iV4 *Webinar*

SECURING THE CLOUD

Office 365 Security Best Practices

Presented By:

Michael Montagliano
Chief Technology Officer
VP of Consulting

Ben Wilcox
Chief Technologist

iV4

Full service IT provider

Consulting, Security, Managed Services, Cloud

Microsoft Gold Partner

2017 Top 200 Microsoft Solutions Provider

2016 Microsoft SMB Northeast Cloud Partner of the Year

2015 Microsoft SMB Northeast Partner of the Year

Microsoft Cyber Defense Strategy

$15 billion dollars invested in their cloud infrastructure

$1 billion spend on security each year

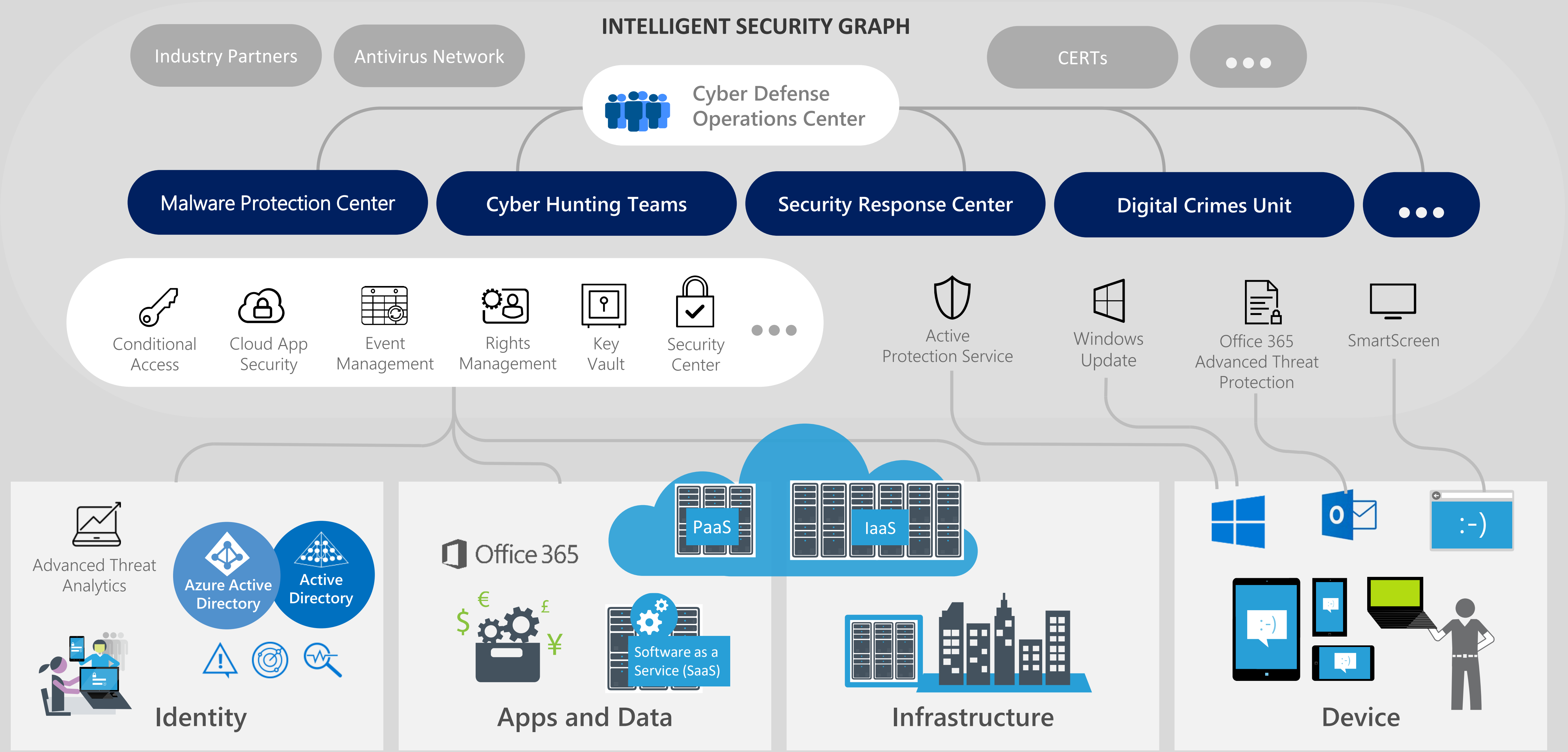
Microsoft delivers more than 200 cloud services including Bing, Outlook.com, Office 365, OneDrive, Skype, Xbox Live, and the Microsoft Azure platform

Operate the Microsoft Cyber Defense Operations Center 24x7 to protect, detect, and respond to security threats against its infrastructure and services

Microsoft ecosystem is analyzed by more than 50 security experts and data scientists connected to over 3,500 security professionals across the company

Are we, as consumers, taking advantage of all of the tools available?

Microsoft Protecting You



INTELLIGENT SECURITY GRAPH

Industry Partners

Antivirus Network

Cyber Defense Operations Center

CERTs

●●●

Malware Protection Center

Cyber Hunting Teams

Security Response Center

Digital Crimes Unit

●●●

Conditional Access

Cloud App Security

Event Management

Rights Management

Key Vault

Security Center

●●●

Active Protection Service

Windows Update

Office 365 Advanced Threat Protection

SmartScreen

Advanced Threat Analytics

Azure Active Directory

Active Directory

Identity

Office 365

PaaS

IaaS

Software as a Service (SaaS)

Apps and Data

Infrastructure

Device

Microsoft Security Trifecta

Office 365 Enterprise

Chat- centric workspace

Email & Calendar

Voice, Video & Meetings

Office applications/ co-authoring

Sites & Content Management

Analytics

Advanced Security & Compliance

Enterprise Mobility+ Security

Identity & Access Management

Managed Mobile Productivity

Information Protection

Identity Driven Security

Windows 10 Enterprise

Advanced Endpoint Security

Designed For Modern IT

More Productive

Powerful, Modern devices

Azure Active Directory
Conditional Access
Windows Hello
Windows Credential Guard

Advanced Threat Analytics
Windows Defender Advanced Threat Protection
Office 365 Advanced Threat Protection
Office 365 Threat Intelligence

Azure Information Protection
Office 365 Data Loss Prevention
Windows Information Protection
Microsoft Cloud App Security
Office 365 Advanced Security Mgmt
Microsoft Intune

Azure Security Center
Office 365 Security & Compliance Center
Windows Defender Advanced Security Center

There are 2 sides to every story…

Office 365: The Good

Benefits of Office 365

Communication and collaboration

Anywhere, any device ubiquitous access

Time to deployment and delivery

IT flexibility

Transfer of ownership and risk

Always current with latest release

iV4

Office 365: The Bad

E-Mail Threats – By the numbers

Your users' productivity and security is more challenged than ever by different types of attacks.

