BeConnected day

BeConnected day

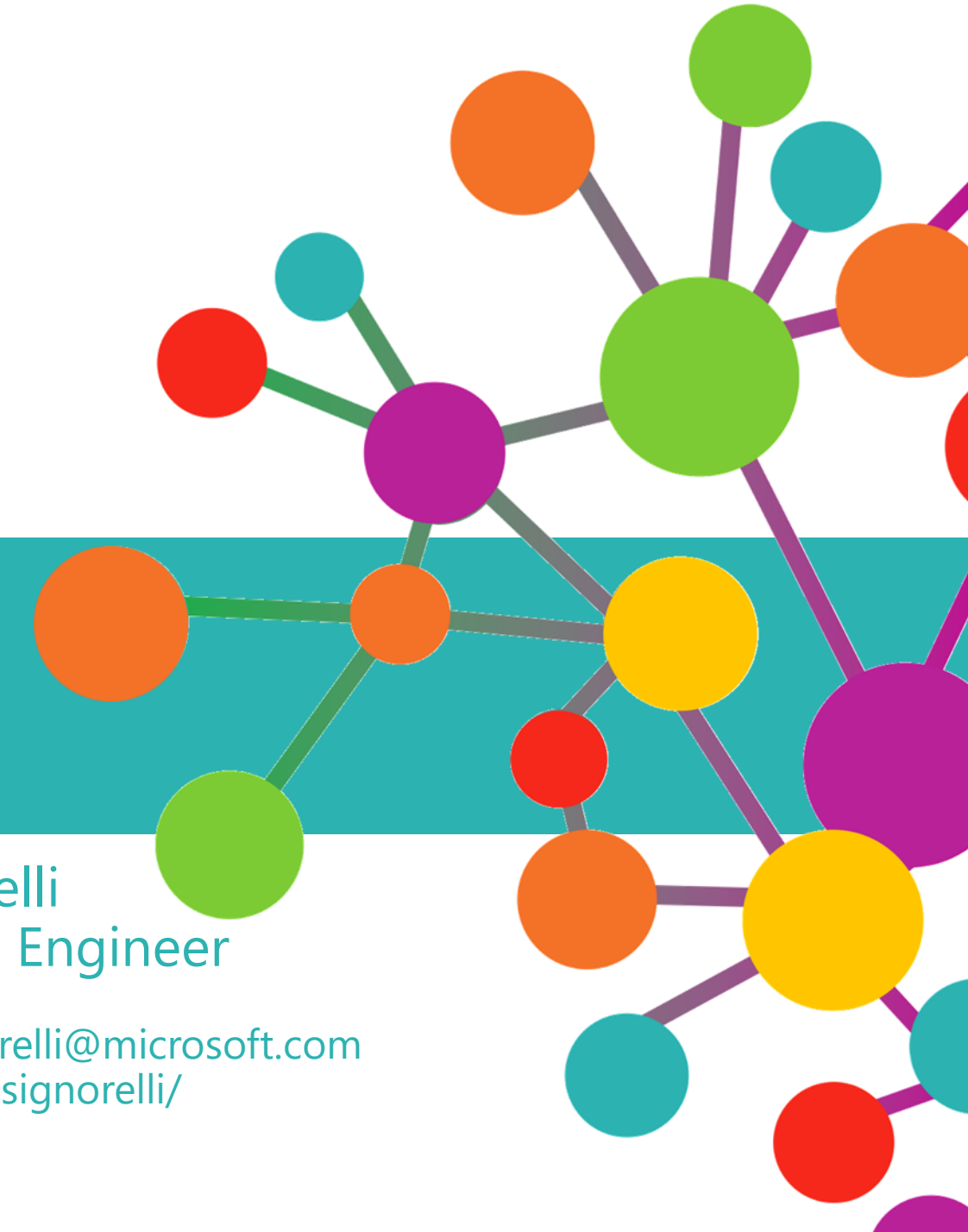
Office 365 Security:
Top customer's mistakes and remediation

Andrea Tedeschi
Sr. Premier Field Engineer

Email antede@microsoft.com
LinkedIn: /in/andreatedeschi/

Denis Signorelli
Premier Field Engineer

Email denis.signorelli@microsoft.com
LinkedIn: /in/denisignorelli/



BeConnected day

Agenda:

- ✓ Secure Modern Workplace
- ✓ Typical deployment vs Kill Chain
- ✓ Customer’s mistakes to avoid

Secure Modern Workplace

BeConnected day

Microsoft 365 helps create a secure modern workplace…

Identity & access management

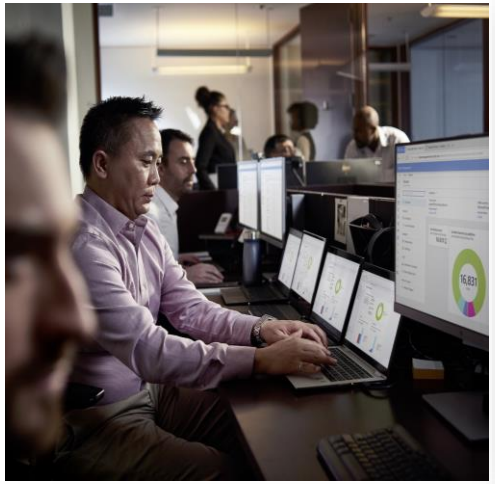
Secure identities, control access

Information protection

Protect your sensitive data– wherever it travels.

