



BeConnected *day*



BeConnected *day*

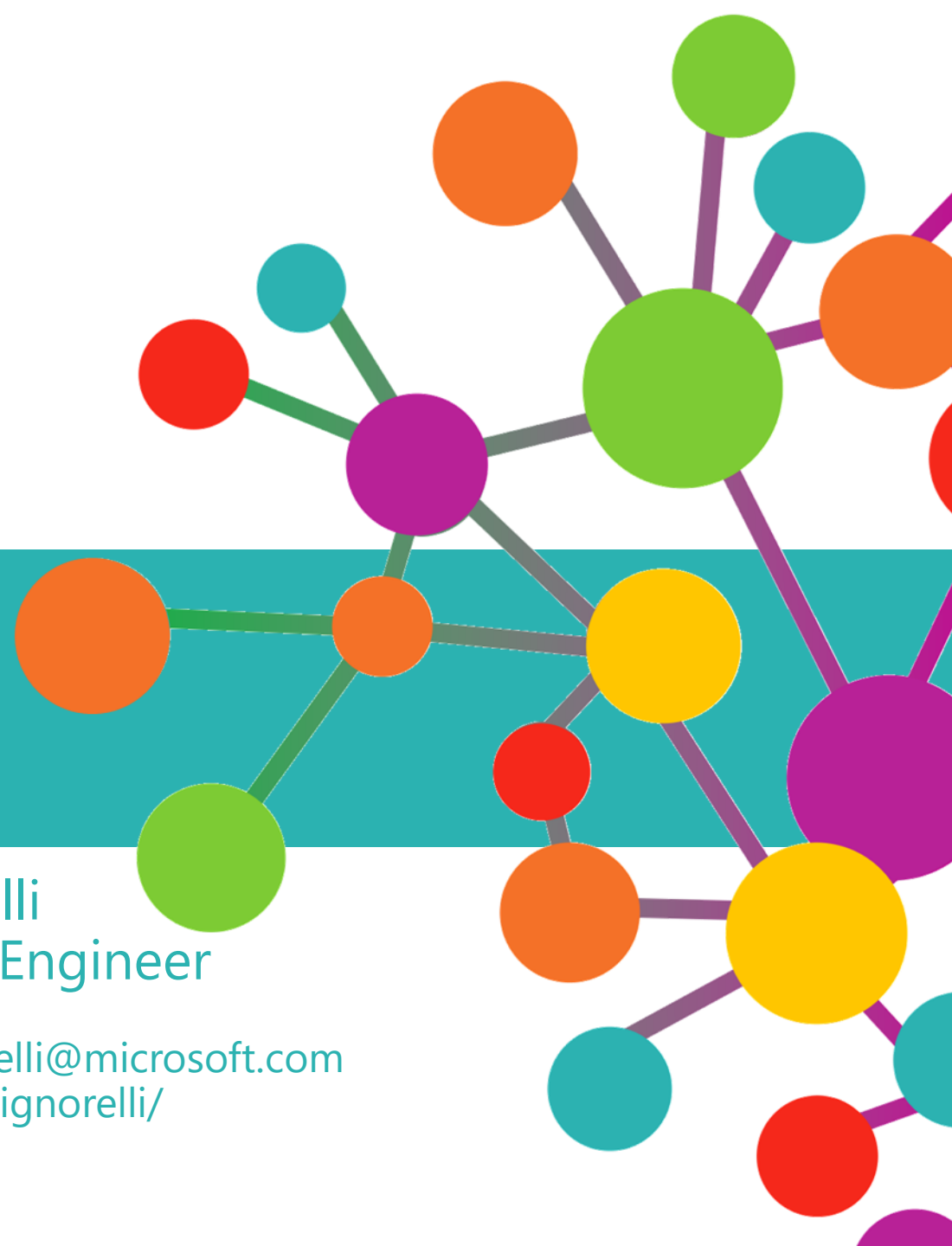
Office 365 Security: Top customer's mistakes and remediation

