Microsoft

DLP, Phishing, Tech Support Scams

Miten Microsoft toteuttaa tietoturvaa ja tietosuojaa?
November 2018

Mikko Viitaila
@mikkoviitaila
National Technology Officer, Teknologiajohtaja
Microsoft Oy

Microsoft Finland

Microsoft in Finland is a strong millennial, born 1992

2+ million active users in Microsoft Office 365 cloud

2,000+ partners generating 8 $ revenue per each $ by MSFT

Partner ecosystem with 40,000 tech jobs in Finland

1,600 start-ups directly supported by Microsoft

Close to 90% of the students in Finland using Office 365

51% of major Finnish companies using the cloud

Agenda

- Digital Estate – Threat Landscape
- Microsoft’s Approach to Security
- DLP
- Phishing
- Tech-support Scams

The digital estate is growing

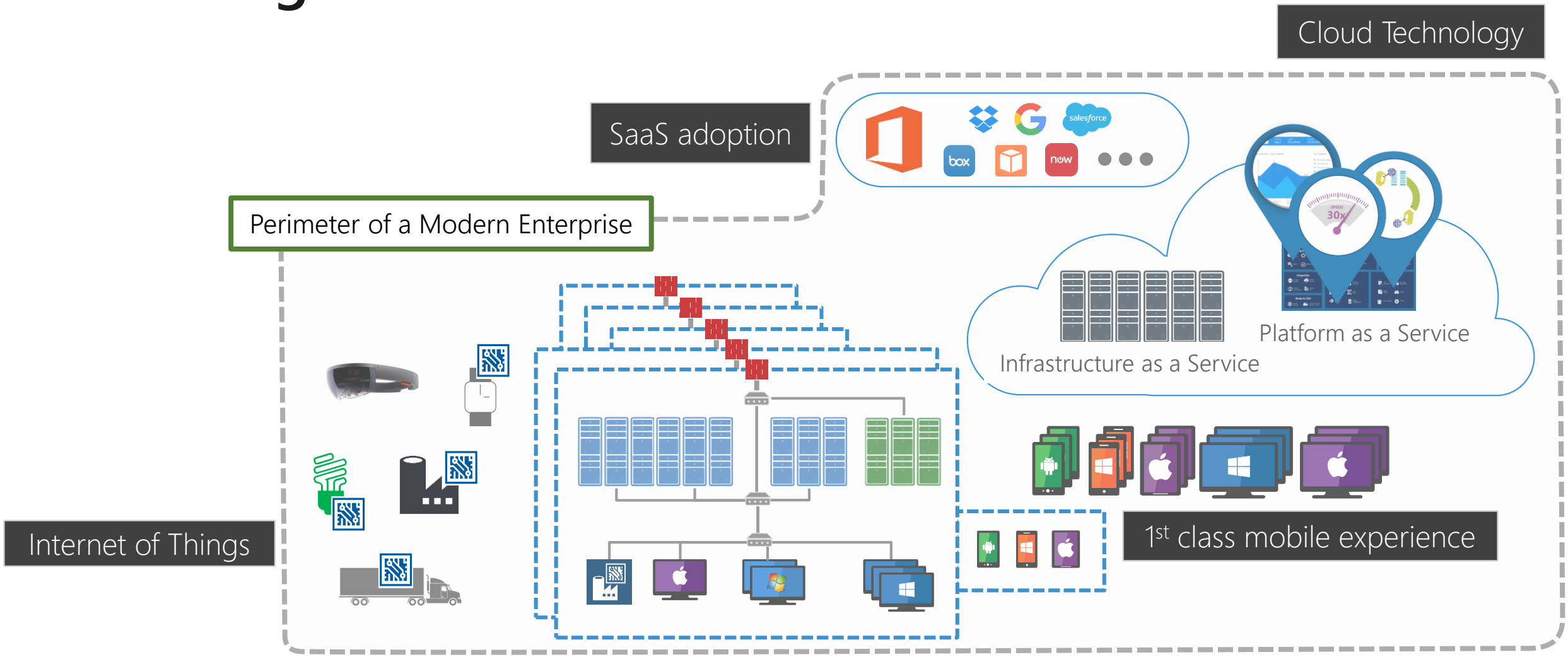
The cybersecurity landscape is rapidly changing

Cyberspace is the new battlefield

Security skills are in short supply

Virtually anything can be attacked

Your Organization in Transformation



Q: WHERE IS YOUR DATA?

A: EVERYWHERE

Devices: fixed and mobile

SaaS apps & file shares

On-premises file shares

Sensitive data is at risk

80 % of employees use non-approved SaaS apps at work

85 % of enterprise organizations keep sensitive information in the cloud

88 % of organizations no longer have confidence to detect and prevent loss of sensitive data

58 % have accidentally sent sensitive information to the wrong person

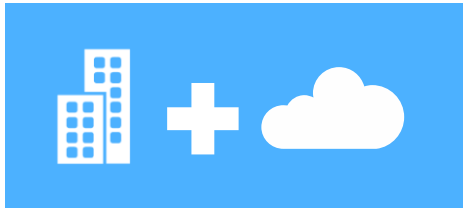
The challenge of securing your environment

Bad actors are using increasingly creative and sophisticated **attacks**.

The digital estate offers a very broad surface area that is difficult to **secure**.

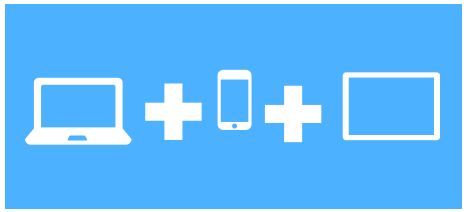
Integrated, intelligent correlation and action on signals is difficult, time-consuming, and **expensive**.

Information Security is in Transformation



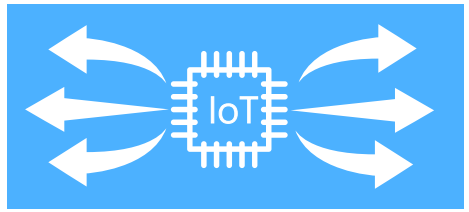
Enterprise IT is Cloud Hybrid

- Cloud adoption is inevitable (Digital Transformation + industry momentum)
- Legacy systems will take years to migrate or retire



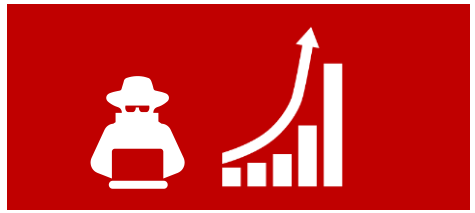
Technology Mobility and Volume is Exploding

- Increasing demand for first class experience on mobile devices
- Variance in trustworthiness of mobile devices



Pervasive Digital Transformation and IoT

- IoT adoption driving a wave of app development and cloud usage
- Enterprise PC Security strategies applies poorly to IoT devices