Discover and respond

Identify, collect and produce content



Data governance

Manage content lifecycle

Manage risks

Enforce communication compliance policies, detect malicious content

BeConnected day

Microsoft Cloud Security Controls & Certifications…

Controls

More than 950 Office 365 controls

- Access control
- Auditing and logging
- Identification and authorization
- Awareness and training
- Continuity planning
- Incident response
- Risk assessment
- Communication protection
- Information integrity
- Deployment Approvals and management

Ongoing compliance processes

- Recurring audits like SOC, FEDRAMP, ISO+ independent verification

Certification

Microsoft Cloud Services Verified with International, Regional and Industry specific standards and terms

Strong Privacy and Security Commitments

- ISO 27001
- ISO 27018
- EU Model Clauses (EUMC)
- GDPR Compliant
- HIPAA Business Associated Agreement
- SSAE 16 SOC 1 & SOC 2 Reports
- FedRAMP Moderate and High
- IRS 1075, UK Official (IL2)
- Health Information Trust Alliance (HITRUST)

Contractual commitment to meet US and EU data residency requirements

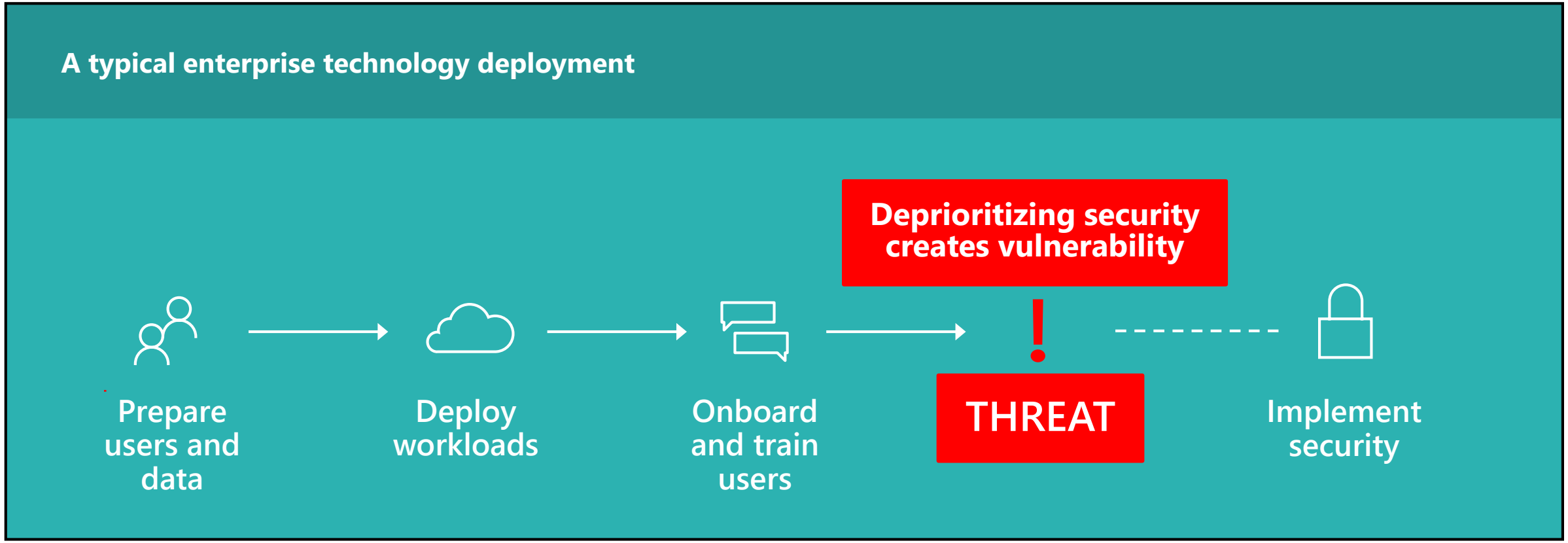
Security

Security by design

- Data Encryption at rest and in transit
- Dedicated security professionals
- Threat models, Security Reviews, Automated Security Tools
- Penetration testing with regular rotation of 3rd party penetration testers
- All keys stored in Azure Key Vault
- Admin: Screening, training, access control
- Host: Access control, anti-malware, patch management, AAD Modern Authentication
- Network: Firewalls, edge routers
- Facility: Physical controls, video surveillance, access control
- Bug Bounty Program (We pay friends, hackers and researchers to find security bugs)

Typical deployment vs Kill Chain

What happens when security is secondary



BeConnected day

Protection across the attack Kill Chain

Microsoft Cloud App Security

Extends protection & conditional access to cloud apps

Exfiltrate data

Attacker accesses sensitive data

Office 365 ATP

Malware detection, safe links, safe attachments, anti-spoofing

Phishing mail

Open attachment

Click a URL

Browse to a website

Azure AD Identity Protection

Identity protection & conditional access

Brute force account or use stolen account credentials

Attacker collects **reconnaissance & configuration data**

Exploitation & Installation

Command & Control

User account is **compromised**

Attacker attempts lateral movement

Privileged account **compromised**

Domain **compromised**

Microsoft Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Azure ATP

Identity protection

99% of the breaches didn't occur because of technology failures...

Time to avoid human mistakes!