80 Billion

Inbound Messages to Office365 in 1 month – only 31% core business mails

55 Billion

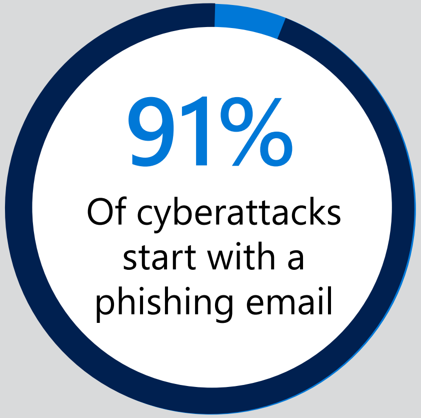
Spam and Bulk mails that could have crowded users' mailboxes

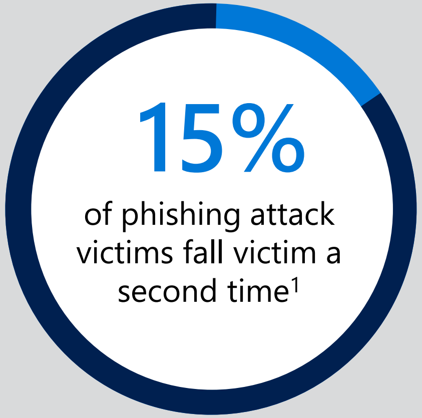
Malware ↑ 600%

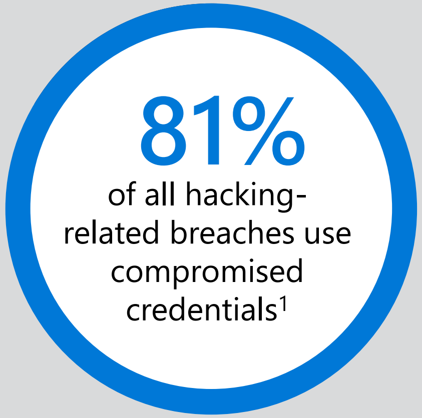
Volume of malware targeting O365 has increased 600% in the past year

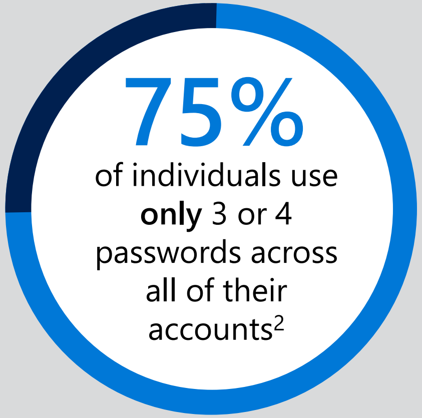
Office 365: The Bad

Most security breaches occur when attackers steal a user's identity.
Once an attacker hacks even low privileged user accounts, it's relatively easy for them to gain access to important company resources through lateral movement.


91%
Of cyberattacks start with a phishing email


15%
of phishing attack victims fall victim a second time[1]


81%
of all hacking-related breaches use compromised credentials[1]

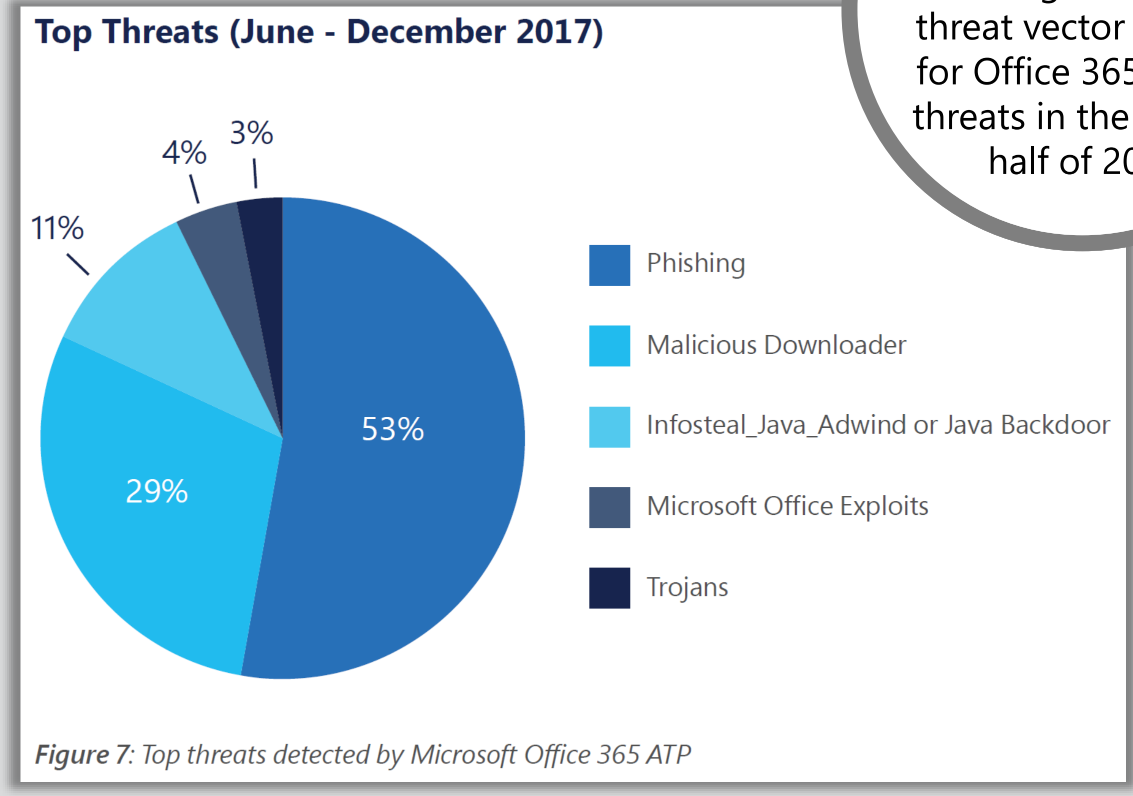

75%
of individuals use **only** 3 or 4 passwords across all of their accounts[2]

