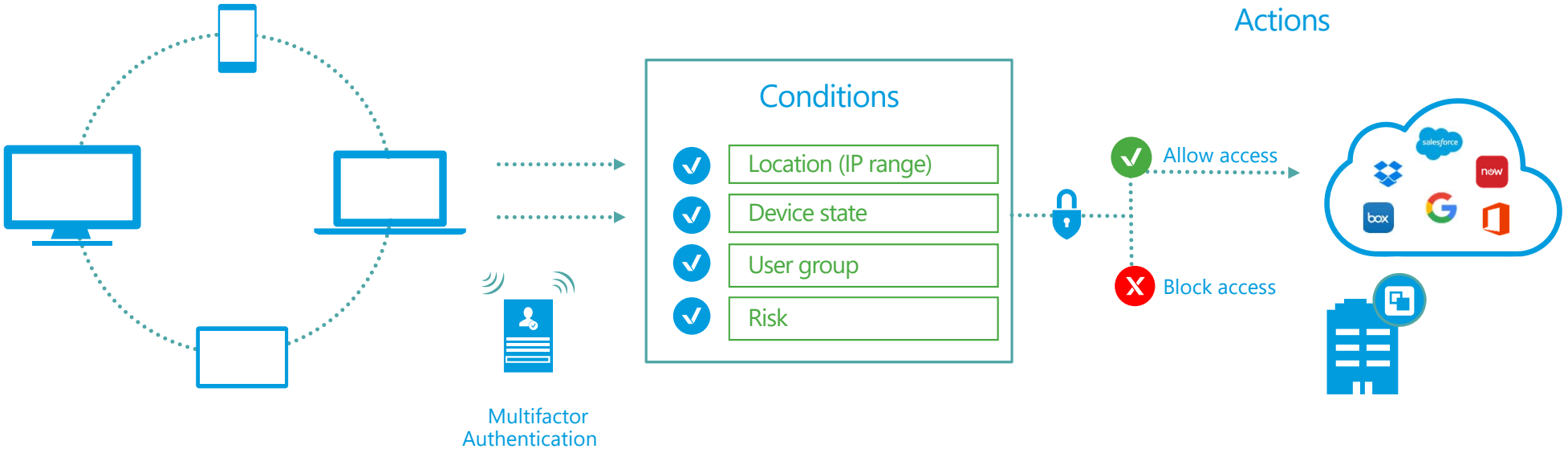
Eliminates many of the weaknesses present in the single factors.