Andrea Tedeschi
Sr. Premier Field Engineer

Email antede@microsoft.com
LinkedIn: [/in/andreatedeschi/](https://www.linkedin.com/in/andreatedeschi/)

Denis Signorelli
Premier Field Engineer

Email denis.signorelli@microsoft.com
LinkedIn: [/in/denisignorelli/](https://www.linkedin.com/in/denisignorelli/)



Agenda:

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



Secure Modern Workplace



Identity & access management

Secure identities,
control access



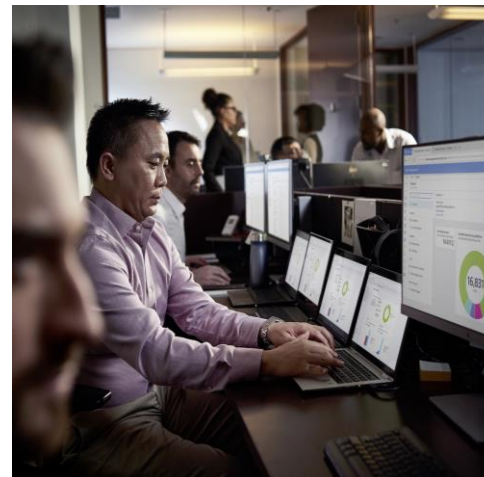
Information protection

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

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

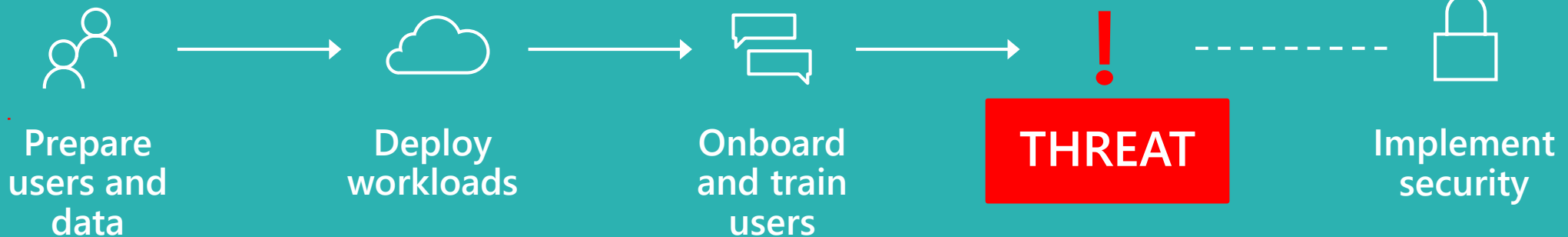
Security

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

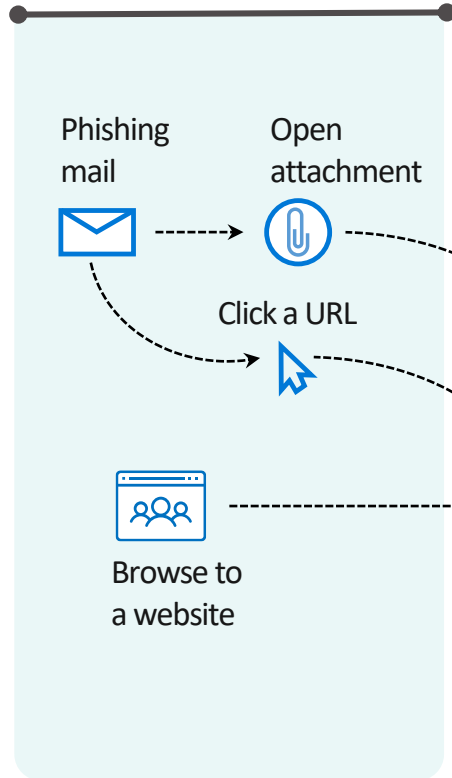
A typical enterprise technology deployment