[1] Verizon 2017 Data Breach Investigations Report (ref. P11 of Security Playbook)
[2] Security Week Survey (ref. P35 of Security Playbook)
3 https://phishme.com/2016-enterprise-phishing-susceptibility-report

Office 365: Social Engineering

As software vendors incorporate stronger security measures into their products, it is becoming more expensive for hackers to successfully penetrate software.

By contrast, *it is easier and less costly* to trick a user into clicking a malicious link or opening a phishing email.



Top Threats (June - December 2017)

***Figure 7**: Top threats detected by Microsoft Office 365 ATP*

#1

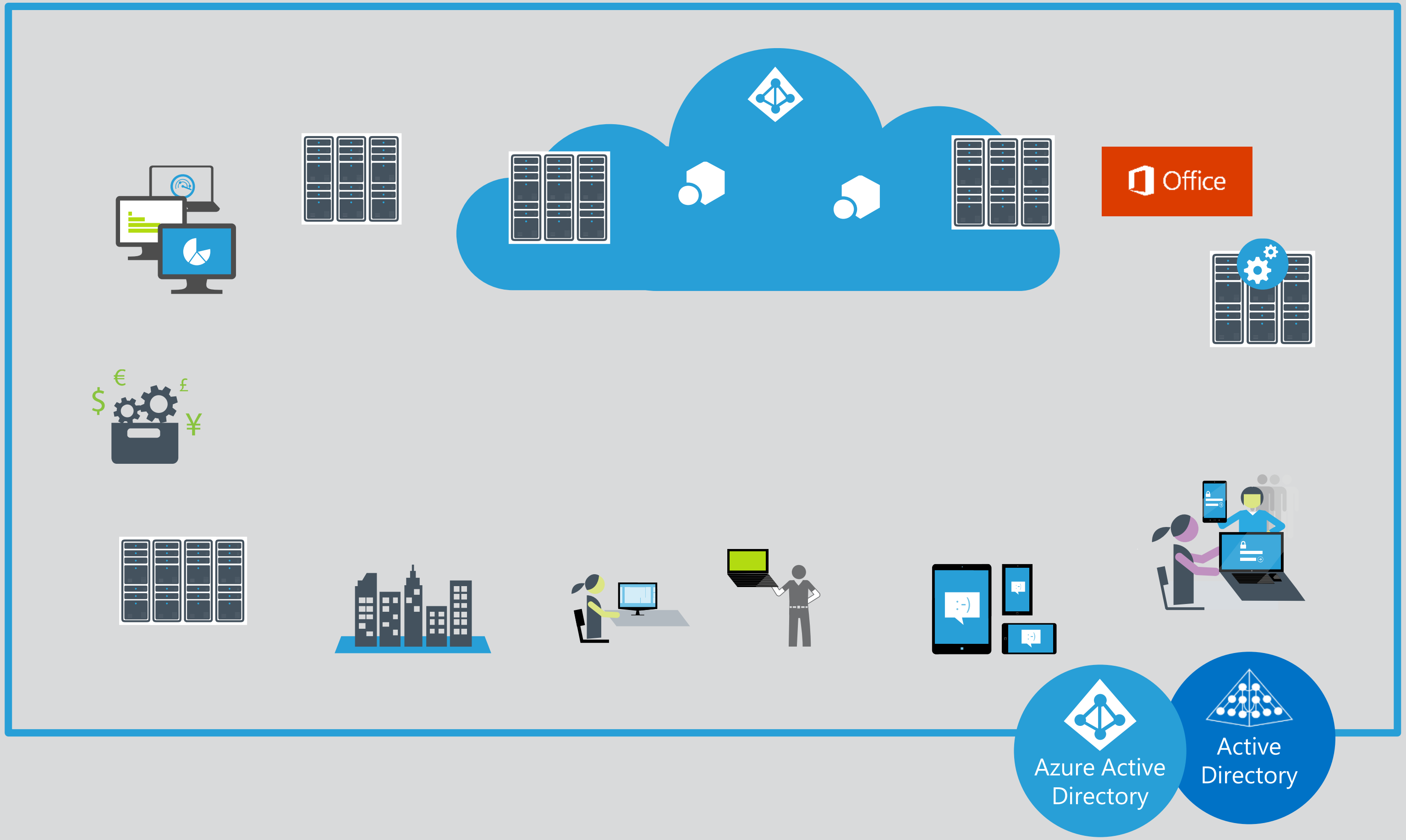
Phishing was the #1 threat vector (>50%) for Office 365-based threats in the second half of 2017

iV4

Office 365: The Bad

Identity is the new security "perimeter"