 |

Conditional access

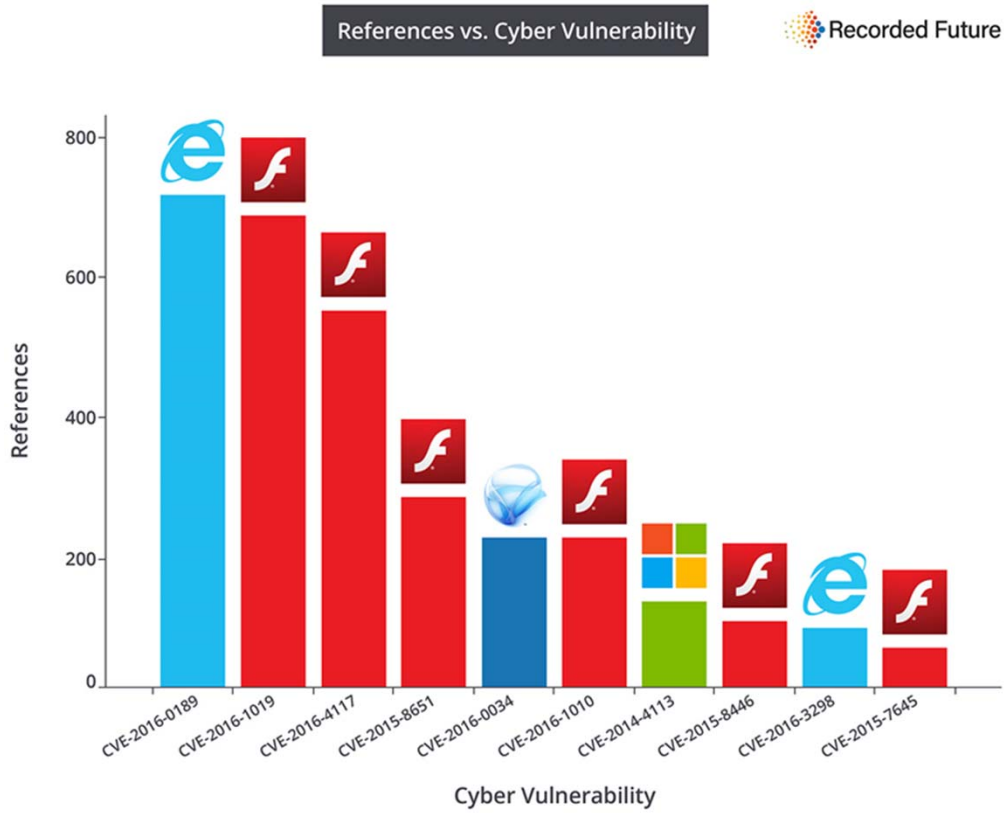


SECURE ENDPOINTS

Secure endpoints

Tools must work wherever our people take their devices.

Patch your devices



- Update software regularly
  - Apply patches consistently
- It's not just Microsoft!
- 6 out of the top 10 vulnerabilities used in breaches and ransomware in a recent year were not Microsoft patches.
- Measure effectiveness of patching with vulnerability management program.

RSM

Secure devices and protect data at the app level

Data control / isolation

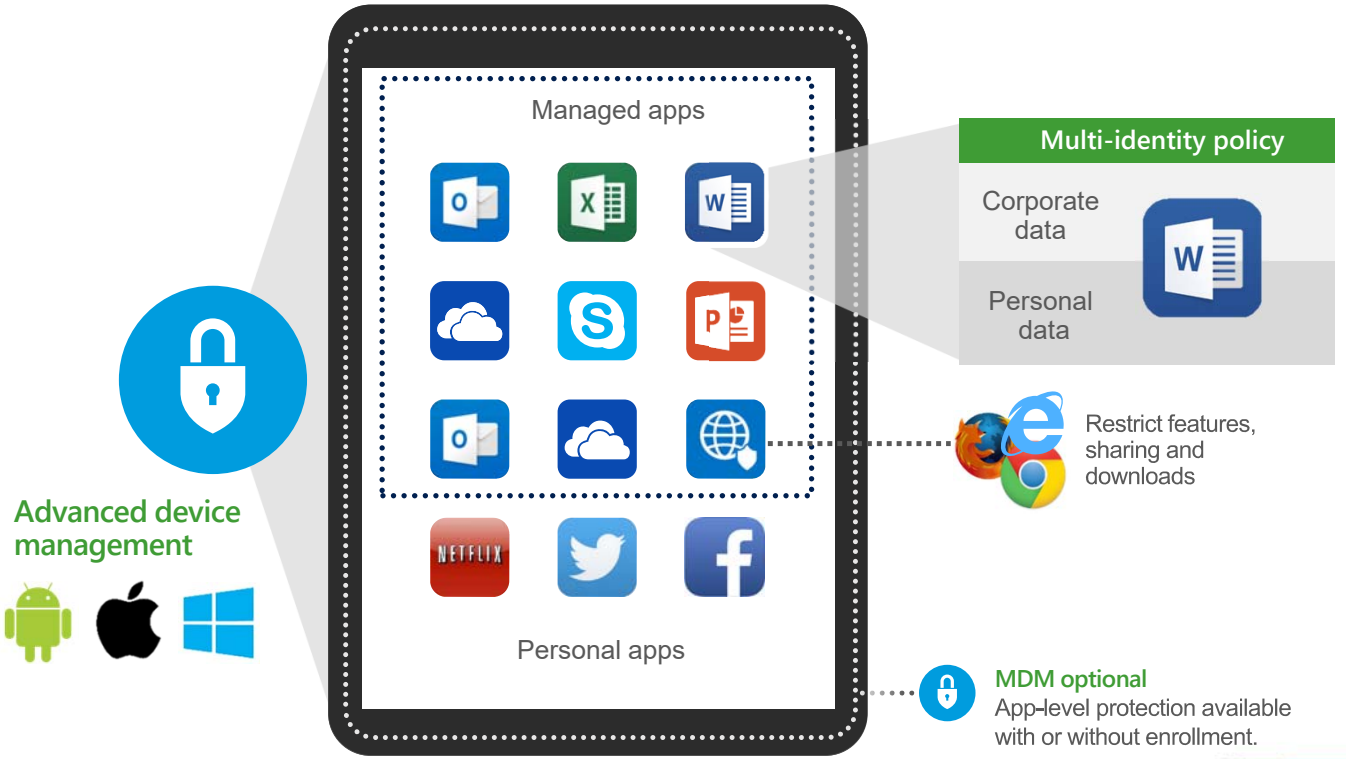
Control company data after it has been accessed, and separate it from personal data.