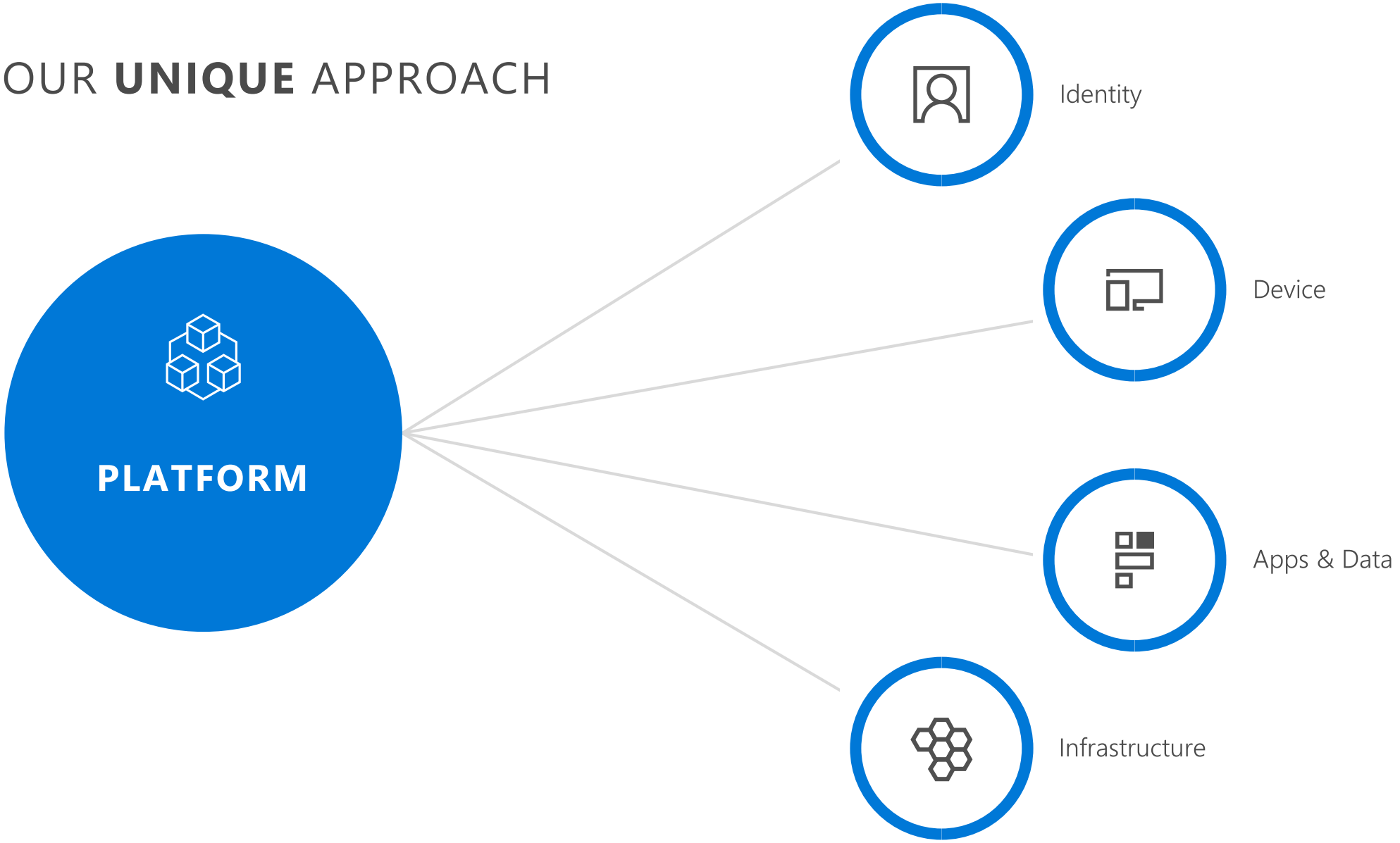


Increasingly Hostile Environment

- Increased attack surface with new technologies creates new blind spots
- Attacks rising in volume and sophistication to capture illicit opportunities

Microsoft’s Approach

OUR **UNIQUE** APPROACH



Focusing security efforts in a complex landscape

Adopt identity-based protection

Enable Seamless and secure identity and access for employees, partners and customers

Apply persistent data protection

Protect sensitive data – wherever it lives or travels.

Protect against sophisticated hackers

Protect, detect and remediate against threats across the modern workplace.

Simplify security management

Streamline management with built-in intelligence and recommendations.