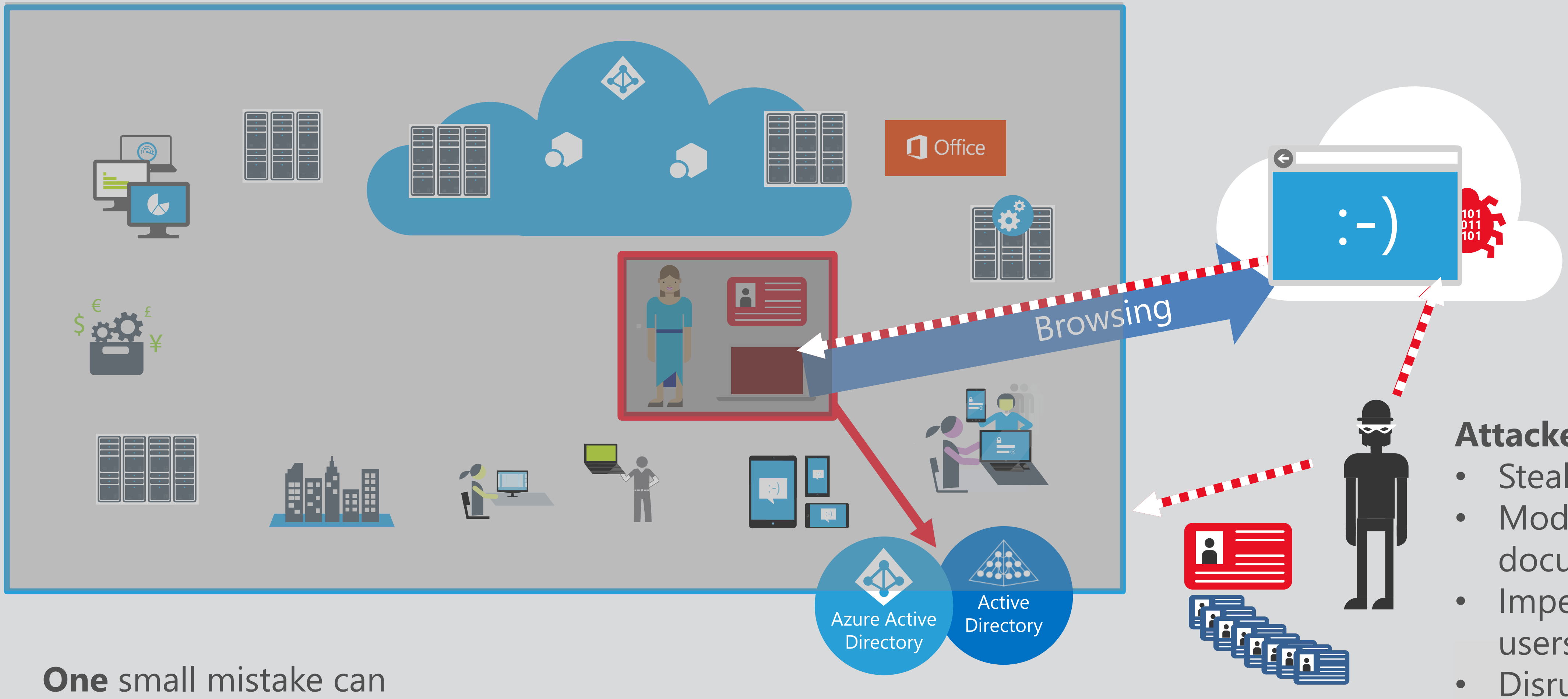
Active Directory and Administrators control all the assets



Office 365: The Bad

Identity is the new security “perimeter” under attack

Active Directory and Administrators control all the assets



Attackers Can

- Steal any data
- Modify documents
- Impersonate users
- Disrupt business operations

One small mistake can lead to attacker control

An Office 365 Security Breach That Can Happen to You

An Office 365 Security Breach That Can Happen to You

Mid-sized organization, 650 users across several states

Phishing campaign compromised key members of the c-level team

Accounts were used to phish the rest of the organization leading to dozens of credentials collected by the hackers

Required a reset of all of the accounts in the organization, many not in Active Directory

iV4

Hackers Were Able To…

1

Configure mail forwarding in a users email client and send email to a Google account using keywords associated with financial information

2

VPN into the network with credentials for any user in the VPN group in AD and expand their presence

3

Log in as an administrator to their Office 365 SharePoint site

In the world of SaaS, a username and password is all the hackers need to take over all of your accounts.

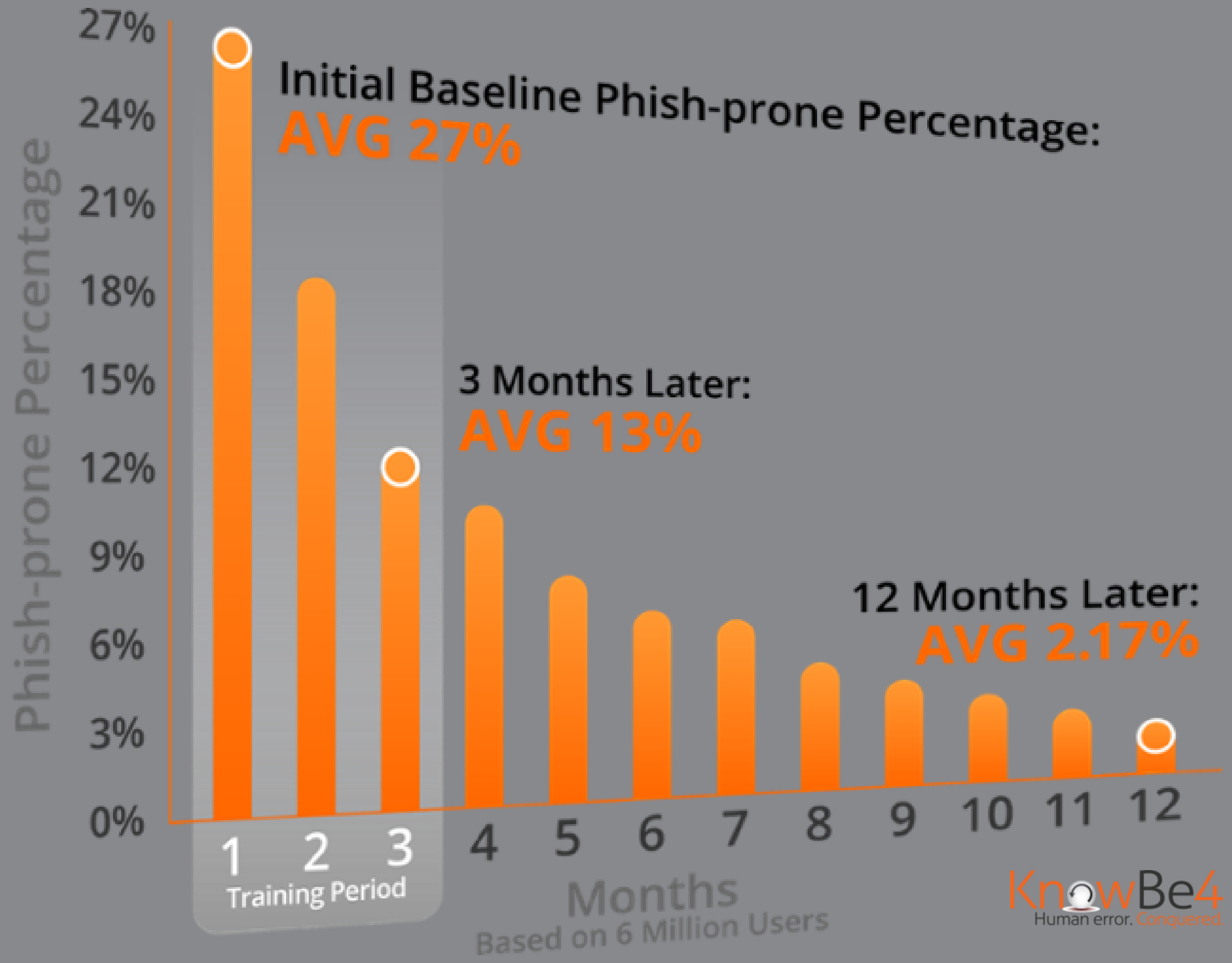
There is no need to put malware on your endpoint or get in through a Firewall. In fact, there is very little practical security after they have your username and password.