Protection across the attack Kill Chain

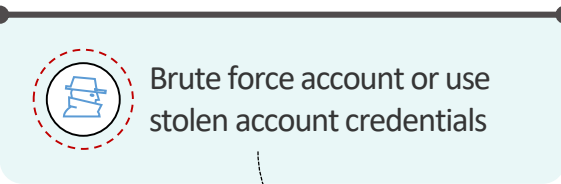
Office 365 ATP

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



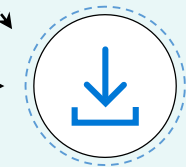
Azure AD Identity Protection

Identity protection & conditional access



Exploitation & Installation

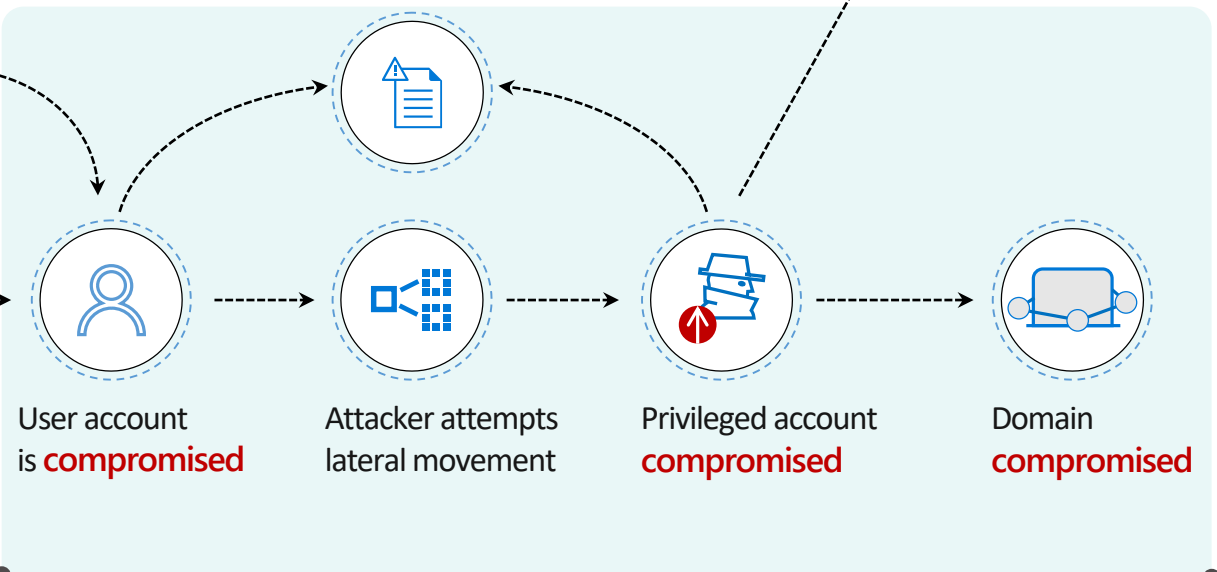
Command & Control



Microsoft Defender ATP

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

Attacker collects **reconnaissance & configuration data**

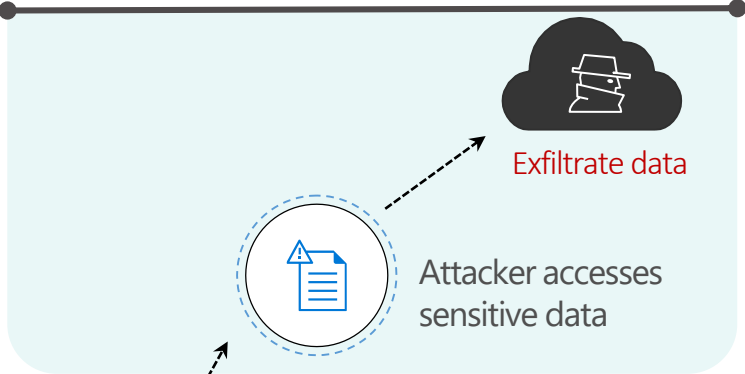


Azure ATP

Identity protection

Microsoft Cloud App Security

