

Enterprise Mobility + Security

Automation + Security for the Digital Workplace

Daniel Dickinson
Digital Workplace Cyber Security Specialist

<https://t.me/learningnets>



Assume Breach



Why?

- **Identity** is the new perimeter, 99% of attacks are focused on identity theft
- **Data** loss / leakage
- **Flexible Workforce** computing
Almost any device, anywhere, anytime.

How?

- 16,000 employees
- 8,000 will open an email within 88 secs
 - **800 will open an attachment (5%)**
 - **2,000 will click a link (12%)**
- 4-8 hours to own the AD
- 1 year to detect



Cyber Threat Intelligence

Billions of sensors across consumer, enterprise, and cloud services



250 million users



Malicious Software Removal Tool

700 million PCs/month
40 billion executions ('05-'14)

Microsoft Security Essentials

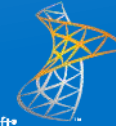
Millions of consumers
Billions of malware removals/year

bing

18+ billion page scans/month

Outlook.com

420 million active users



Microsoft Exchange Online

35 billion messages/month



MICROSOFT DIGITAL CRIMES UNIT

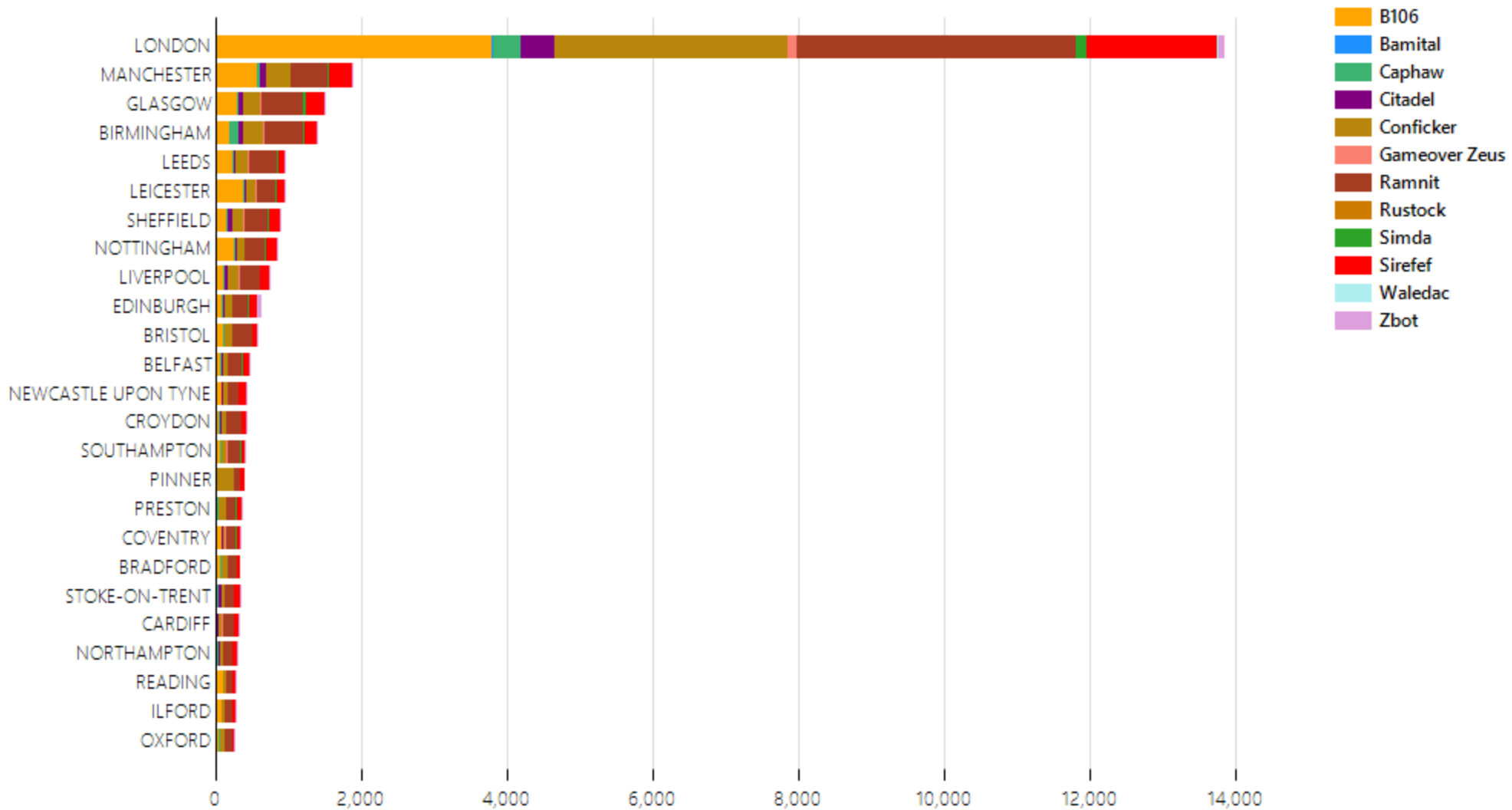
Microsoft System Center 2012 Endpoint Protection
Millions of PCs