Training Your People

Habits take time to form and become part of one's daily life –

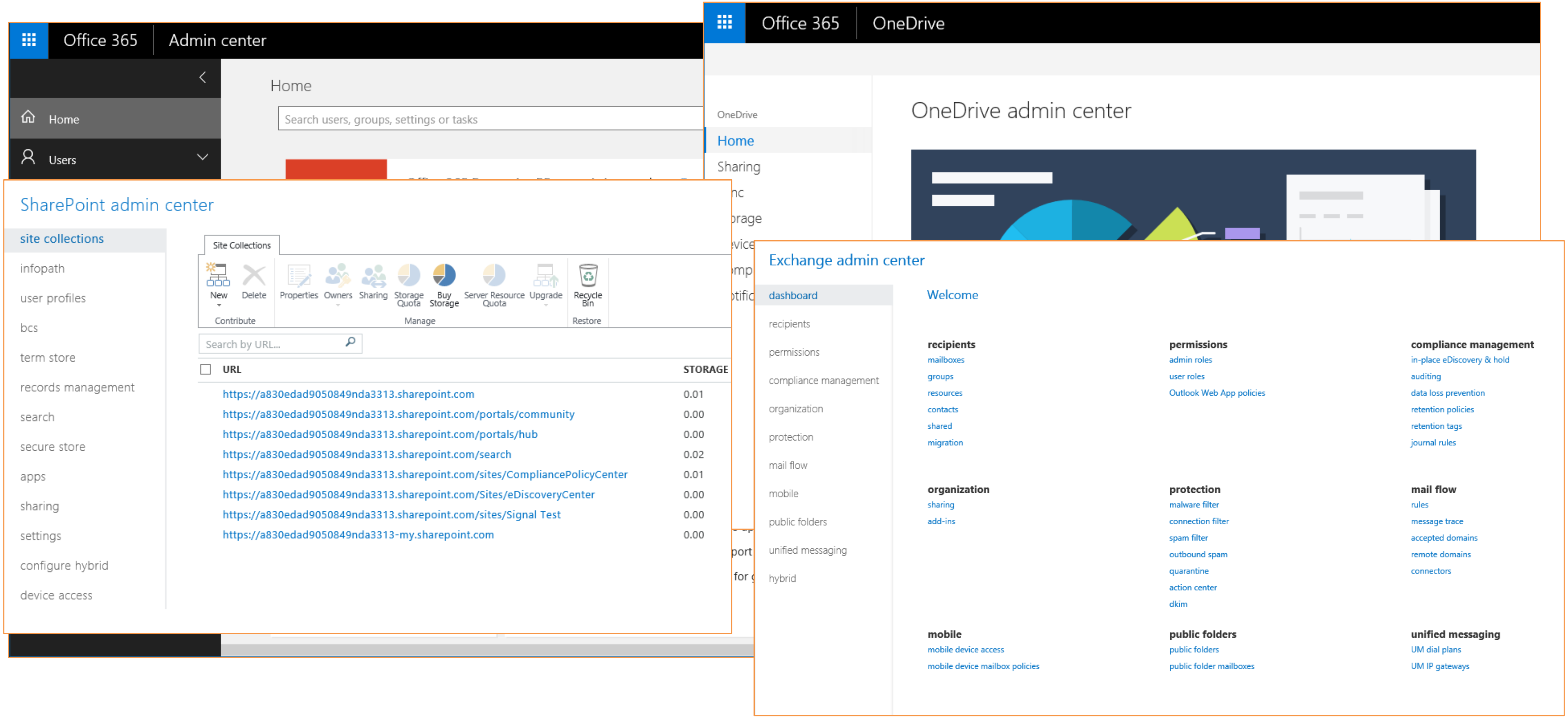
The same applies to being cyber street smart and phishing prevention.

Taking a whole organization from zero to front line defenders against cyber criminals takes gradual education, and patience in understanding the human landscape of an organization.



Avoiding The Risks:
Office 365 Secure Score - actionable security analytics

Where do I go to enable security features?