Extends protection & conditional access to cloud apps



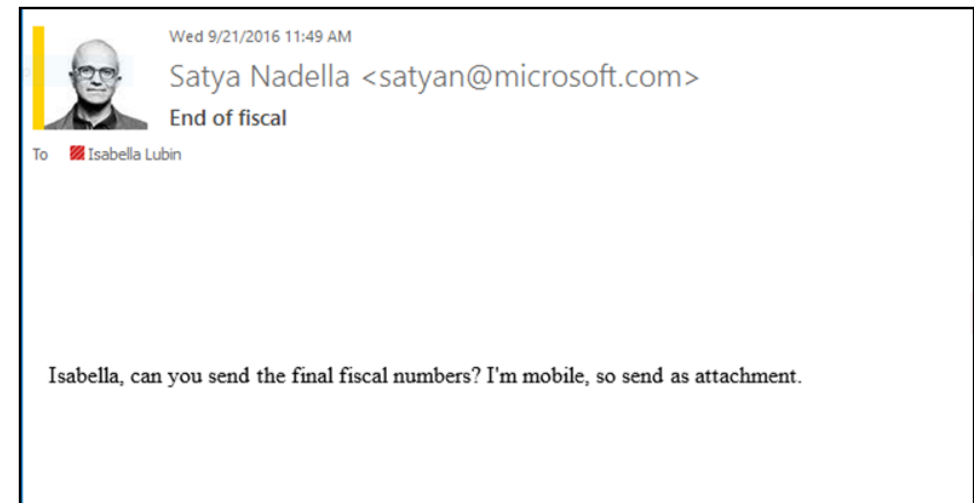
99% of the breaches didn't occur
because of technology failures...

Time to avoid human mistakes!



Top mistakes to avoid

- 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



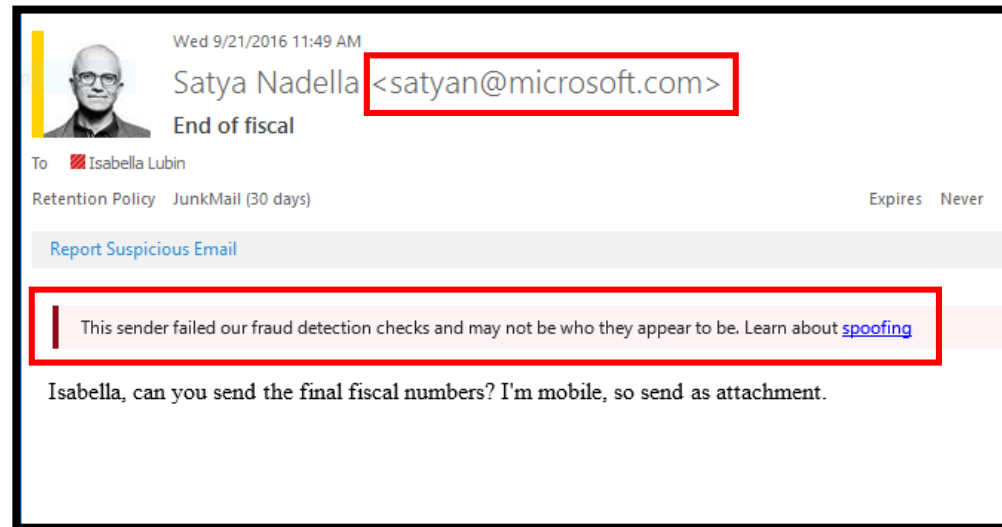
- Reduce or avoid the usage of safe lists
- DO NOT put your own domains in the safe lists!
- DO NOT put famous brands in the safe lists (microsoft.com)
- Use Transport Rules and leverage **Authentication-Results** header
 - Using SPF, DKIM, DMARC and Composite Auth results is safer