Microsoft Security

Identities

Users and admins

Endpoints

Devices and sensors

User Data

Email messages and documents

Cloud Apps

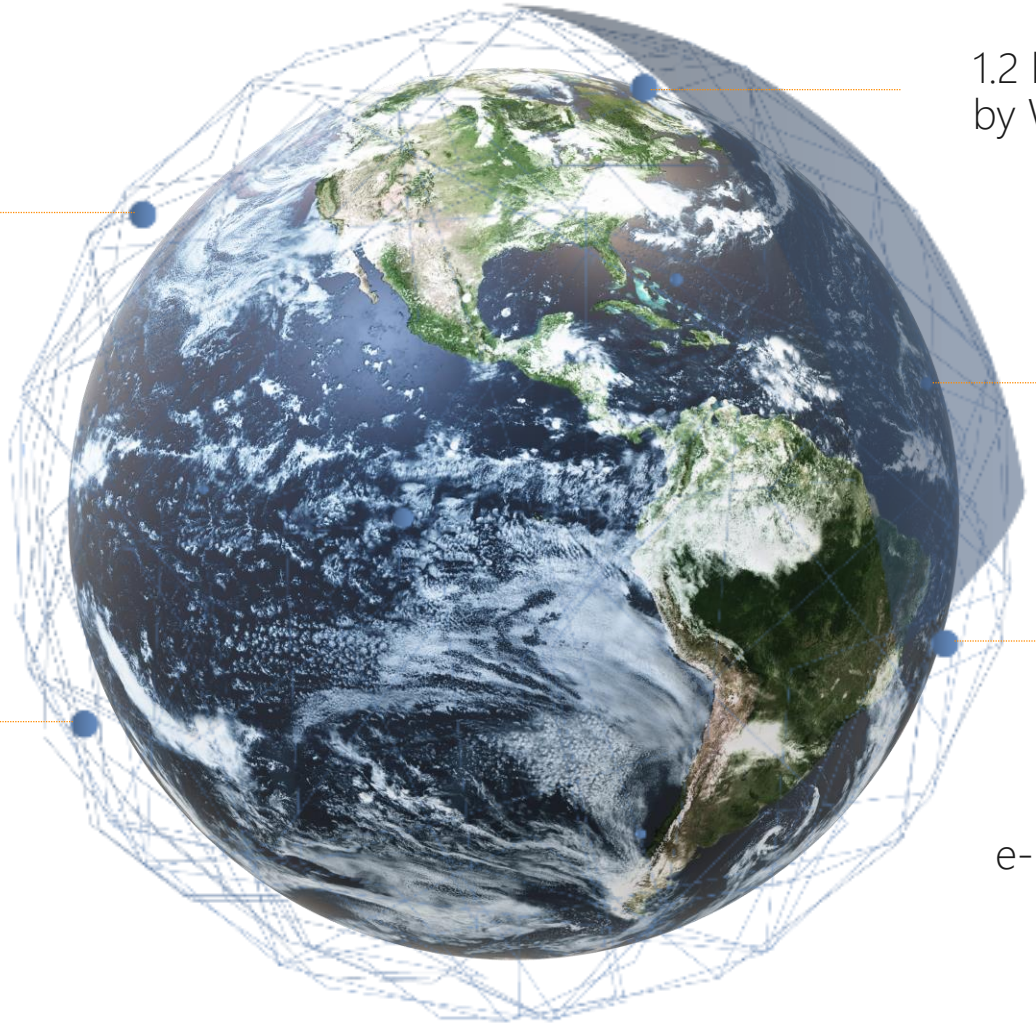
SaaS applications and data stores

Infrastructure

Servers, virtual machines, databases, networks

Intelligent Security Graph
6.5 TRILLION signals per day

Holistic view on security…



1.2 billion devices scanned by Windows Defender

200+ global cloud consumer and commercial services

450 billion authentications

18+ billion web pages scanned by Bing

400 billion e-mails analyzed

The Microsoft Intelligent Security Graph

…provides new insights

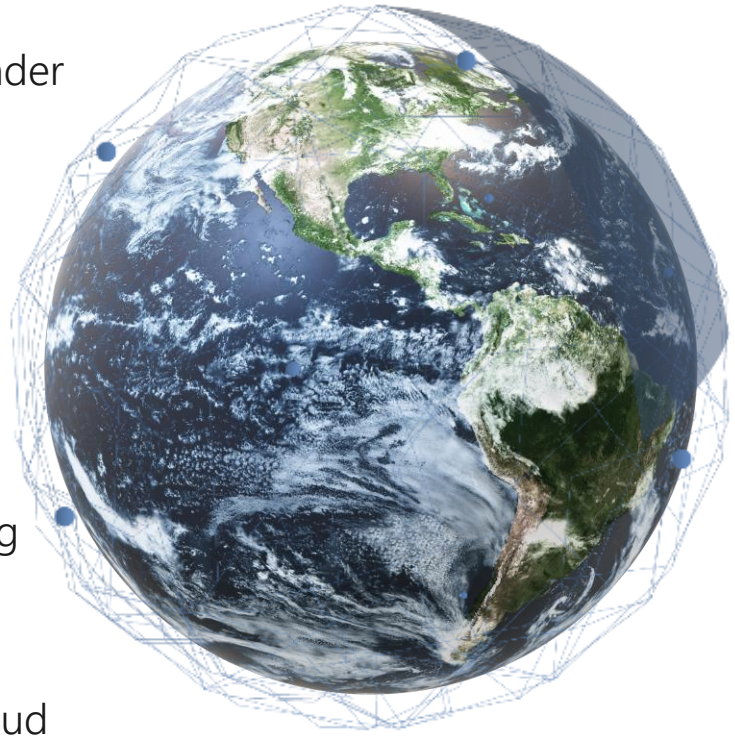
450 billion authentications

1.2 billion devices scanned by Windows Defender

400 billion e-mails analyzed

18+ billion web pages scanned by Bing

200+ global cloud consumer and commercial services

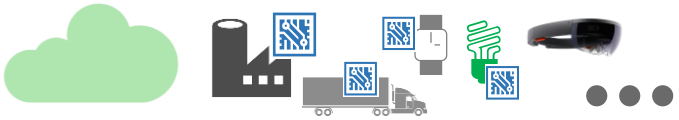


Intelligence

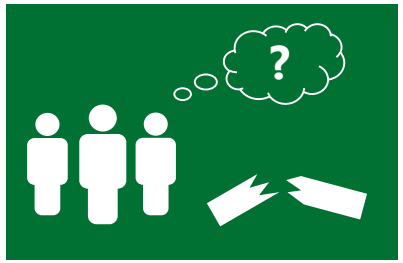
The Microsoft Intelligent Security Graph

Data Loss Prevention

Evolution of Information Protection

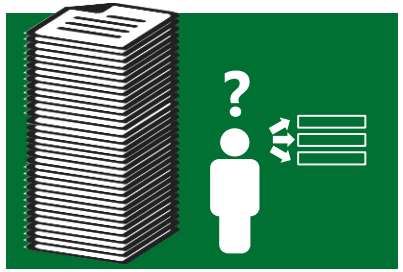
Microsoft Security Philosophy	*Access Controls + Encryption*	*+ Rights Management*	*+ Full Lifecycle Protection (Auto Classification, SaaS)*
Information Protection Trends	*Fileshare & USB stick Sprawl*	*SharePoint & Email/Mobile Sprawl*	*Cloud & Shadow IT Sprawl*
Information Technology	 *Mainframes + PCs*	 *+ Datacenters + Mobile Devices*	 *+ Cloud + Internet of Things (IoT)*

Data Security Challenges



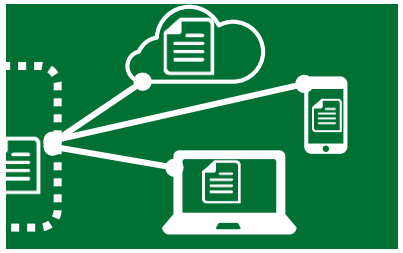
Reduce and manage risk of user errors

Collaboration to create new business value requires data sharing and data mobility
Critically important to prevent unauthorized disclosure, modification, or destruction



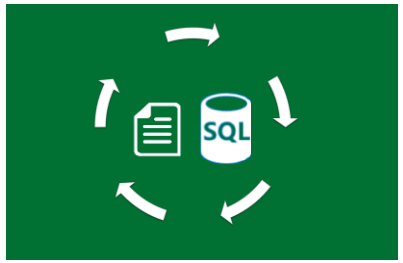
Classification is challenging

Manual user classification is impractical at scale
Large set of existing documents and more being created all the time



Data must be protected outside of the network

Data must be protected as it traverses mobile devices and cloud services
Data created outside the network must be classified and protected



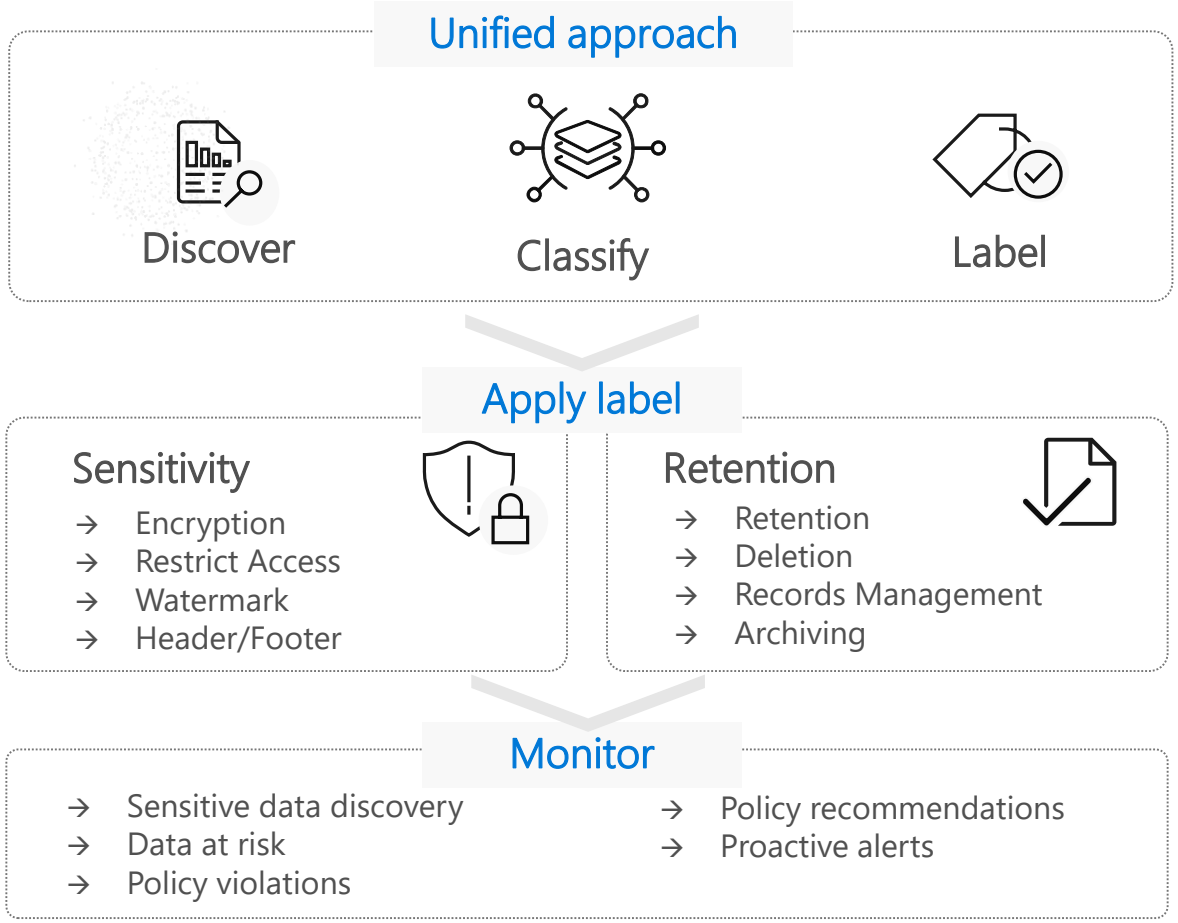
Compliance & security require a complete strategy