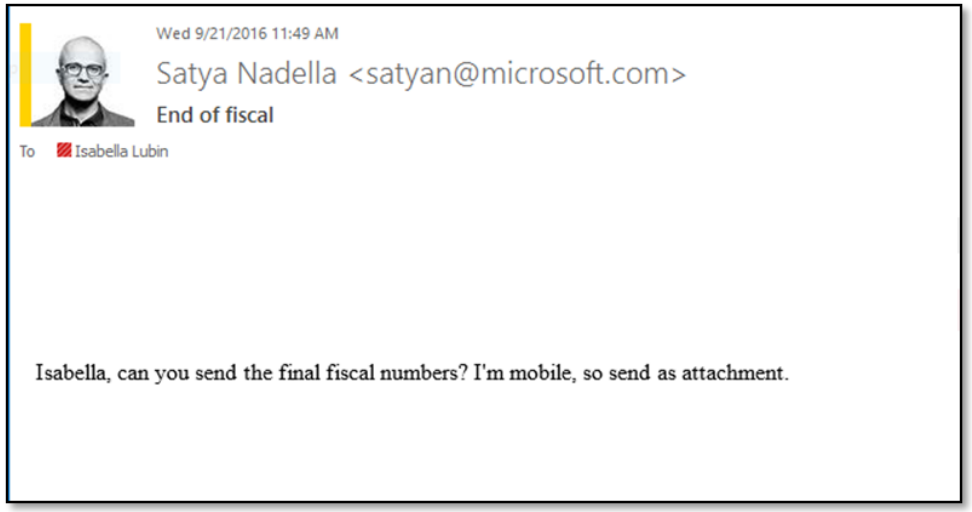
Top mistakes to avoid

BeConnected day

Mistake #1 : Usage of Exchange Online Safe Lists…

- Domain Allow / Sender Allow Lists
  - Customer own domain in Allow List (50% customers affected)
  - Presence of several domains: microsoft.com, salesforce.com, gmail.com…
  - Sender exact domain and addresses can be impersonated very easily

- IP Allow List
  - Any external sender can be spoofed or impersonated very easily



BeConnected day

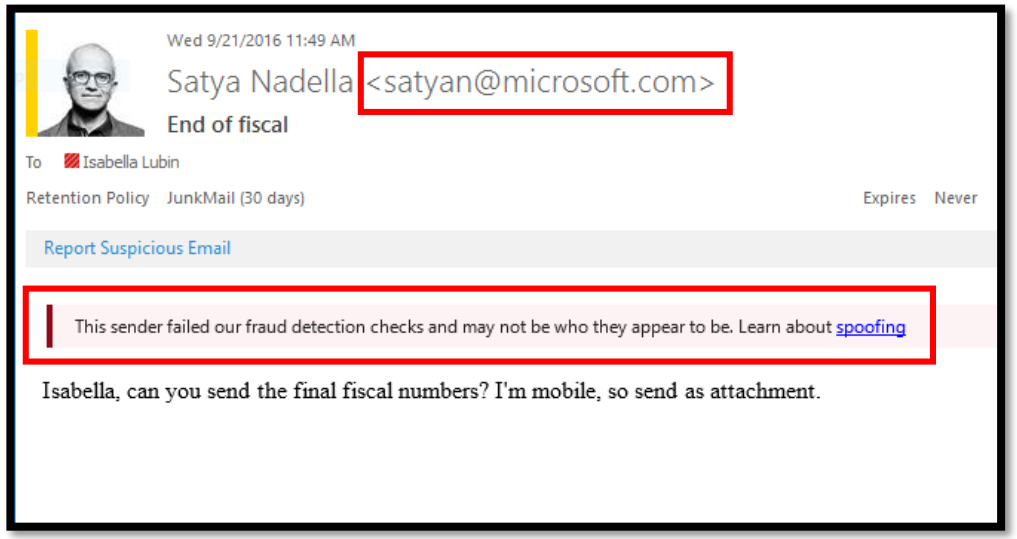
Mistake #1 : Usage of Exchange Online Safe Lists…

- Reduce or avoid the usage of safe lists

- DO NOT put your own domains in the safe lists!
- DO NOT put famous brands in the safe lists (microsoft.com)

- Use Transport Rules and leverage **Authentication-Results** header
  - Using SPF, DKIM, DMARC and Composite Auth results is safer