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

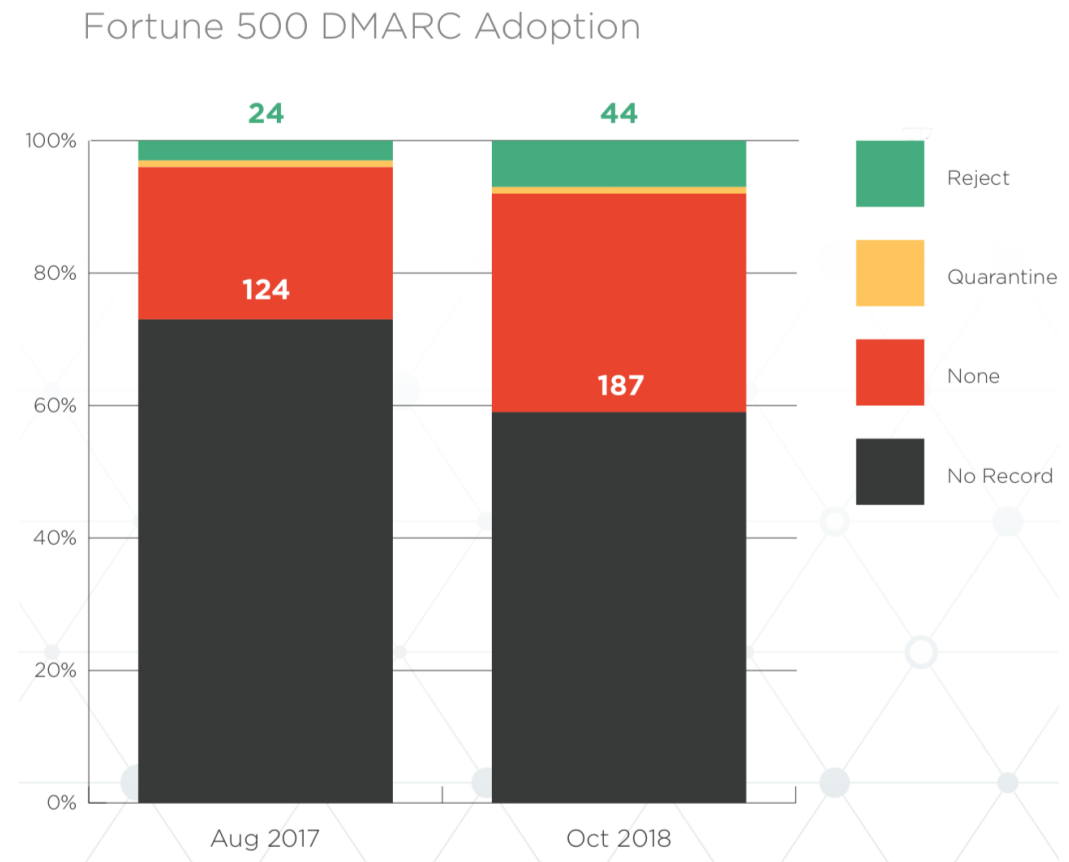


Customers don't implement Sender Authentication correctly...

- 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



Mistake #3 : Impersonation protection missing or misconfigured...

Look-alike spoofing / “typo squatting”