Compliance penalties are increasing and measuring outcomes vs. methods
Need full lifecycle protection for information assets (appropriate to valuation)

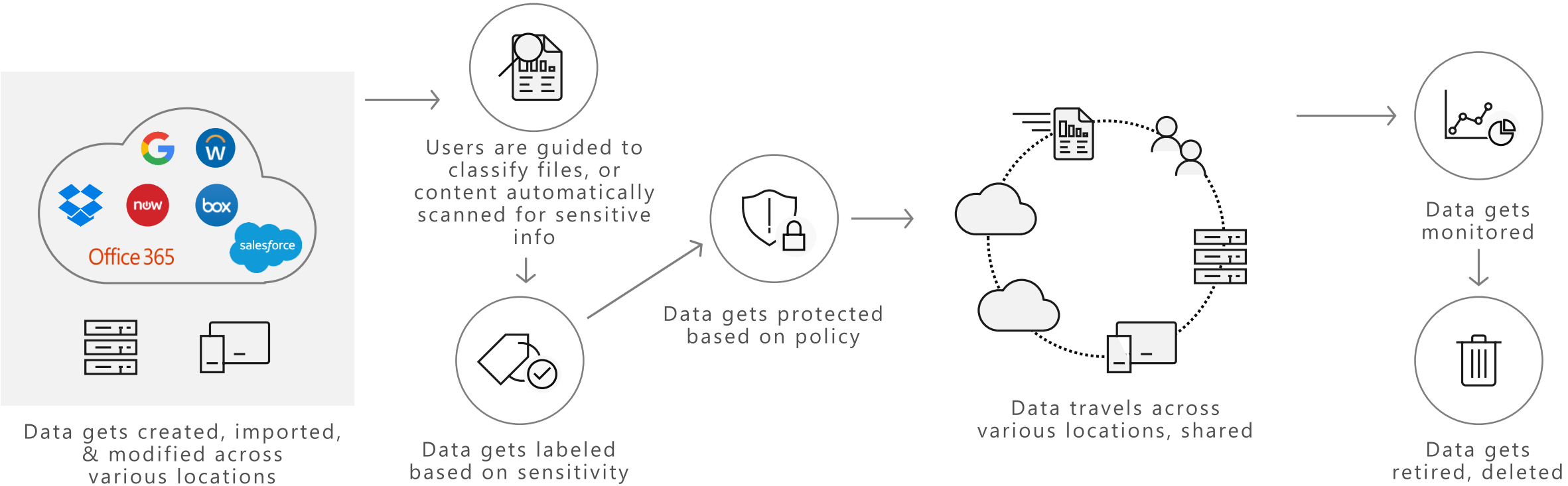
Data protection & data governance go hand-in-hand

Comprehensive policies to protect and govern your most important data – throughout its lifecycle

- Unified approach to discover, classify & label
- Automatically apply policy-based actions
- Proactive monitoring to identify risks
- Broad coverage across locations



Follow data throughout its lifecycle



Data gets created, imported, & modified across various locations

Users are guided to classify files, or content automatically scanned for sensitive info

Data gets labeled based on sensitivity

Data gets protected based on policy

Data travels across various locations, shared

Data gets monitored

Data gets retired, deleted

Detect & classify sensitive information

Have you defined what "sensitive data" means for your company?

Do you have a way to detect sensitive data across your company?

Do you have a way to ensure that labels persist with the data—wherever it travels?

Which regulations and compliance factors impact you?

Are you able to empower end-users to classify and label content themselves, or apply automatically based on company policies?

Apply protection based on policy

Do you need the flexibility to apply a range of protection actions, based on how sensitive the data is?

Does protection need to persist with the data, even as it travels across devices, SaaS apps and on-premises

Are you able to apply the protection options you need in order to comply with internal policies and external regulatory requirements?

Are you able to empower end-users to protect content themselves, or apply automatically based on company policies?

Do you have the right notifications and education for end-users so they are being responsible with sensitive data?

Monitor & remediate

Do you have visibility into how sensitive data is being accessed and shared across 3rd-party SaaS apps and cloud services?

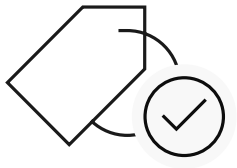
Are you able to remediate actions immediately, such as quarantine data or block access?

Are you able to integrate event information into your SIEM system or other tools?

Microsoft Information Protection solutions

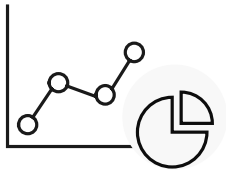
Protect your sensitive data – wherever it lives or travels