Device security configuration

Enforce device encryption, password/PIN requirements, jailbreak/root detection, etc.

Restrict apps and URLs

Restrict access to specific applications or URL addresses on mobile devices and PCs.



 |

Advanced Endpoint Detection and Response

Records telemetry data on all endpoints.

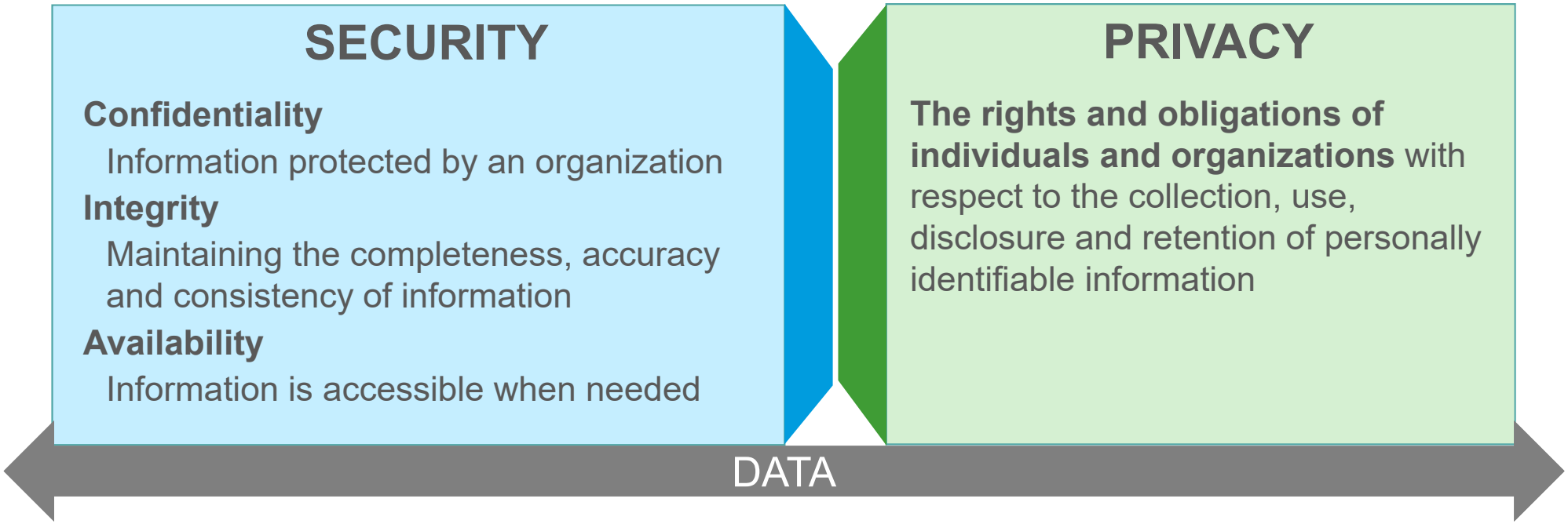
Uses that telemetry data to detect suspicious behavior.

Security analysts review alerts 24/7, and remove false positives, only alerting to actual threats

Can automate responses to threats, making the most of limited tech services staff time.

PRIVACY

Data security vs. data privacy



“All human beings have three lives: public, private, and secret.”

-**Gabriel García Márquez,** *Gabriel García Márquez: A Life*

Privacy 101

How many privacy regulations are you familiar with?