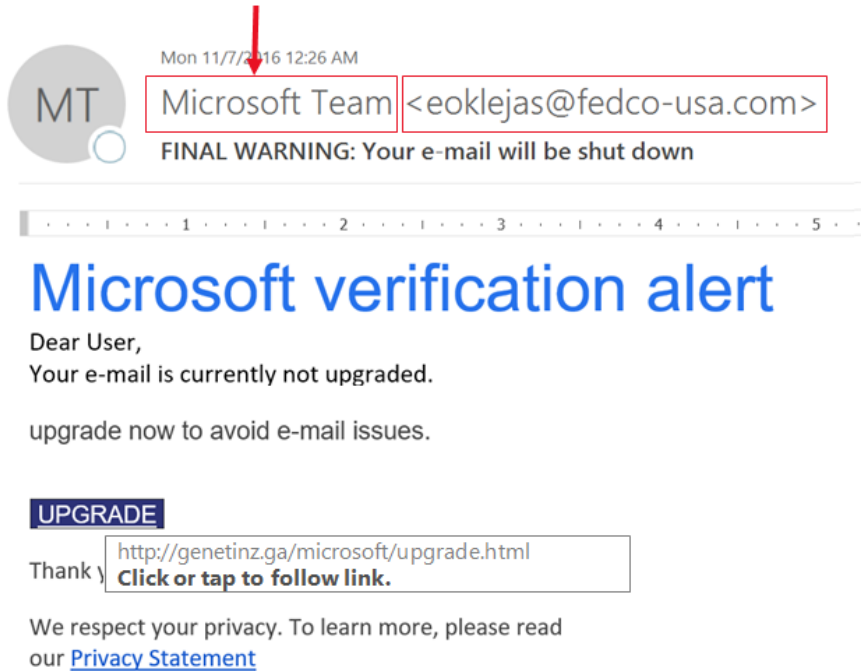
Sender Authentication is ineffective since attacker can register his own records.



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!

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

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

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, and Microsoft Teams
If a file in any SharePoint, OneDrive, or Microsoft Teams

☒ Turn on ATP for SharePoint, OneDrive, and Mic

The screenshot shows a SharePoint interface with a search bar at the top. Below the search bar, there are tabs for 'General', 'Posts', 'Files', 'OneNote', 'SPO+ODB Prod Malw...', 'MSIT Tenant ODB Mal...', 'Advanced Security Ma...', and 'ATP Infographic'. The 'Files' tab is selected. Below the tabs, there are buttons for '+ New', 'Upload', 'Sync', 'Copy link', 'Download', 'Add cloud storage', and 'Open in SharePoint'. The file list shows a folder named 'COSMOS scripts' and several files. Two files, 'testfile.doc' and 'testfile.doc.exe', are marked with red 'X' icons, indicating they are compromised. A warning message is displayed on the right side of the screen.

File Name	Icon	Date	Owner
COSMOS scripts	Folder	February 23, 2018	
[Search] All Tab + Rich Recent Suggestion.a...	Document	June 18	
Test file.pdf	PDF	June 18	
spootptest.txt	Text	April 3	
testfile - Copy.doc	Document	April 3	
testfile.doc.exe	Document	April 3	
Spec_FileCreate.docx	Document	November 19, 2018	Snigdha Verma
firstform.xlsx	Spreadsheet	November 12, 2018	Snigdha Verma
Document.docx	Document	November 12, 2018	Snigdha Verma
Files Metrics.docx	Document	October 23, 2018	Snigdha Verma
SPOatptest_Teams_mabodke.docx	Document	May 3, 2018	Manohar Bodke
eicar.com	Document	March 6, 2018	Sumit Malhotra
eicar.com.txt	Document	March 6, 2018	Sumit Malhotra

This file is compromised by malware

To protect your PC and other files, we've removed Open commands. You can download this file if you want to re yourself. Contact your admin for options or [learn more](#).

This file is compromised by malware

To protect your PC and other files, we've removed Open commands. Contact your admin for options or [learn more](#).

This file is compromised by malware

To protect your PC and other files, we've removed Open, Share, and other commands. You can download this file if you want to remove the malware yourself. Contact your admin for options or [learn more](#).

This file is compromised by malware

To protect your PC and other files, we've removed Open, Share, and other commands. Contact your admin for options or [learn more](#).

OK

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

Safe links

Reports for this feature just got better

Policies that apply to the entire organization



NAME

Default

Policies that apply to specific users



ENABLED

NAME



Recommended safe links



testpolicy1



TeamsTestPolicy

Safe links policy - [InPrivate] - Microsoft Edge

https://sip.protection.office.com/ecp/SafeLinks/NewSafeLinksPolicy.aspx?ActivityCorrelationID=fe10f437-e5dc-05d4-b0ad-a7044

new safe links policy

*Name:
Safe Links Policy

Description:
Safe Links Policy

Select the action for unknown potentially malicious URLs in messages.