Mistake #2 : Sender Authentication, Spoofing & Phishing



Using your exact addresses to phish your customers or your own users

Very difficult for users to detect if it's a legitimate message or a fake email

Sender Authentication is the key

Customers don't implement Sender Authentication correctly…

BeConnected day

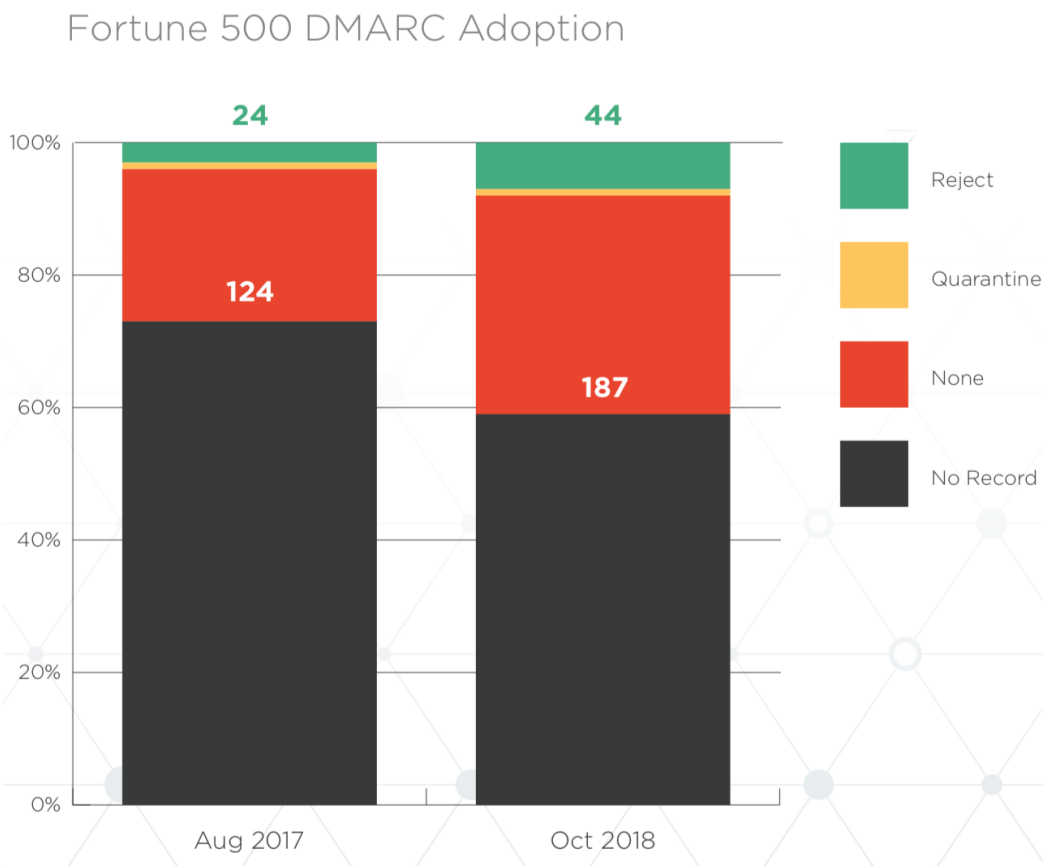
Mistake #2 : Sender Authentication, Spoofing & Phishing

- SPF record not registered or wrongly defined:
  - Syntax Errors (i.e. includes, too many DNS Lookups, etc)
  - Qualifiers (i.e. -all is omitted, ?all SPF Neutral)
  - Multiple Records (and with different content as well)

- DKIM almost always not enabled on custom domains
  - Defaults to tenant domain signature keys -> not effective

Mistake #2 : Sender Authentication, Spoofing & Phishing

- DMARC is the only effective way to protect your brand from spoofing (SPF and DKIM alone does not)
- DMARC almost always not deployed in Italy
- Unprotected parked domains
  - Can be leveraged for spoofing



BeConnected day

Mistake #3 : Impersonation protection missing or misconfigured…

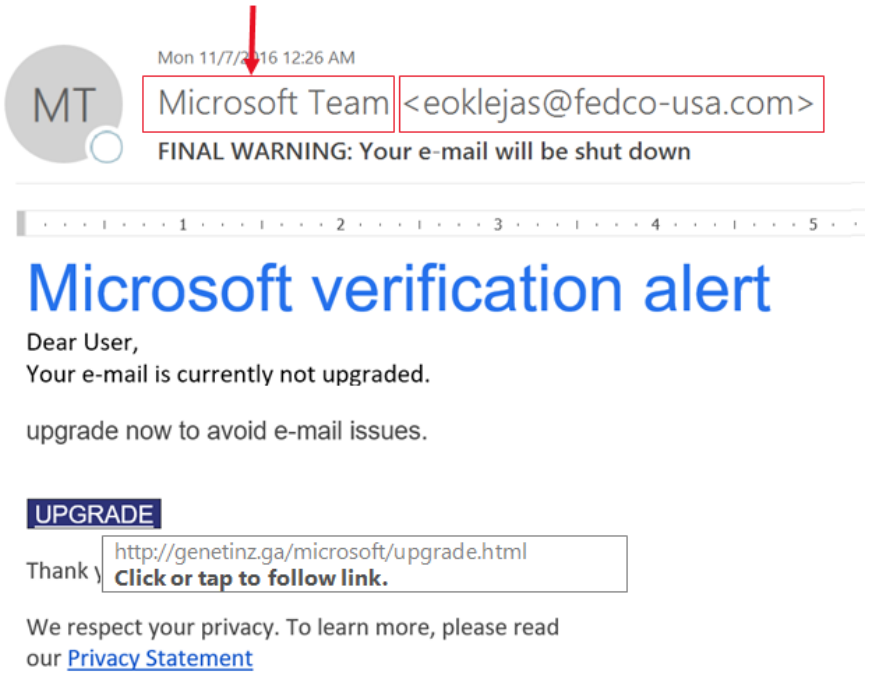
Look-alike spoofing / "typo squatting"

Sender Authentication is ineffective since attacker can register his own records.

End User Training is the key!

Office 365 ATP domain and user impersonation protection helps.

Mistake #3 : Impersonation protection missing or misconfigured…



Display name spoofing

54% of attacks leverage impersonated brands in display name

Sender Authentication won't help…

End User Training is key!