Office 365 | Admin center

Home

Users

Search users, groups, settings or tasks

Office 365 | OneDrive

OneDrive admin center

OneDrive

Home

Sharing

nc

orage

vice

mp

tific

port

for

SharePoint admin center

site collections
infopath
user profiles
bcs
term store
records management
search
secure store
apps
sharing
settings
configure hybrid
device access

URL	STORAGE
https://a830edad9050849nda3313.sharepoint.com	0.01
https://a830edad9050849nda3313.sharepoint.com/portals/community	0.00
https://a830edad9050849nda3313.sharepoint.com/portals/hub	0.00
https://a830edad9050849nda3313.sharepoint.com/search	0.02
https://a830edad9050849nda3313.sharepoint.com/sites/CompliancePolicyCenter	0.01
https://a830edad9050849nda3313.sharepoint.com/Sites/eDiscoveryCenter	0.00
https://a830edad9050849nda3313.sharepoint.com/sites/Signal Test	0.00
https://a830edad9050849nda3313-my.sharepoint.com	0.00

Exchange admin center

dashboard
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging
hybrid

Welcome

recipients
mailboxes
groups
resources
contacts
shared
migration

permissions
admin roles
user roles
Outlook Web App policies

compliance management
in-place eDiscovery & hold
auditing
data loss prevention
retention policies
retention tags
journal rules

organization
sharing
add-ins

protection
malware filter
connection filter
spam filter
outbound spam
quarantine
action center
dkim

mail flow
rules
message trace
accepted domains
remote domains
connectors

mobile
mobile device access
mobile device mailbox policies

public folders
public folders
public folder mailboxes

unified messaging
UM dial plans
UM IP gateways

Microsoft Secure Score

All Cloud Security Controls were in one place, with a score-based framework to determine what the highest impact actions are, and an easy way to do them.

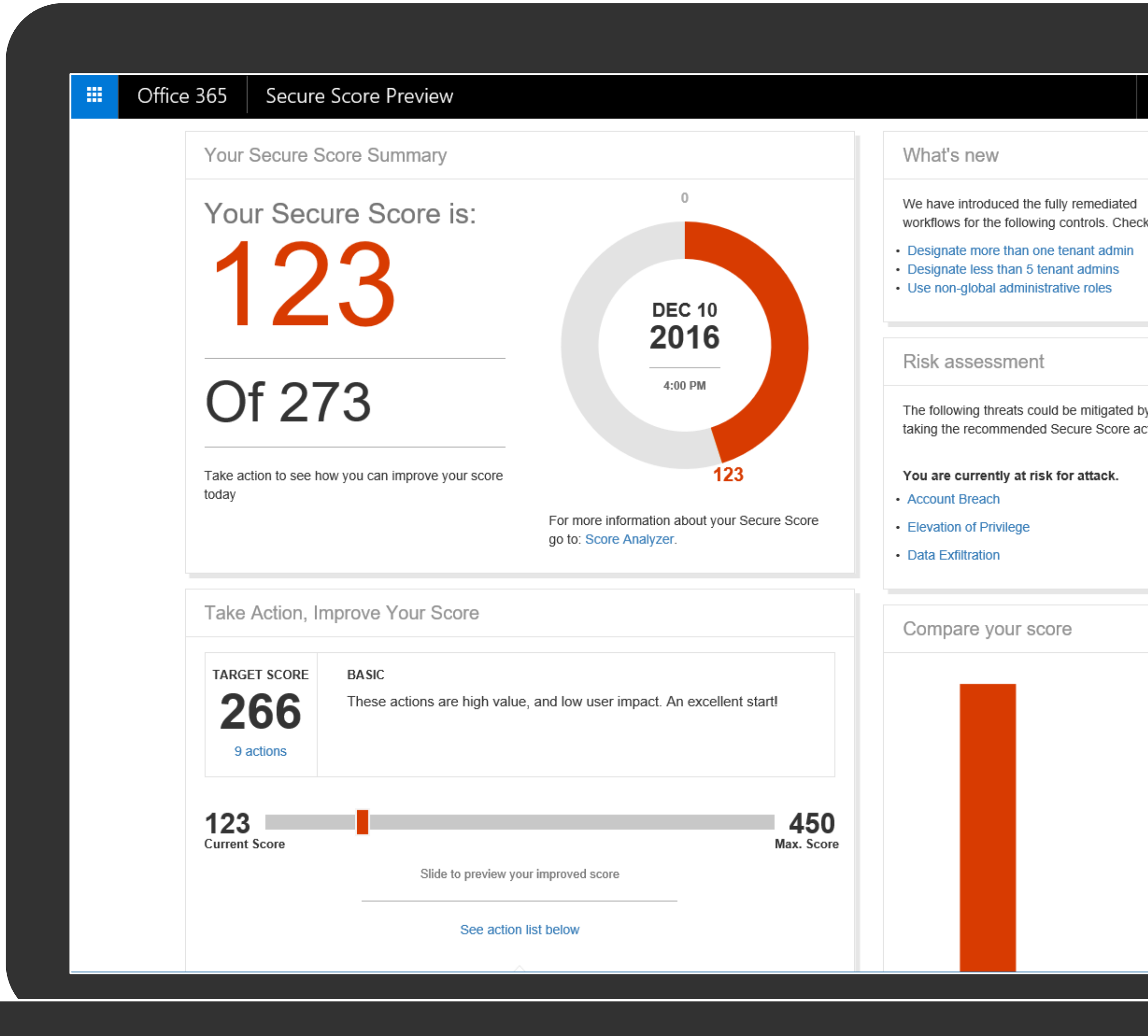
Insights into your security position

One place to understand your security position and what features you have enabled.

Guidance to increase your security level

Learn what security features are available to reduce risk while helping you balance productivity and security.

Admins can access Secure Score at securescore.office.com.



Your Secure Score Summary

Your Secure Score is:
123
Of 273

Take action to see how you can improve your score today

0
DEC 10
2016
4:00 PM
123

For more information about your Secure Score go to: Score Analyzer.

What's new

We have introduced the fully remediated workflows for the following controls. Check

- Designate more than one tenant admin
- Designate less than 5 tenant admins
- Use non-global administrative roles

Risk assessment

The following threats could be mitigated by taking the recommended Secure Score ac

You are currently at risk for attack.

- Account Breach
- Elevation of Privilege
- Data Exfiltration

Take Action, Improve Your Score

TARGET SCORE
266
9 actions

BASIC
These actions are high value, and low user impact. An excellent start!