Discover



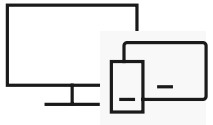
Classify

Protect

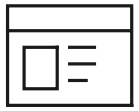


Monitor

Across



Devices



Apps

Cloud services

On-premises

Phishing

Phishing attacks are fast and hard to stop

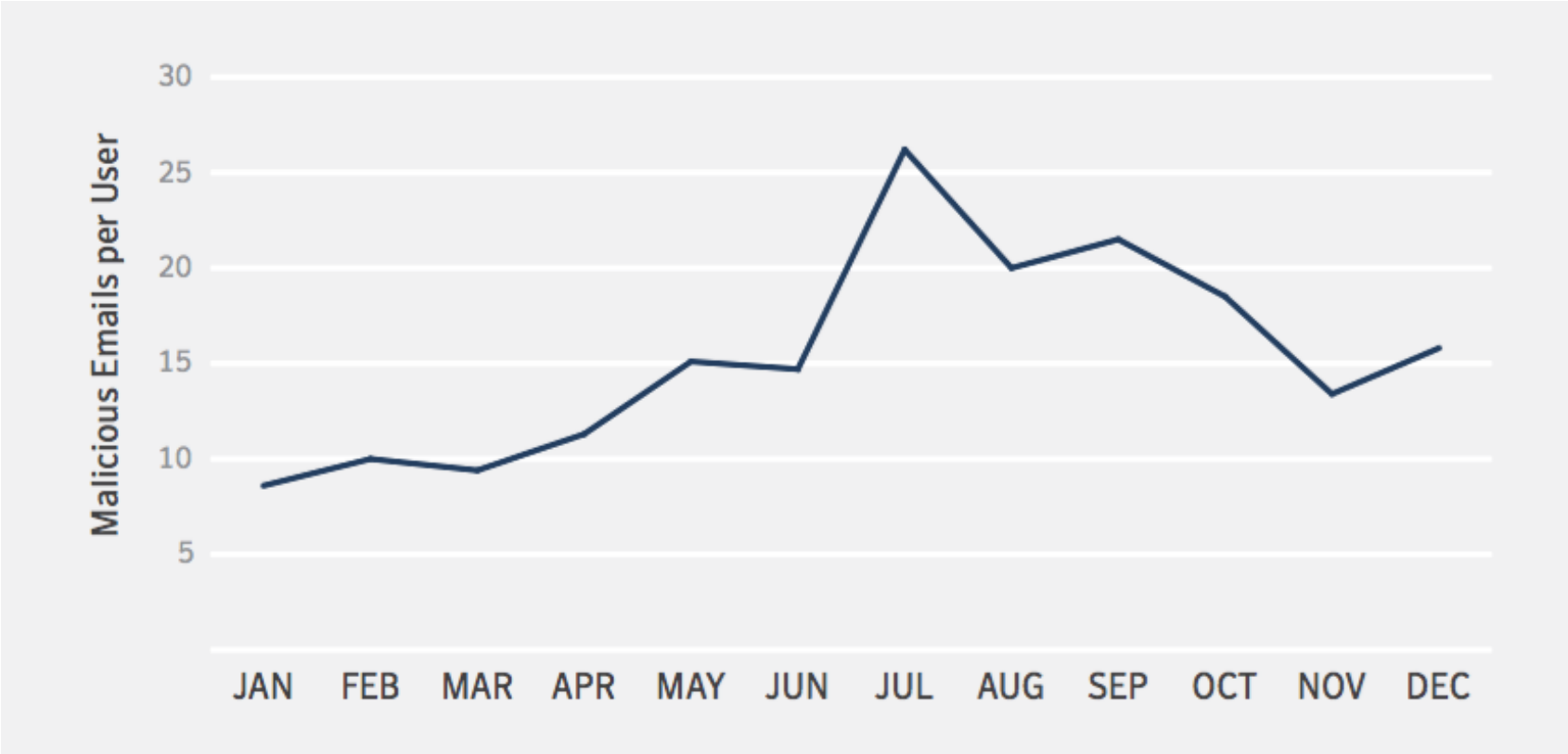
If an attacker sends an email to **100 people** in your company…

…**23 people** will open it…

…**11 people** will open the attachment…

…and **six** will do it in the **first hour.**

Statistics



On average,
16 malicious
emails per month
per user

https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Statistics

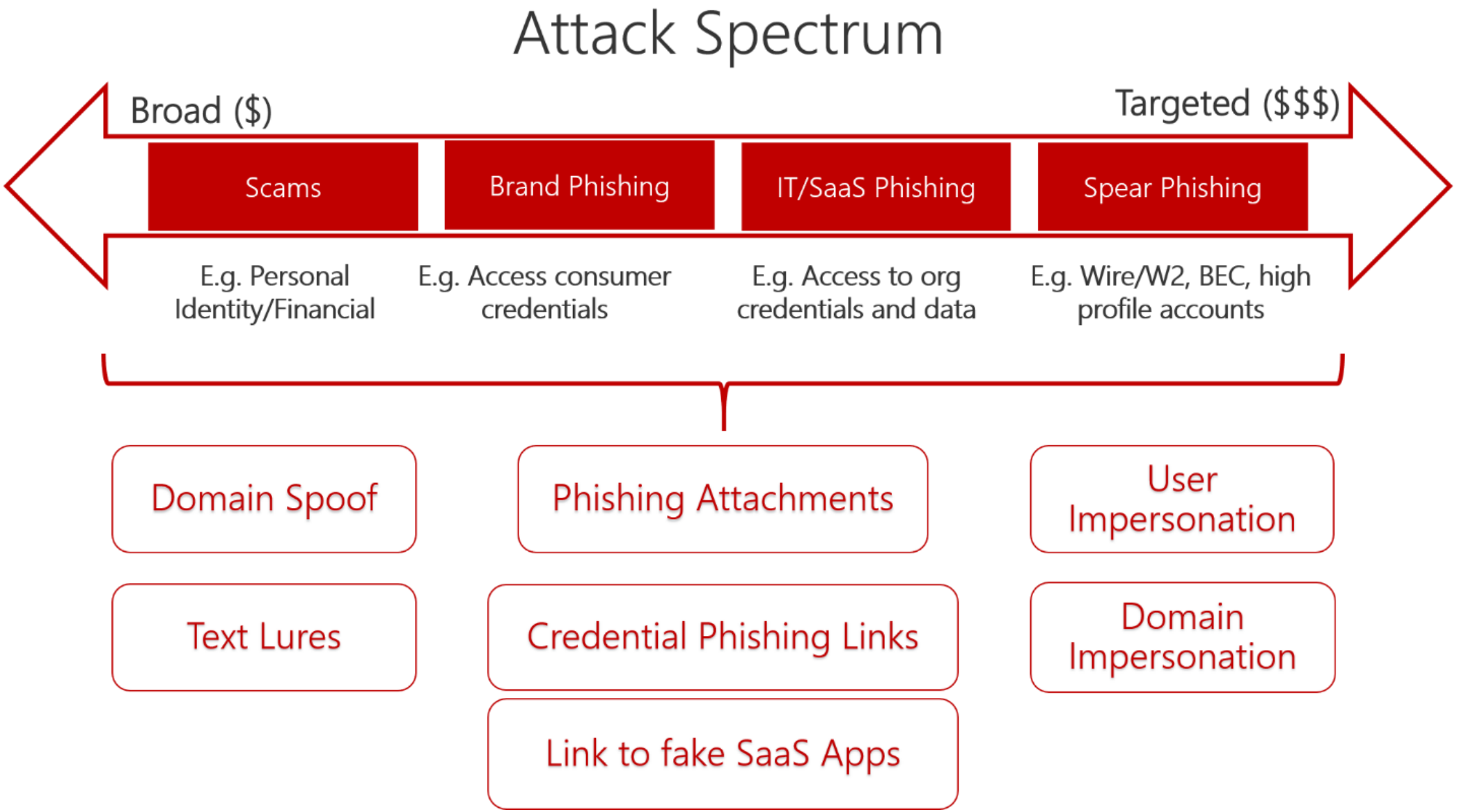
92.4% of malware is delivered via email.

https://enterprise.verizon.com/resources/reports/dbir/

Fake invoices are the #1 disguise for distributing malware.

https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

The Phishing Landscape



Microsoft statistics

300,000

Phish Campaigns Analyzed in 2018

8 million

Business Email Compromise Attempts in 2018

20%

Of users click on a malicious link in first

5 minutes

Phishing email statistics from Office 365 from January 2018 to September 2018

Anti-phish capabilities in Office 365

5 billion

Phish Emails Blocked in Office 365 in 2018

7 billion

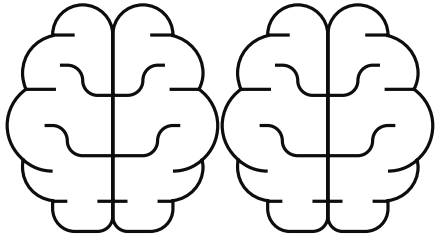
URL clicks protected by Safe Links in 2018

11 billion

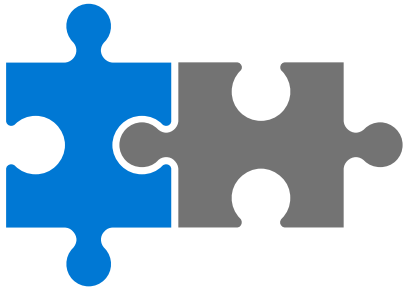
Unique items detonated by ATP sandboxing in 2018