Office 365 ATP user impersonation protection helps again here!

BeConnected day

Mistake #3 : Impersonation protection missing or misconfigured…

Common errors in ATP Anti-Impersonation configuration:

- Protected Users and Policy Scope mis-interpretation
- Feature enabled only on a small subset of users
- Safe lists bypass controls and can allow impersonating addresses

BeConnected day

Mistake #4 : Automatic mail forwarding to external…

Commonly used by attackers after gaining access to mailboxes

- SMTP Forwarding Address
- Inbox Rules with forwarding action

How can we protect from this?

1) Identify or monitor who's using them
2) Leverage alerts and reports in Security & Compliance
3) Block email forwarding via Transport Rules

BeConnected day

Mistake #5 : 0-day protection not available or incorrectly configured

Anti-malware signatures aren't effective against 0-day threats

Office 365 ATP is the key for an efficient protection

- Office 365 ATP enabled only for a subset of users
- Safe Attachments for SPO, OD and Teams not enabled
- Download of infected files not blocked

- Safe Links URL rewrite not enabled for internal traffic
- Safe Links URL check disabled on Office ProPlus, iOS, Android

Mistake #5 : 0-day protection not available or incorrectly configured

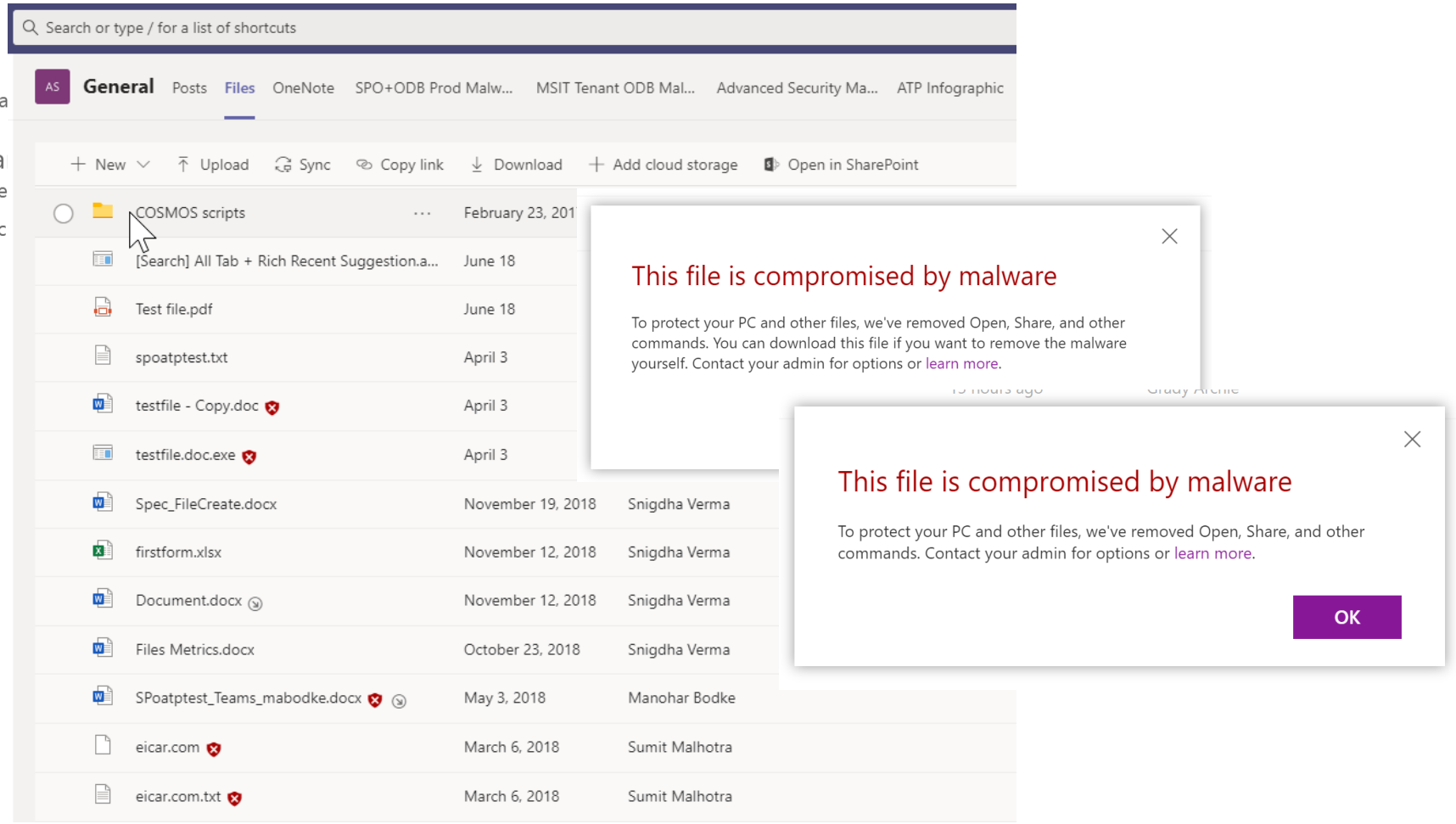
Safe attachments

Use this page to protect your organization from ma

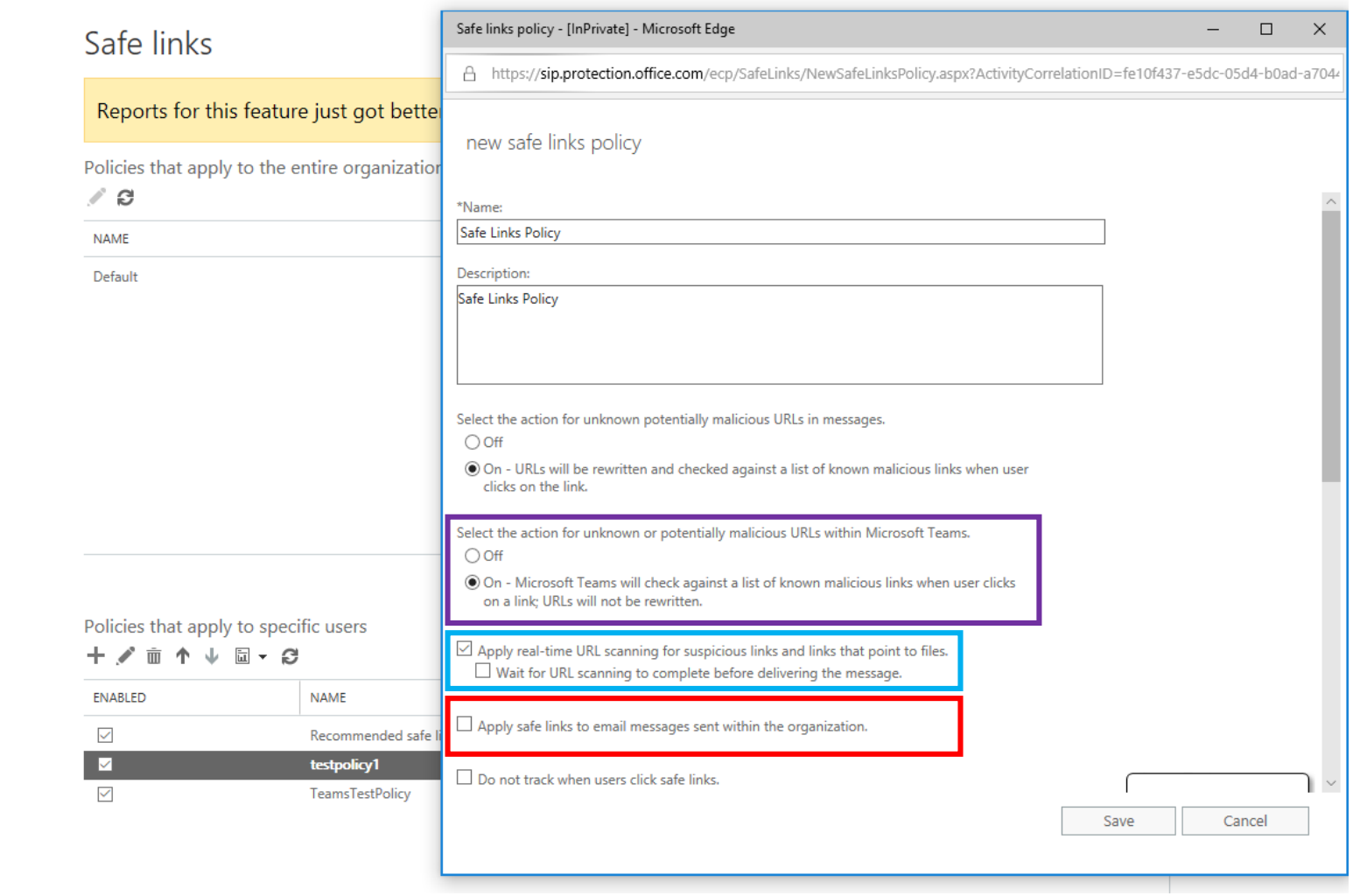
Protect files in SharePoint, OneDrive, a

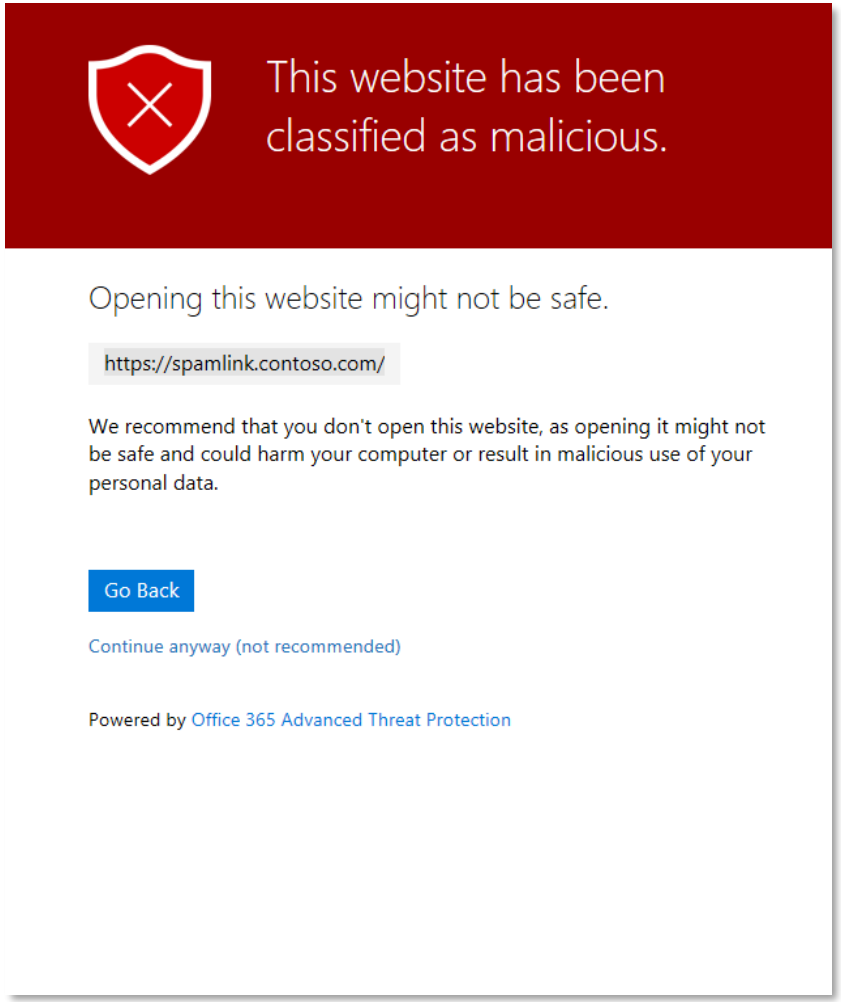
If a file in any SharePoint, OneDrive, or Microsoft Te