☐ Off

☒ On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Select the action for unknown or potentially malicious URLs within Microsoft Teams.

☐ Off

☒ On - Microsoft Teams will check against a list of known malicious links when user clicks on a link; URLs will not be rewritten.

☒ Apply real-time URL scanning for suspicious links and links that point to files.
☐ Wait for URL scanning to complete before delivering the message.

☐ Apply safe links to email messages sent within the organization.

☐ Do not track when users click safe links.

Save Cancel



This website has been
classified as malicious.

Opening this website might not be safe.

<https://spamlink.contoso.com/>

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

[Go Back](#)

[Continue anyway \(not recommended\)](#)

Powered by [Office 365 Advanced Threat Protection](#)

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)

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

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

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

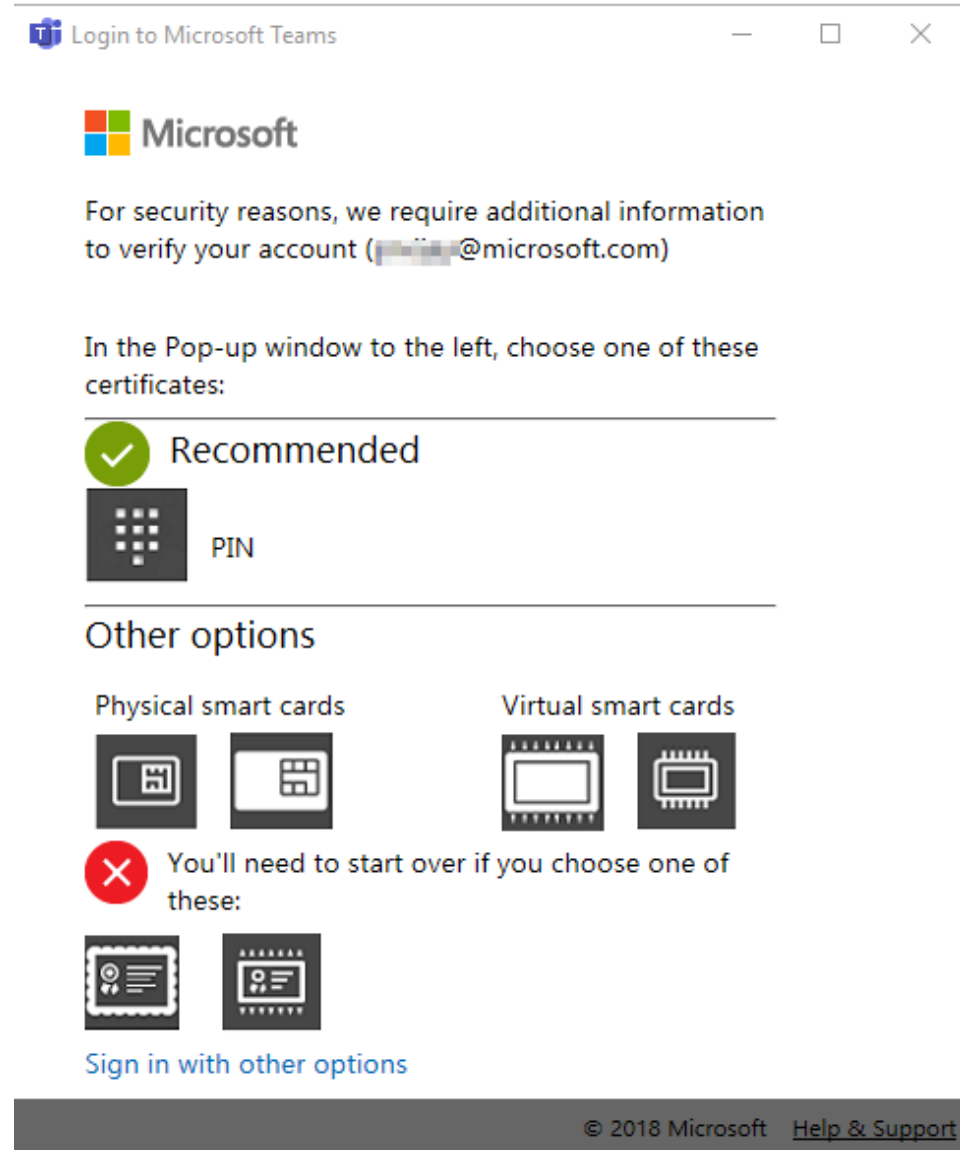


Push
Notification



FIDO2
Security key

MFA prevents 99.9% of identity attacks

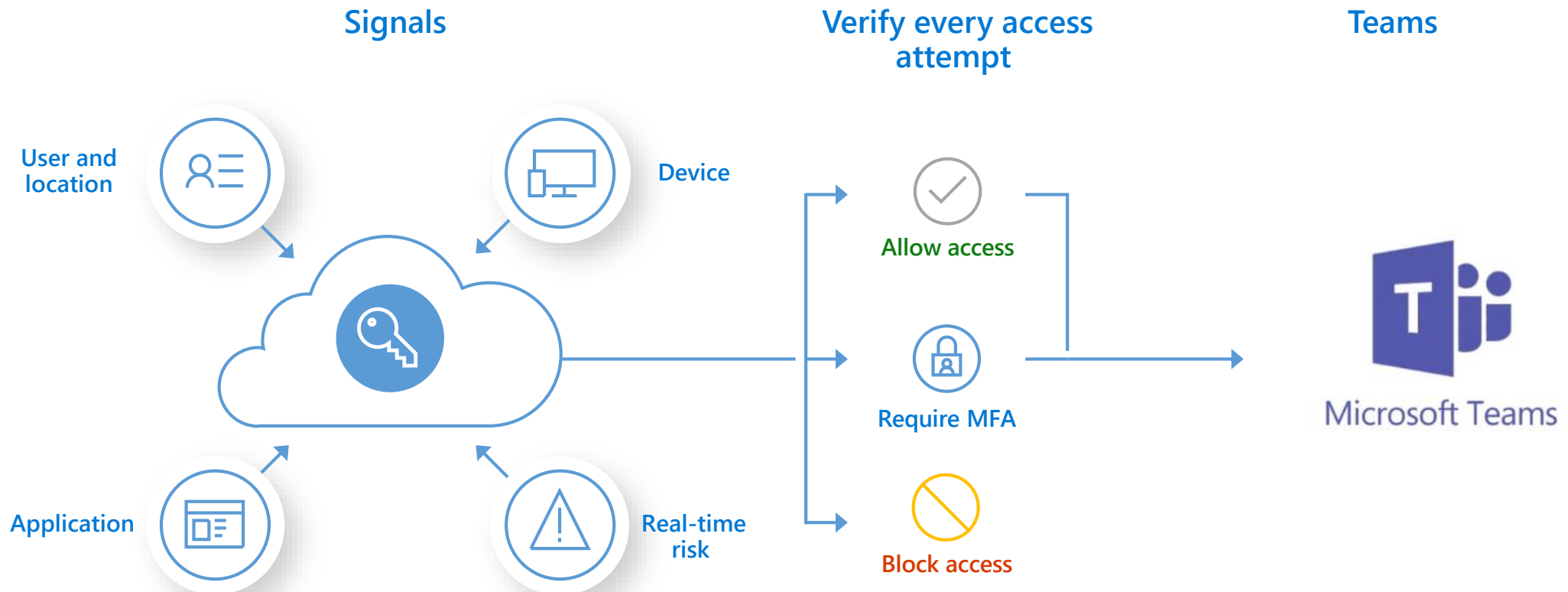


- Tenants with Modern Authentication still disabled (for EXO/SfB)
- Multifactor Authentication not enabled for Global Admins
- Multifactor Authentication not enabled for Service Admins
- Multifactor Authentication not enabled for Users

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

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*