- Children's Online Privacy Protection Act (**COPPA**)
- Health Insurance Portability and Accountability Act (**HIPAA**)
- Health Information Technology for Economic and Clinical Health Act (**HITECH**)
- Payment Card Industry Data Security Standards (**PCI-DSS**)
- California Consumer Protection Act (**CCPA**)
- General Data Protection Regulation (**GDPR**)
- Brazilian General Data Protection Law (**LGPD**)
- Gramm-Leach-Bliley Act (**GLBA**)
- Family Educational Rights and Privacy Act (**FERPA**)
- Sarbanes-Oxley Act (**SOA**)
- USA PATRIOT Act
- Homeland Security Act
- Bank Secrecy Act (**BSA**)
- FTC Security Rule
- FACTA Red Flags Program
- State Executive Orders

Privacy – why now?

Lt. Commander Zuck in court after his plan to study humans in greater detail backfires

 |

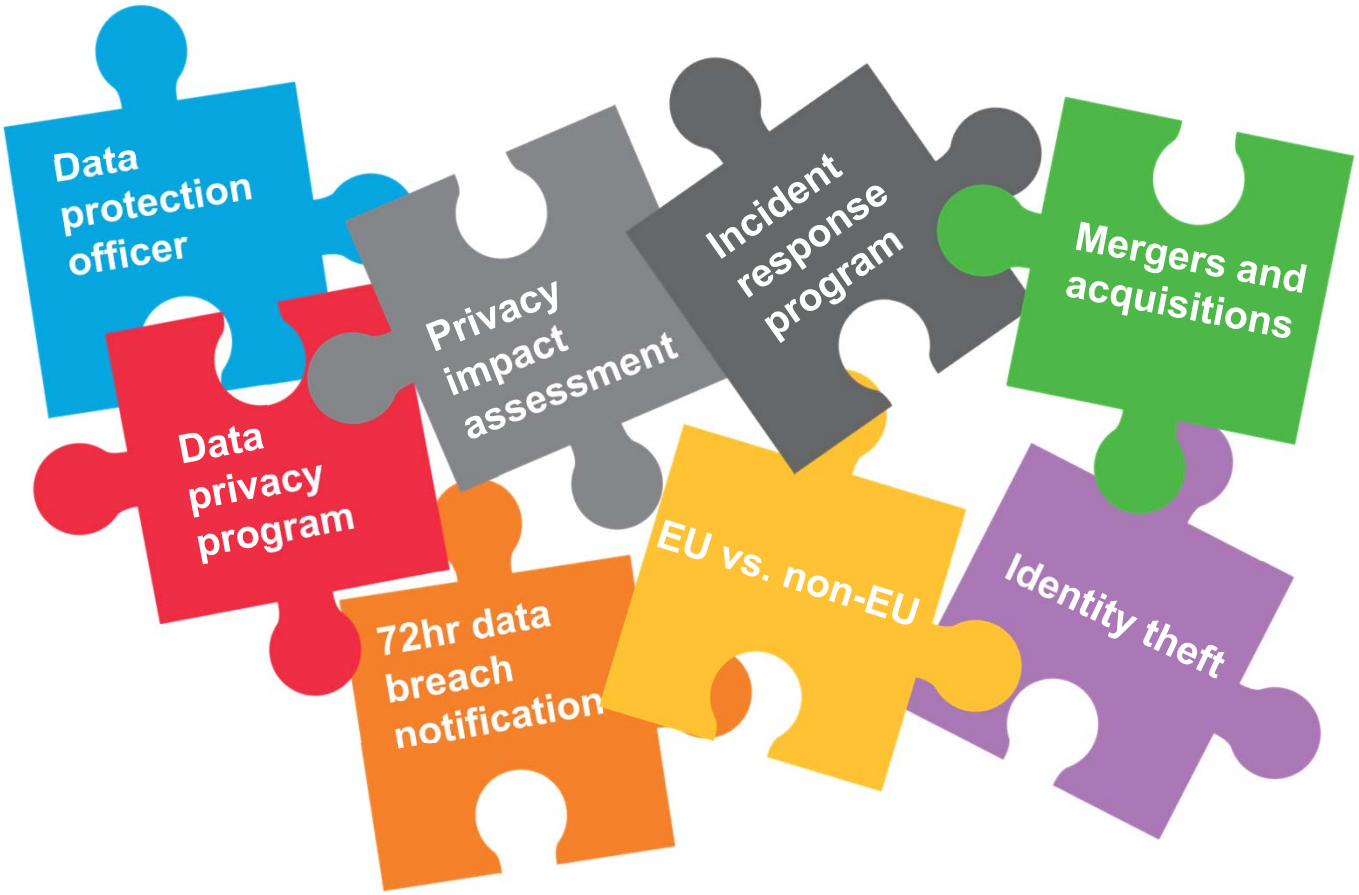
Privacy – why now?

"Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

CCPA Definition; Personal Information

Are you the slowest zebra?

What's the risk?



 |

How to not be the slowest privacy zebra…during a pandemic

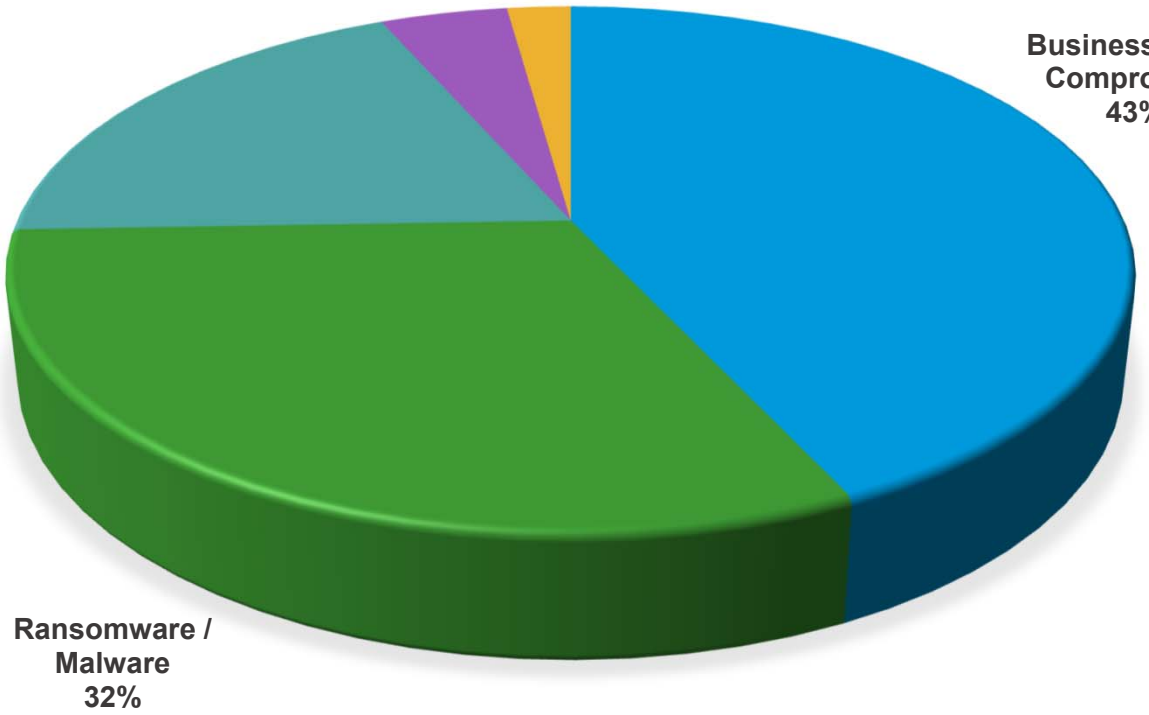
- **Review**
- **Understand**
- **Determine**
- **Implement**