☑ Turn on ATP for SharePoint, OneDrive, and Mic



Mistake #5 : 0-day protection not available or incorrectly configured





BeConnected day

Mistake #6 : Auditing, Logs Retention and SIEM not in use…

Audit Logs are the key for detecting signals and perform forensics

- Exchange Mailbox auditing not enabled (MailboxLogin / FolderBind)
- Office 365 Alerting (event based) not configured
- Missing retention process for audit logs:
  - Unified Audit Logs Retention limited to 90 days
  - Message Trace limited to 90 days
- Missing integration with SIEM
  - Office 365 Activity API -> Log Analytics -> Azure Sentinel (SIEM)

BeConnected day

Mistake #7 : Authentication Security not optimized…

ADFS widely used in the past to implement SSO with O365

Misconfigurations on ADFS can increase vulnerability of accounts

- Farms with Web Application Proxy not deployed
  - Customer publishing Intranet ADFS directly!!
- ADFS Soft-Lockout and Smart-Lockout not enabled on WAP
  - Protection against credential harvest attacks
- ADFS Login Audit monitoring not implemented
  - AADConnect Health Agent for ADFS

BeConnected day

Mistake #7 : Authentication Security not optimized

Is ADFS still required to obtain SSO for Office 365?

Today it's possible to obtain SSO in different ways:

- Pass-Through Authentication + SSSO
- Password Hash Sync + SSSO

- PHS very often is not implemented by customers
  - Leaked Credential Detection
  - Backup Method for Authentication