123 Current Score
450 Max. Score

Slide to preview your improved score

See action list below

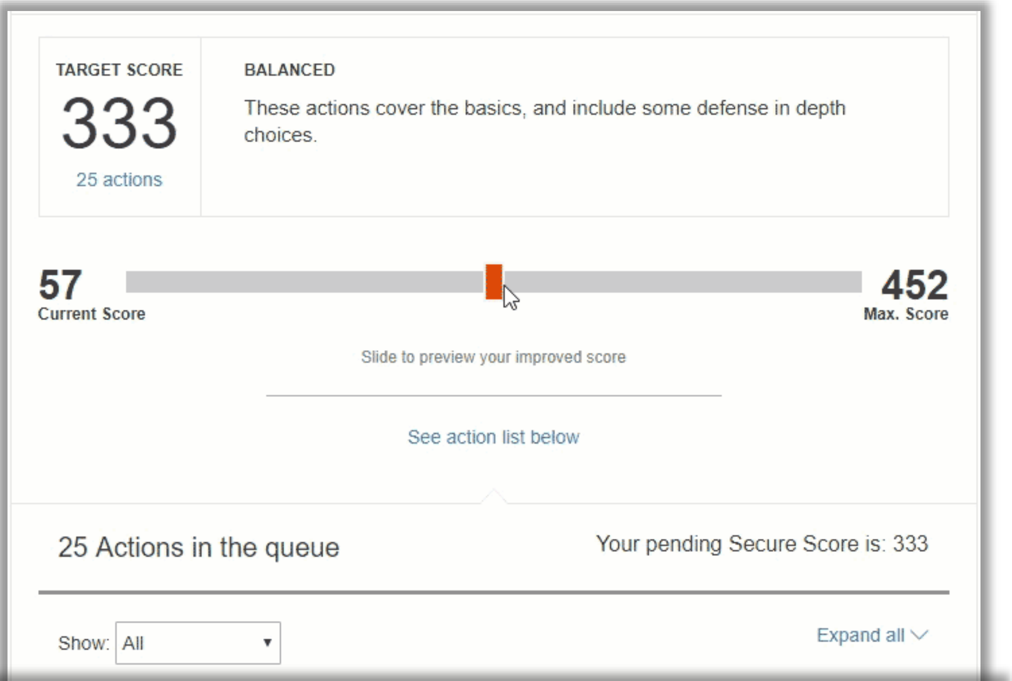
Compare your score

Secure Score: Analyzing Your Score

Quickly figure out what actions to take to improve your score.

Rather than reacting or responding to security alerts, the Secure Score lets you track and plan incremental improvements over a longer period of time.

Check the action queue to find changes that most improves your security posture with the least amount of usability impact for users.



TARGET SCORE

333

25 actions

BALANCED

These actions cover the basics, and include some defense in depth choices.

57 Current Score

452 Max. Score

Slide to preview your improved score

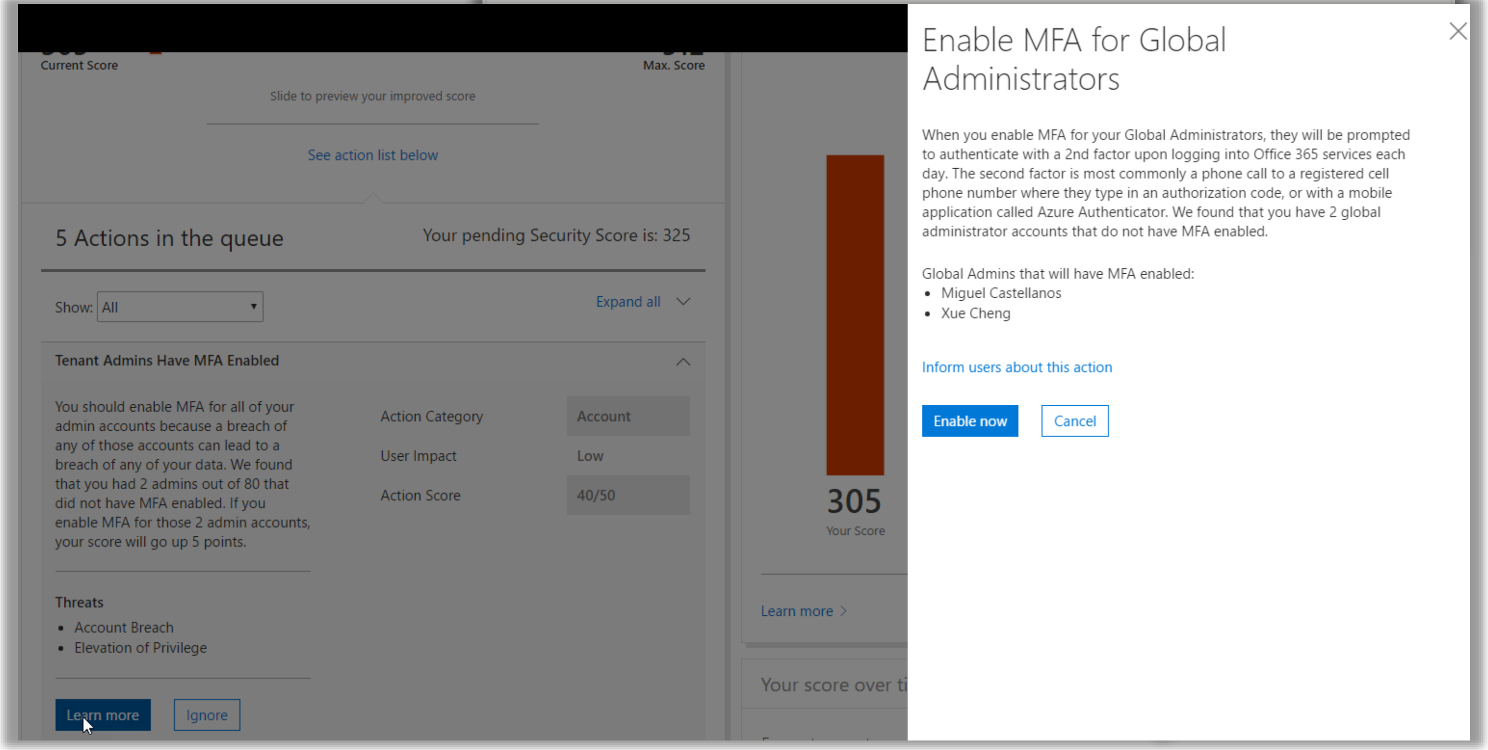
See action list below

25 Actions in the queue

Your pending Secure Score is: 333

Show: All

Expand all



Current Score

Max. Score

Slide to preview your improved score

See action list below

5 Actions in the queue

Your pending Security Score is: 325

Show: All

Expand all

Tenant Admins Have MFA Enabled

You should enable MFA for all of your admin accounts because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 2 admins out of 80 that did not have MFA enabled. If you enable MFA for those 2 admin accounts, your score will go up 5 points.