Keep out of the spotlight, stay in the limelight

 |

EDUCATED AND SUSPICIOUS WORKFORCE

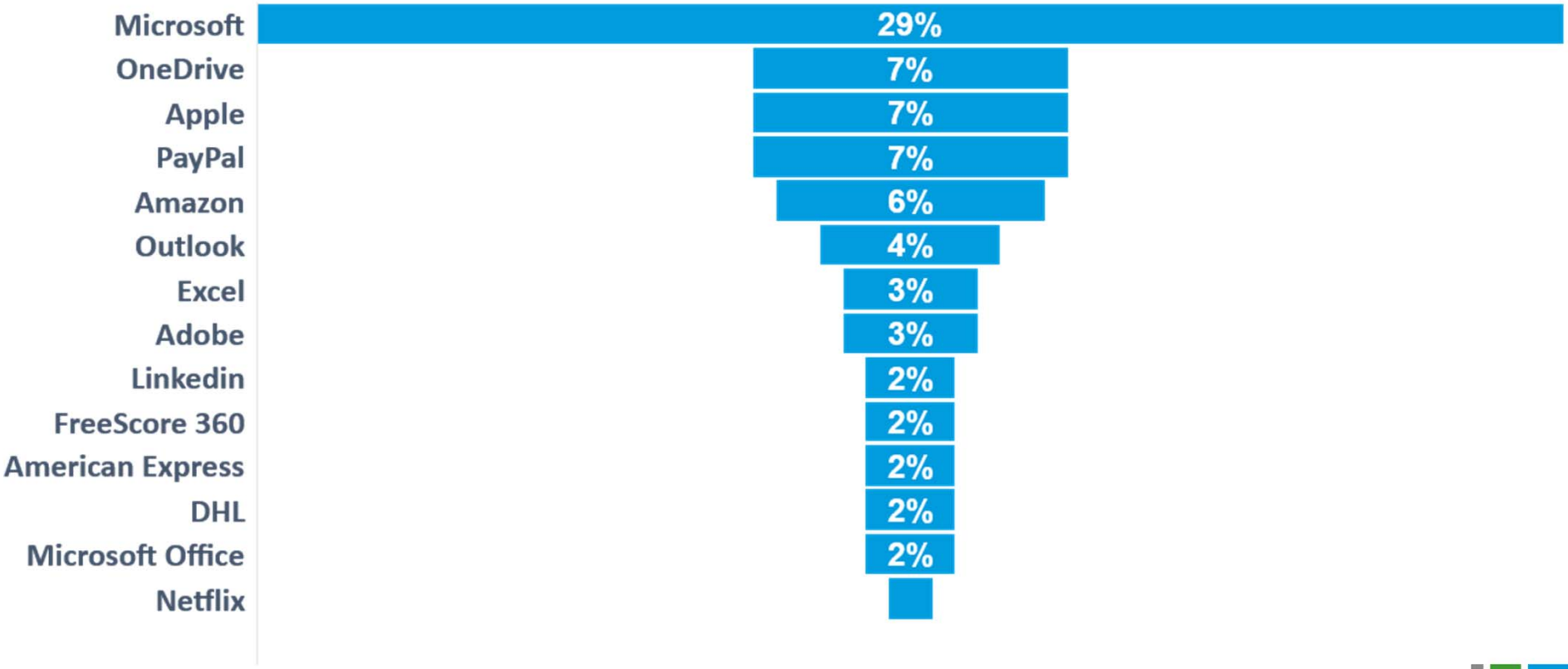
Cyber incident – attack types 2019



Majority of Cyber-Incidents can be prevented by appropriate employee behavior.

Source: Cyber incidents handled by RSM 5/1/2019 – 10/31/2019

Most common brands mentioned in phishing attacks



Train your employees

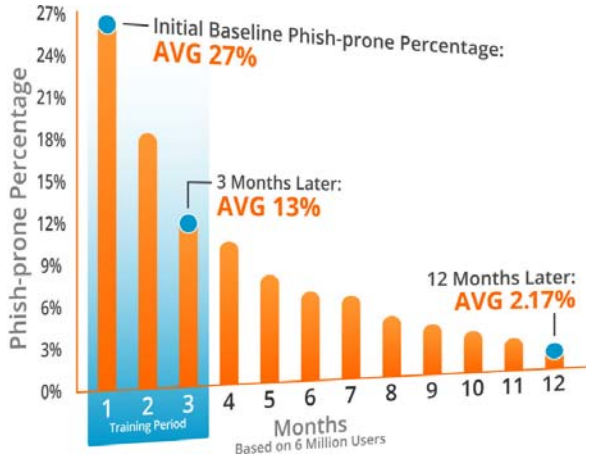
- Policies and Procedures
  - Incident Response Plans
- Recognize suspicious emails
- Safe browsing habits
- Of security breaches caused by an employee, how many were unintentional?
- …77% were unintentional.

RSM

Security awareness: measure effectiveness

Making sure your employees understand the mechanisms of spam, phishing, spear phishing, malware, ransomware and social engineering and can apply this knowledge in their day-to-day job.

- Baseline testing to assess the Phish-prone percentage of your users through a simulated phishing attack.
- Online security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.
- Reporting, showing stats and graphs for both training and phishing, ready for management.



 |