Microsoft's Approach

Rich signal across M365



Artificial Intelligence



Rich client & Service Integration

Protect

During mail flow and post delivery

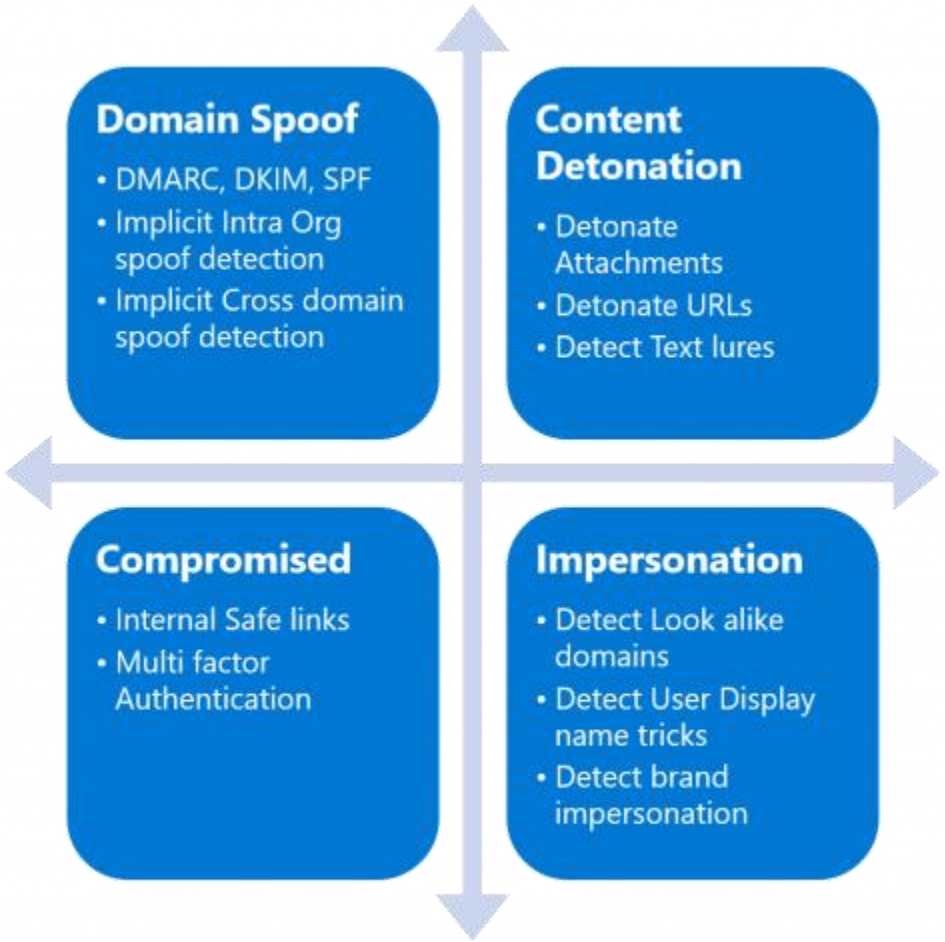
Detect

User and Admin controls

Respond

Visibility and actionable insights

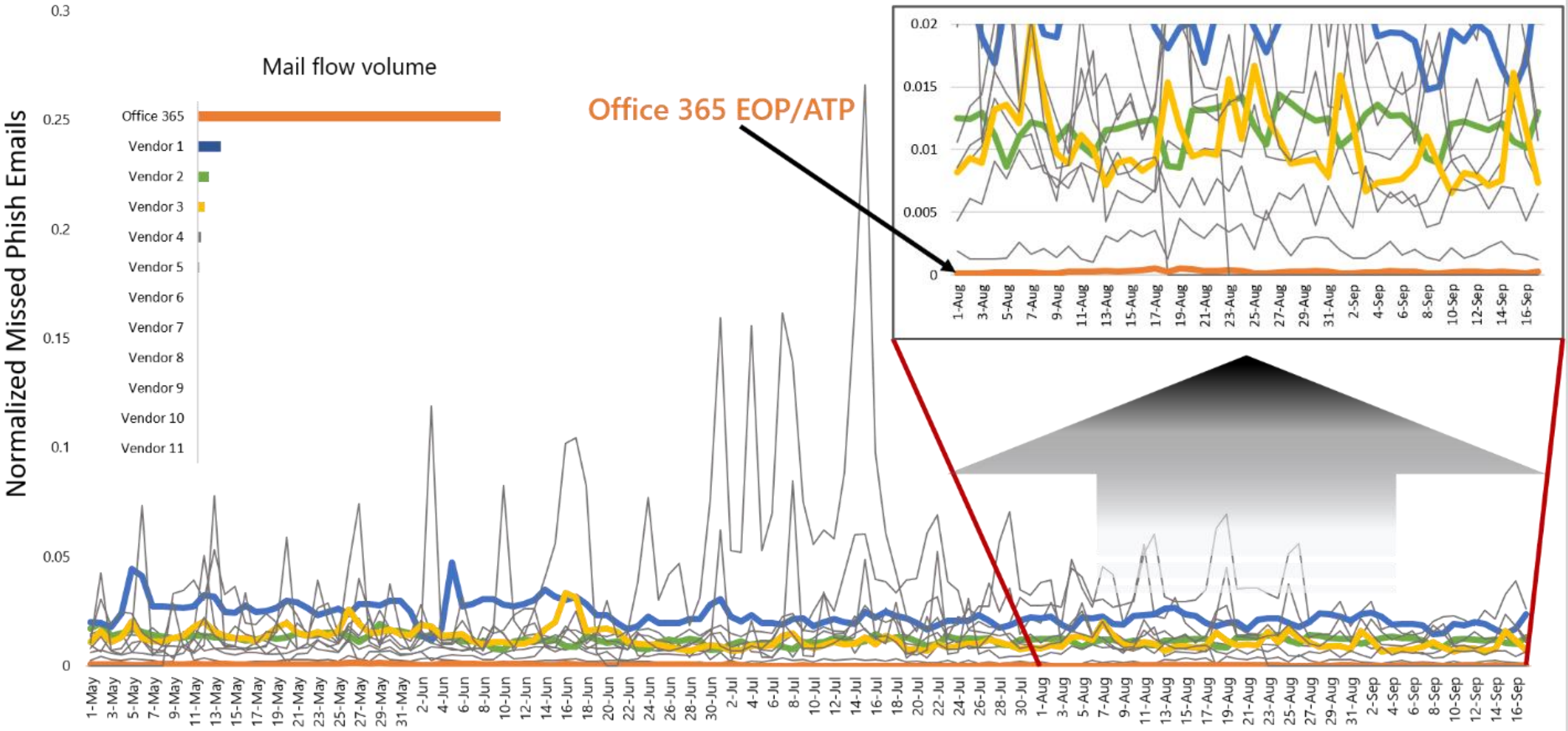
Phish email categories and anti-phish enhancements



Anti-phish Enhancements

- ✓ Spoof Intelligence for intra-org and cross domain spoof detection
- ✓ Advanced Machine Learning Models
- ✓ Time of Click Protection (Safe links)
- ✓ Internal Safe links
- ✓ Detonation of attachments for phish/malware
- ✓ Detonation of Link Content for malware/phishing sites & attachments
- ✓ Detonation and detection of malicious files in SharePoint/OneDrive/Microsoft Teams
- ✓ Mailbox Intelligence for user contact graph
- ✓ User and Domain Impersonation protection
- ✓ Real time reporting
- ✓ Rich Insights

