



Securing Office
365 for free





Office 365 Threat Landscape

How are the bad guys
attacking you?

Threat Landscape

Attackers are focusing on people, not technology

- » Password spraying
- » Brute force login attempts
- » Phishing/Social Engineering
- » Misconfigured services



Protecting Identities

Because you can't install
antivirus on your users.



Multifactor Authentication

Yes, it's that important.

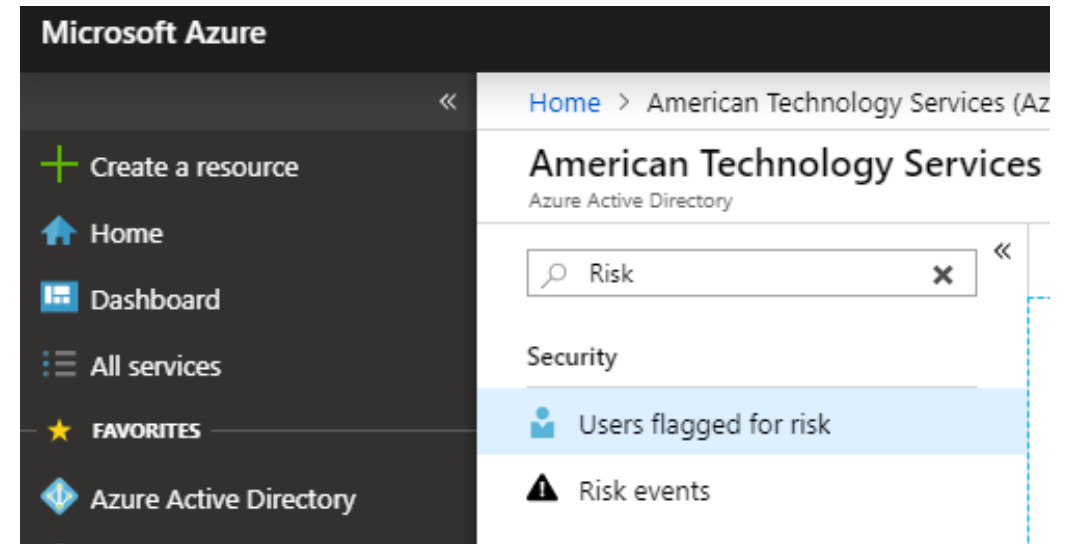
Available Methods:

- » Random code
- » Push notification
- » Phone call/Text
- » Smart card
- » Biometric device

Available to all license levels.
[Azure AD Premium](#) unlocks advanced features.

Risky sign-in report

Why did Sara log in from Virginia this morning and Nigeria tonight?



Available to all license levels.
[Azure AD Premium](#) unlocks
advanced features.

License Level Comparison

Free and Basic Editions

USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
John Nash	193.90.12.87	Oslo, Oslo, NO	11/21/2016 01:03	Active
John Nash	193.90.12.87	Oslo, Oslo, NO	11/20/2016 01:04	Active
John Nash	193.90.12.87	Oslo, Oslo, NO	11/19/2016 01:04	Active
John Nash			11/19/2016 01:03	Active
John Nash			11/18/2016 01:03	Active

Azure AD Premium

Contoso Cloud - Risky Sign-ins
Azure Active Directory

Search (Ctrl+) | Last 90 days | Download | Refresh

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials	0 of 3	2/13/2017, 12:00 AM
Medium	Real-time	Sign-ins from anonymous IP addresses	56 of 67	2/16/2017, 9:18 PM
Medium	Offline	Impossible travels to atypical locations	1 of 10	2/12/2017, 1:02 AM
Medium	Real-time	Sign-ins from unfamiliar locations	39 of 51	2/16/2017, 9:18 PM
Low	Offline	Sign-ins from infected devices	0 of 28	2/12/2017, 12:38 AM

Jennifer Davis

All sign-ins | Reset password | Dismiss all events

User has a high risk level

Essentials

Risk level	High	Status	At risk
Role	User	Contact	JenDavis@contosobuild.com
Location	N/A	MFA registered	No
Department	N/A	Object Id	c0de123c-ee1e-4c5a-b115-e11cf66aba92

Risk events

5

0 11/24 12/12 12/30 01/17 02/04

HIGH 0 MEDIUM 6 LOW 4 CLOSED 0

TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
2/12/2017 5:26 ...	77.109.41.30	Sign-in from anonymous IP address	Medium
2/12/2017 1:02 ...	125.37.113.28	Impossible travel to atypical location	Medium
2/12/2017 12:38...	81.25.53.98	Sign-in from infected device	Low
1/16/2017 5:15 A.	77.109.41.30	Sign-in from anonymous IP address	Medium

Protecting Data

Are users giving away your sensitive documents?