Action Category	Account
User Impact	Low
Action Score	40/50

Threats

- Account Breach
- Elevation of Privilege

Enable MFA for Global Administrators

When you enable MFA for your Global Administrators, they will be prompted to authenticate with a 2nd factor upon logging into Office 365 services each day. The second factor is most commonly a phone call to a registered cell phone number where they type in an authorization code, or with a mobile application called Azure Authenticator. We found that you have 2 global administrator accounts that do not have MFA enabled.

Global Admins that will have MFA enabled:

- Miguel Castellanos
- Xue Cheng

Inform users about this action

Office 365 Controls: Behavioral

Cost	Effort	Name
No	Low	Designate more than one global admin
No	Low	[Not Scored] Do not use mail forwarding rules to external domains
No	Moderate	Use non-global administrative roles
No	Moderate	Disable accounts not used in last 30 days
No	Moderate	User alternate contact info is completed for all users

Office 365 Controls: Configuration

Cost	Effort	Name
No	Low	Enable MFA for all global admins
Yes	Moderate	Enable MFA for all users ($2 per user per month)
No	Low	Enable Client Rules Forwarding Block
No	Low	[Not Scored] Set outbound spam notifications
No	Low	Enable mailbox auditing for all users
No	Low	[Not Scored] Do not use transport rule to external domains
No	Low	[Not Scored] Do not use transport white lists. Review existing if place and needed.
No	Low	[Not Scored] Do not allow anonymous calendar sharing
No	Low	[Not Scored] Do not allow calendar details sharing
No	Low	Configure expiration time for external sharing links
No	Low	Enable versioning on all SharePoint online document libraries
No	Low	Allow anonymous guest sharing links for sites and docs

Office 365 Controls: Configuration

Cost	Effort	Name
Yes (Labor)	High	Enable Data Loss Prevention policies
Yes (E5)	Low	Enable Advanced Security Management Console (E5)
Yes	Low	Enable Advanced Threat Protection safe attachments policy($2 per user per month
Yes	Low	Enable Advanced Threat Protection safe links policy
Yes (Labor)	Moderate	Enable mobile device management services
Yes (Labor)	Low	Require mobile devices to use a password
Yes (Labor)	Low	Require mobile devices to block access and report policy violations
Yes (Labor)	Low	Require mobile devices to manage email profile
Yes (Labor)	Low	Do not allow simple passwords on mobile devices
Yes (Labor)	Low	Set a policy to require users to use a complex password with a at least two character sets
Yes (Labor)	Low	Require mobile devices to use encryption
Yes (Labor)	Low	Require mobile devices to lock on inactivity
Yes (Labor)	Low	Require mobile devices to have minimum password length
Yes (Labor)	Low	Require mobile devices to wipe on multiple sign-in failures
Yes (Labor)	Low	Do not allow jail broken or rooted mobile devices to connect
Yes (Labor)	Low	Require mobile devices to never expire password
Yes (Labor)	Low	Do not allow mobile device password re-use

Office 365 Controls: Review

Cost	Effort	Name
No	Moderate	Review signs-ins after multiple failures report weekly
No	Moderate	Review sign-ins from unknown sources report weekly
No	Low	Review signs-ins from multiple geographies report weekly
No	Low	Review role changes weekly
No	Moderate	Use audit data
No	Moderate	Review mailbox forwarding rules weekly
No	Moderate	Review mailbox access by non-owners report bi-weekly
No	Moderate	Review malware detections report weekly
No	Moderate	Review sign-in devices report weekly
No	Moderate	Review account provisioning activity report weekly
No	Moderate	Review non-global administrators weekly
No	Moderate	Review list of external users you have invited to documents monthly

More options

Enable Multi-Factor Authentication for all users:

A breach of any account can lead to a breach of the data that user has access to.

Enable Advanced Threat Protection:

Protect against sophisticated threats hidden in email attachments and links, and it provides cutting-edge defenses against zero-day threats, ransomware, and other advanced malware attempts.

Enable Advanced Security Management Console (Office 365 E5):

Get insight into suspicious activity in Office 365 so you can investigate situations that are potentially problematic and, if needed, take action to address security issues.

Enable Data Loss Prevention Policies:

Data Loss Prevention (DLP) policies help protect your data from accidental, or malicious exposure.

Demo: Office 365 Secure Score

iV4 Office 365 Hardening Review

This flat fee engagement uses the Office 365 Secure Score tool to evaluate and prioritize Office 365 tenant security settings for your organization.

Implementing the items included in the Office 365 Security Hardening has the potential to increase your Secure Score up to 146 points.

iV4

iV4 Office 365 Hardening Review

This flat fee engagement uses the Office 365 Secure Score tool to evaluate and prioritize Office 365 tenant security settings for your organization.

Implementing the items included in the Office 365 Security Hardening has the potential to increase your Secure Score up to 146 points.

SPECIAL OFFER

iV4 Office 365 Security Health Check

Monthly review of key Office 365 reports and configurations, which if left ignored, could result in malicious activity and ultimately a compromised account.

Just as you should perform monthly Net Health Checks to make sure backups are running properly and anti-virus patches are rolled out, reviewing your Office 365 tenancy is just as important.

Questions?

iV4