Normalized Phish Miss in Office 365 by Vendor, May 1 – Sep 16 2018



Inbox - tifc@IgniteDemo2018.onmicrosoft.com - Outlook

File | Home | Send / Receive | Folder | View | Help | Tell me what you want to do

New Email | New Items | Ignore | Clean Up | Junk | Delete | Archive | Reply | Reply All | Forward | Meeting | IM | More | Move to: ? | To Manager | Team Email | Done | Move | Rules | OneNote | Assign Policy | Unread/ Read | Categorize | Follow Up | New Group | Browse Groups | Search People | Address Book | Filter Email | Read Aloud | Get Add-ins | MyAnalytics

New | Delete | Respond | Quick Steps | Move | Tags | Groups | Find | Speech | Add-ins

Junk Email [155]

Search Current Mailbox | Current Mailbox

Focused | Other | By Date

FROM	SUBJECT	RECEIVED
Date: Last Week		
Office 365 Message Center	Message Center Major Change Update Notification	Sun 9/9/2018 3:16 PM
Date: Two Weeks Ago		
Office 365 Message Center	Message Center Major Change Update Notification	Thu 9/6/2018 3:08 AM
Office 365 Message Center	Message Center Major Change Update Notification	Wed 9/5/2018 5:17 PM
Office 365 Message Center	Weekly digest: Office 365 changes	Mon 9/3/2018 2:13 AM
Date: Three Weeks Ago		
Office 365 Message Center	Weekly digest: Office 365 changes	Mon 8/27/2018 3:48 AM
Date: Last Month		
Skype for Business	You now have Office 365 Audio Conferencing	Fri 8/17/2018 4:05 PM

Fri 9/21/2018 11:24 AM

MA

Microsoft Account Administration

User account suspension information

To Sumit Malhotra

This sender might be impersonating a domain that's associated with your organization. Learn why this could be a risk Feedback

Microsoft

Your user account is going to be disabled. Login now to prevent suspension.

https://login.m1cr0soft.ru/
Click or tap to follow link.

Go to the sign-in page, https://portal.office.com

Sincerely,
The Microsoft Office 365 Team

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager.

This message was sent from an unmonitored e-mail address. Please do not reply to this

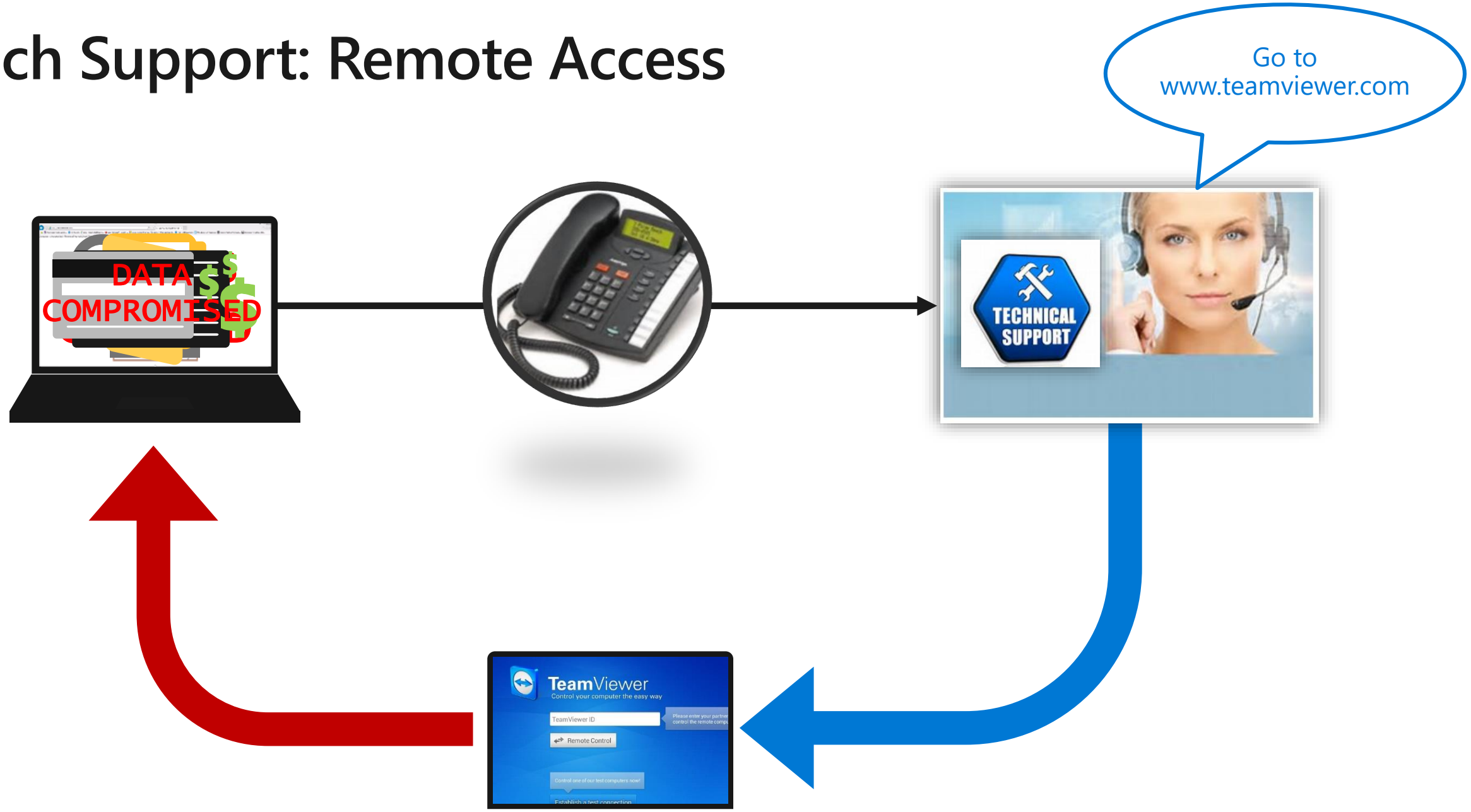
https://login.m1cr0soft.ru/ | All folders are up to date. | Connected to: Microsoft Exchange | Display Settings | 100%