Default SharePoint permissions

Oh yea, I forgot about that.

Available Methods:

Default link type

Choose the type of link that is created by default when users get links. [Learn more.](#)

- Direct - specific people
- Internal - only people in your organization
- Anonymous Access - anyone with the link

Use shorter links when sharing files and folders

Default link permission

Choose the default permission that is selected when users share. This applies to anonymous access, internal and direct links.

- View
- Edit

Available to [all license levels.](#)

Protecting Email

Where does all this spam
come from, anyway?



Tweaking the spam filter

A tragically unused option.

Available Options:

Default

general

spam and bulk actions

block lists

allow lists

international spam

• advanced options

advanced options

Increase Spam Score
Specify whether to increase the spam score for messages that include these types of links or URLs.

Image links to remote sites:

▼

Numeric IP address in URL:

▼

URL redirect to other port:

▼

URL to .biz or .info websites:

▼

Mark as Spam

Specify whether to mark messages that include these properties as spam.

Empty messages:

▼

JavaScript or VBScript in HTML:

▼

Frame or IFrame tags in HTML:

▼

Object tags in HTML:

▼

Embed tags in HTML:

▼

Form tags in HTML:

▼

Web bugs in HTML:

▼

Apply sensitive word list:

▼

SPF record: hard fail:

▼

Conditional Sender ID filtering: hard fail:

▼

NDR backscatter:

▼

Test Mode Options

Configure the test mode options for when a match is made to a test-enabled advanced option.

- None
- Add the default test X-header text
- Send a Bcc message to this address:

Available to **all license levels.**

External email banner

Exchange admin center

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

rules message trace accepted domains remote domains connectors

new rule - Google Chrome
https://outlook.office365.com/ecp/@astho.onmicrosoft.com/RulesEditor/NewTransportRule.aspx?Activi...

new rule

Name:

*Apply this rule if...
 [Outside the organization](#)

*Do the following...
 [and fall back to action Wrap if the disclaimer can't be inserted.](#)

Properties of this rule:

Audit this rule with severity level:

Choose a mode for this rule:

- Enforce
- Test with Policy Tips
- Test without Policy Tips

[More options...](#)

i Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. [Learn more](#)

Available to **all license levels.**

“Advanced” DNS config

SPF, DKIM and DMARC, oh my!

- » SPF – *Tells the world where your email should come from.*
- » DKIM – *Cryptographically sign each email to prove it came from you.*
- » DMARC – *Additional checks to identify incoming spoofed emails.*

Available to **all license levels.**

Mailbox audit logging

Tracing the bad guys' steps.

Why auditing?

Enabled by default...sort of.

Get-OrganizationConfig | FL AuditDisabled
(Exchange Online Powershell)

What is audited?

Available to **all license levels.**

Mailbox audit logging

Continued

Default settings:

Action	Description	Admin	Delegate	Owner
Copy	A message was copied to another folder.	Yes	No	No
Create	An item is created in the Calendar, Contacts, Notes, or Tasks folder in the mailbox; for example, a new meeting request is created. Note that creating, sending, or receiving a message isn't audited. Also, creating a mailbox folder is not audited.	Yes*	Yes*	Yes
FolderBind**	A mailbox folder was accessed. This action is also logged when the admin or delegate opens the mailbox.	Yes	Yes	No
HardDelete	A message was purged from the Recoverable Items folder.	Yes*	Yes*	Yes*
MailboxLogin	The user signed into their mailbox.	No	No	Yes
MessageBind***	A message was viewed in the preview pane or opened.	Yes	No	No
Move	A message was moved to another folder.	Yes	Yes	Yes
MoveToDeletedItems	A message was deleted and moved to the Deleted Items folder.	Yes*	Yes*	Yes*
SendAs	A message was sent using the SendAs permission. This means another user sent the message as though it came from the mailbox owner.	Yes*	Yes*	No
SendOnBehalf	A message was sent using the SendOnBehalf permission. This means another user sent the message on behalf of the mailbox owner. The message indicates to the recipient who the message was sent on behalf of and who actually sent the message.	Yes*	Yes*	No
SoftDelete	A message was permanently deleted or deleted from the Deleted Items folder. Soft-deleted items are moved to the Recoverable Items folder.	Yes*	Yes*	Yes*
Update	A message or its properties was changed.	Yes*	Yes*	Yes*





On your way to greener pastures. Questions?




Thank You

 Chris Schoenwetter

 (703) 876-0300

 cschoenwetter@networkats.com

 networkats.com