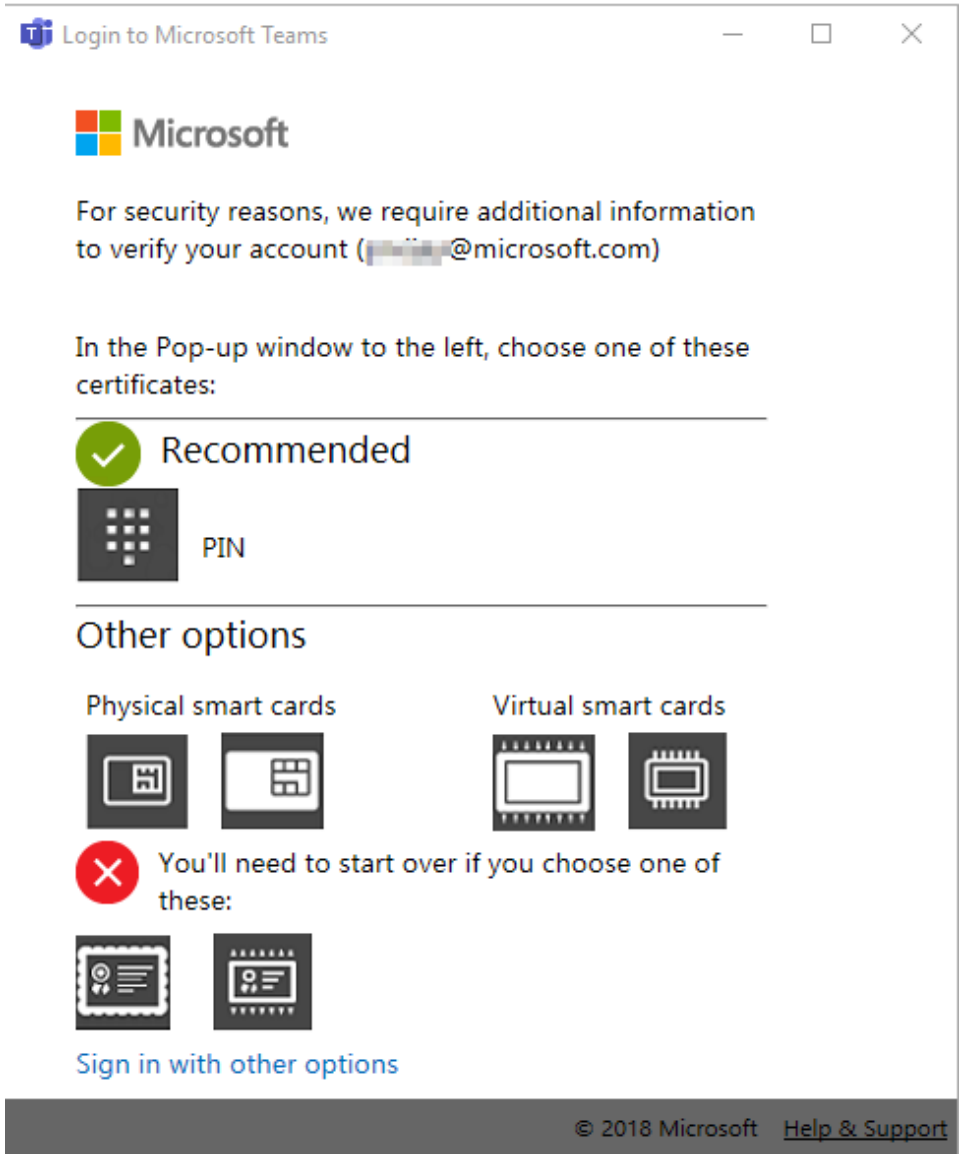
BeConnected day

Mistake #8 : Multi-Factor Authentication still not implemented…

81%

of breaches leverage stolen or weak passwords

- Microsoft Authenticator
- Windows Hello
- Hard Tokens OTP
- SMS, Voice
- Push Notification
- FIDO2 Security key



MFA prevents 99.9% of identity attacks

BeConnected day

Mistake #8 : Multi-Factor Authentication still not implemented…

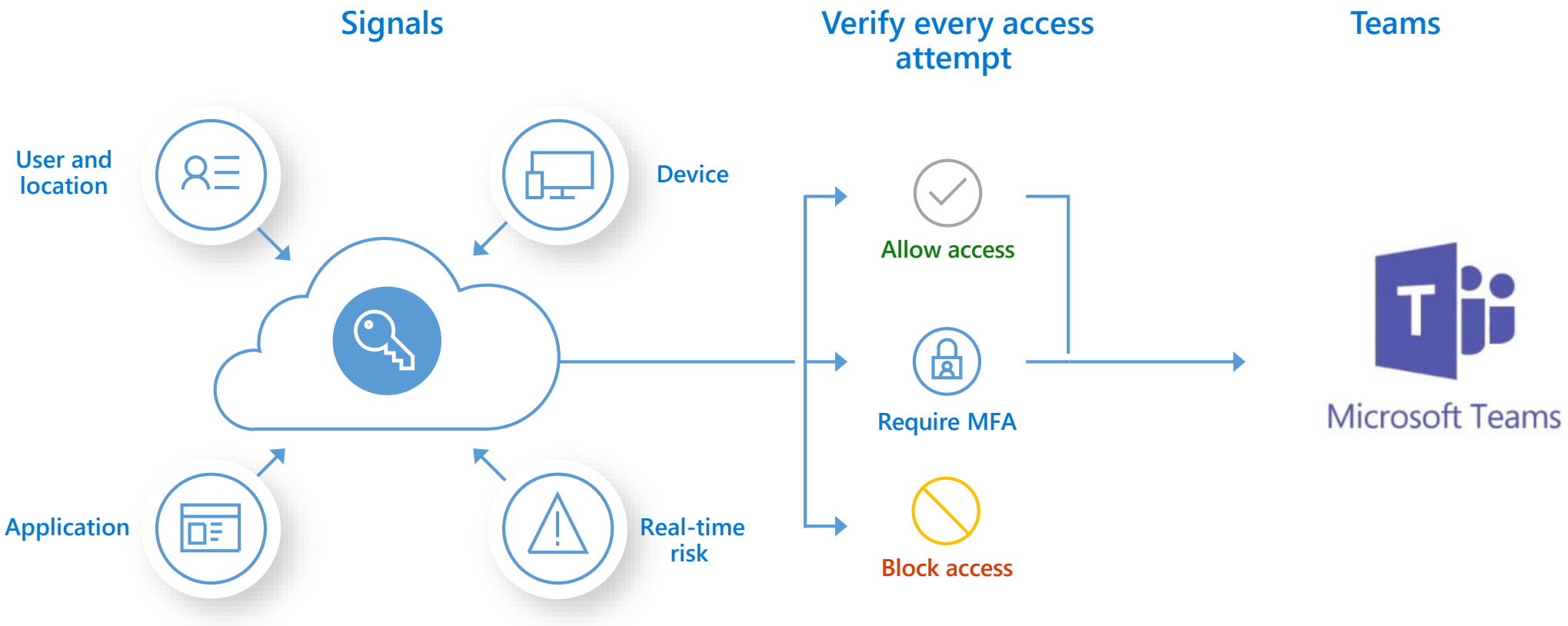
- Tenants with Modern Authentication still disabled (for EXO/SfB)
- Multifactor Authentication not enabled for Global Admins
- Multifactor Authentication not enabled for Service Admins
- Multifactor Authentication not enabled for Users

Office 365 MFA is included in all subscriptions
MFA reduces the account compromise by 99,9%!!

BeConnected day

Mistake #8 : Multi-Factor Authentication still not implemented…

- MFA enforcement based on location -> weak condition
- MFA enrolment permitted on external network -> avoid



Q&A

BeConnected day