Phishing: Six Best Practices to apply TODAY

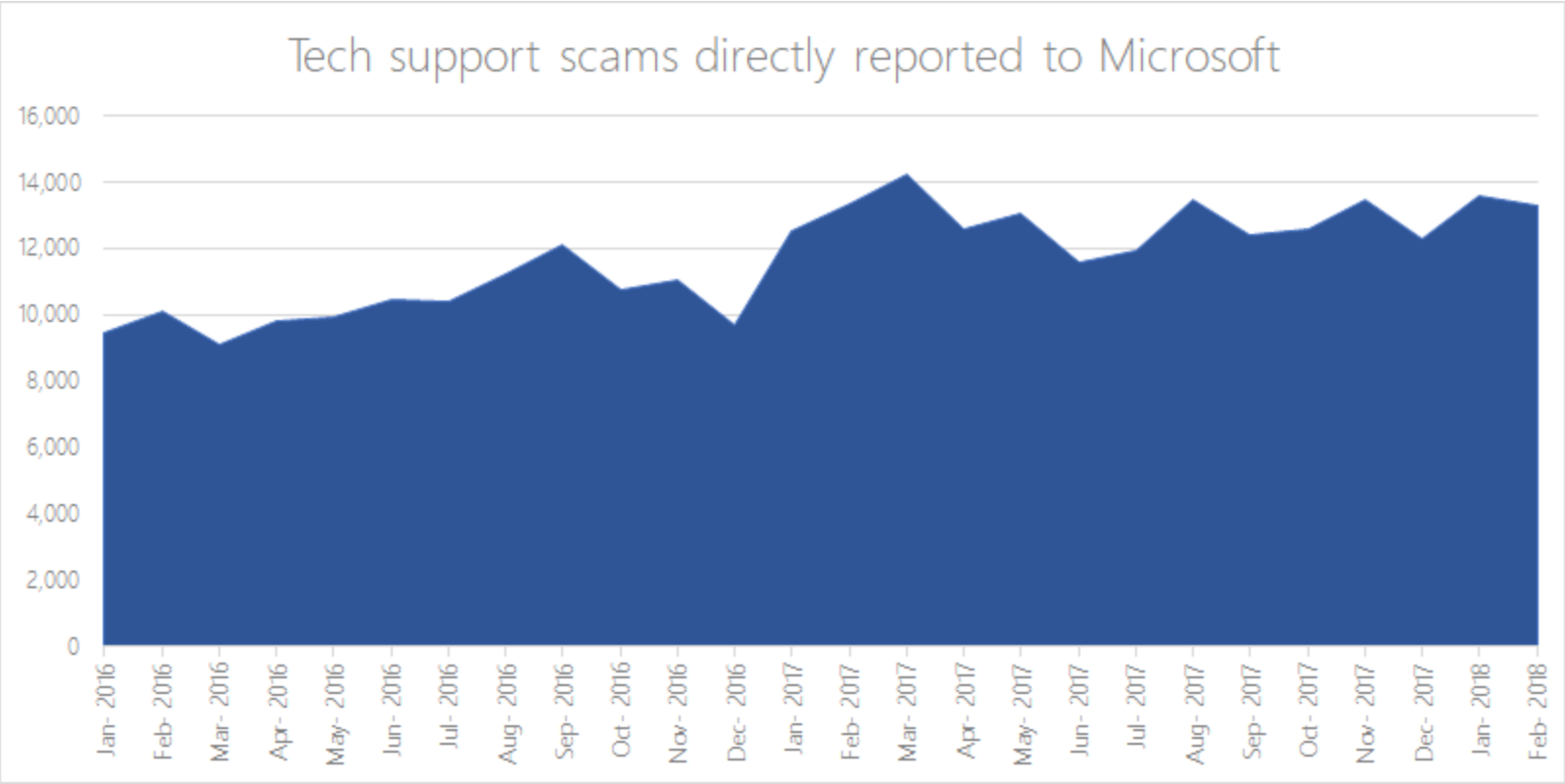
1. Enable ATP Safe links and Safe attachments for ALL users
2. Tune machine models tolerance for Phishing
   - Lower the phish threshold for key users
3. Review ETR Rules (Exchange Transport Rule)
   - Ensure IP/Domain allow rules include checks for authentication
4. Utilize the new reporting Add-in to gain insights
5. Enable MFA
6. Get to DMARC p=Reject
   - DMARC = Domain-based Message Authentication, Reporting and Conformance

Tech Support Scams

Tech Support: Remote Access



Microsoft statistics



Some stats

- **FBI:** 11 000 tech-support fraud complaints in 2017 with claimed losses totaling nearly $15m, up 86 percent on reported losses in 2016. It received reports from victims in over 80 countries. https://www.ic3.gov/media/2018/180328.aspx

- **Microsoft:** In 2017, Microsoft Customer Support Services received 153,000 reports from customers who encountered or fell victim to tech support scams, a 24% growth from the previous year. These reports came from 183 countries, indicating a global problem. https://cloudblogs.microsoft.com/microsoftsecure/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/

Tech Support Scams – Scope of the problem

2 out of 3 people have experienced a tech support scam in the last year.

1 in 5 consumers surveyed continued with a potential fraudulent interactions; meaning they downloaded software, visited a scam website, gave the fraudsters remote access to their device, or provided credit card information or other form of payment.

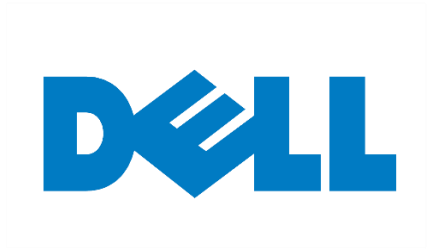
Nearly 1 in 10 have lost money to a tech support scam.

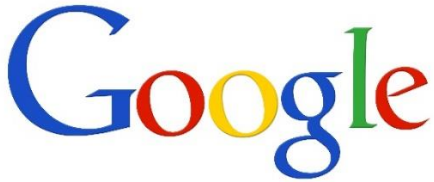
Of those who continued with a fraudulent interaction, **17% of them were older than 55, while 34% were between the ages of 36 and 54.**

50% of those who continued were millennials, between the ages of 18 and 34.

Source: Ipsos, Global Market Research, commissioned by Microsoft, July 2016.

An Industry Wide Problem





Protect yourself from tech support scams

- Microsoft does not send unsolicited email messages or make unsolicited phone calls to request for personal or financial information, or fix your computer.
- Microsoft will never proactively reach out to you to provide unsolicited PC or technical support → Any communication we have with you must be initiated by you.
- Don't call the number in pop-ups → Microsoft's error and warning messages never include a phone number.
- Report it
  - www.microsoft.com/reportascam

Microsoft | FRAUD WATCH NETWORK

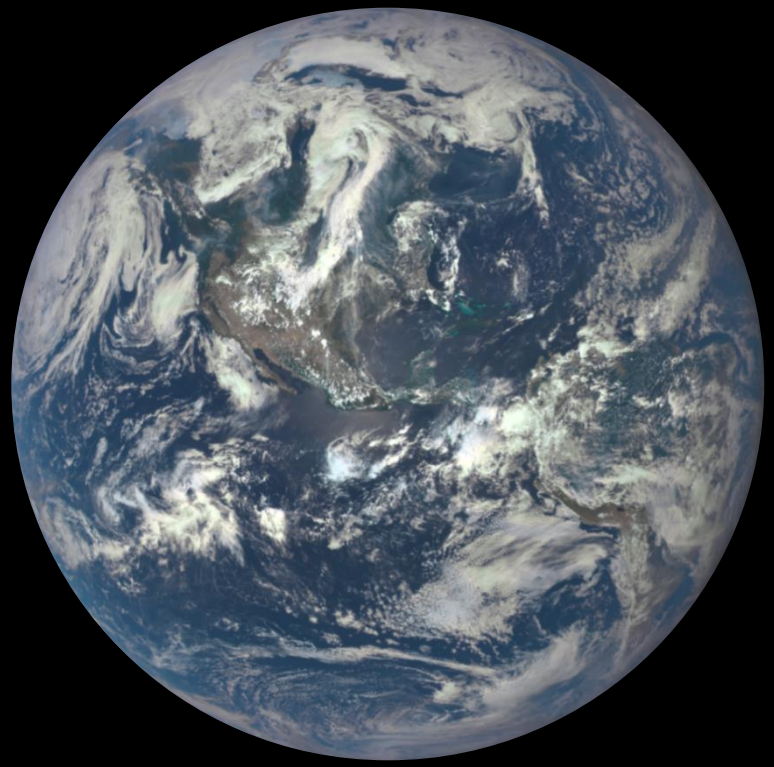
Jatketaan keskustelua…

Mikko Viitaila
Teknologiajohtaja, National Technology Officer (NTO)
Microsoft Oy

mikko.viitaila@microsoft.com
@mikkoviitaila
www.linkedin.com/in/viitaila
+358 40 8098757

Microsoft mission

Empower every person and every organization on the planet to achieve more



Microsoft