Worlds largest threat telemetry

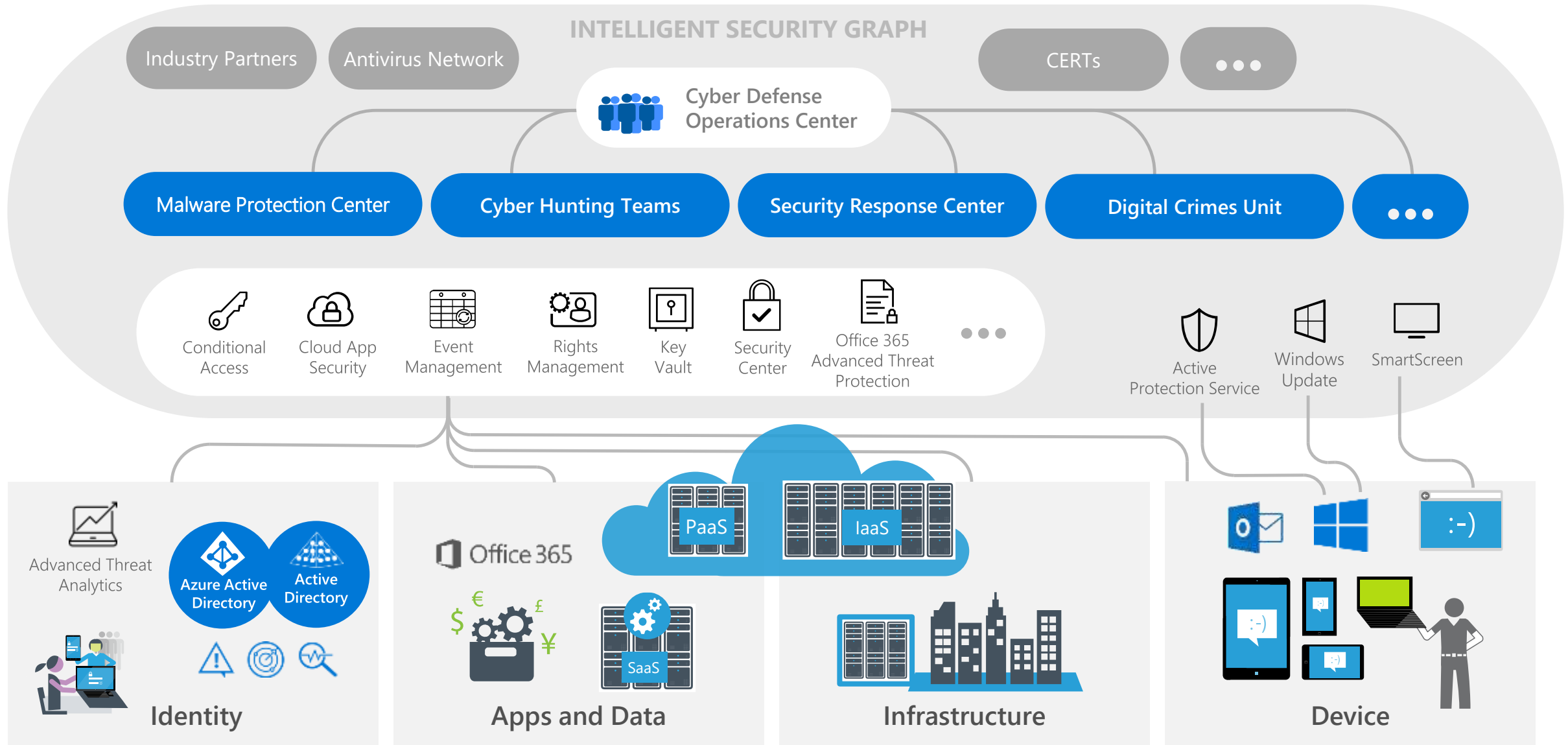


United Kingdom

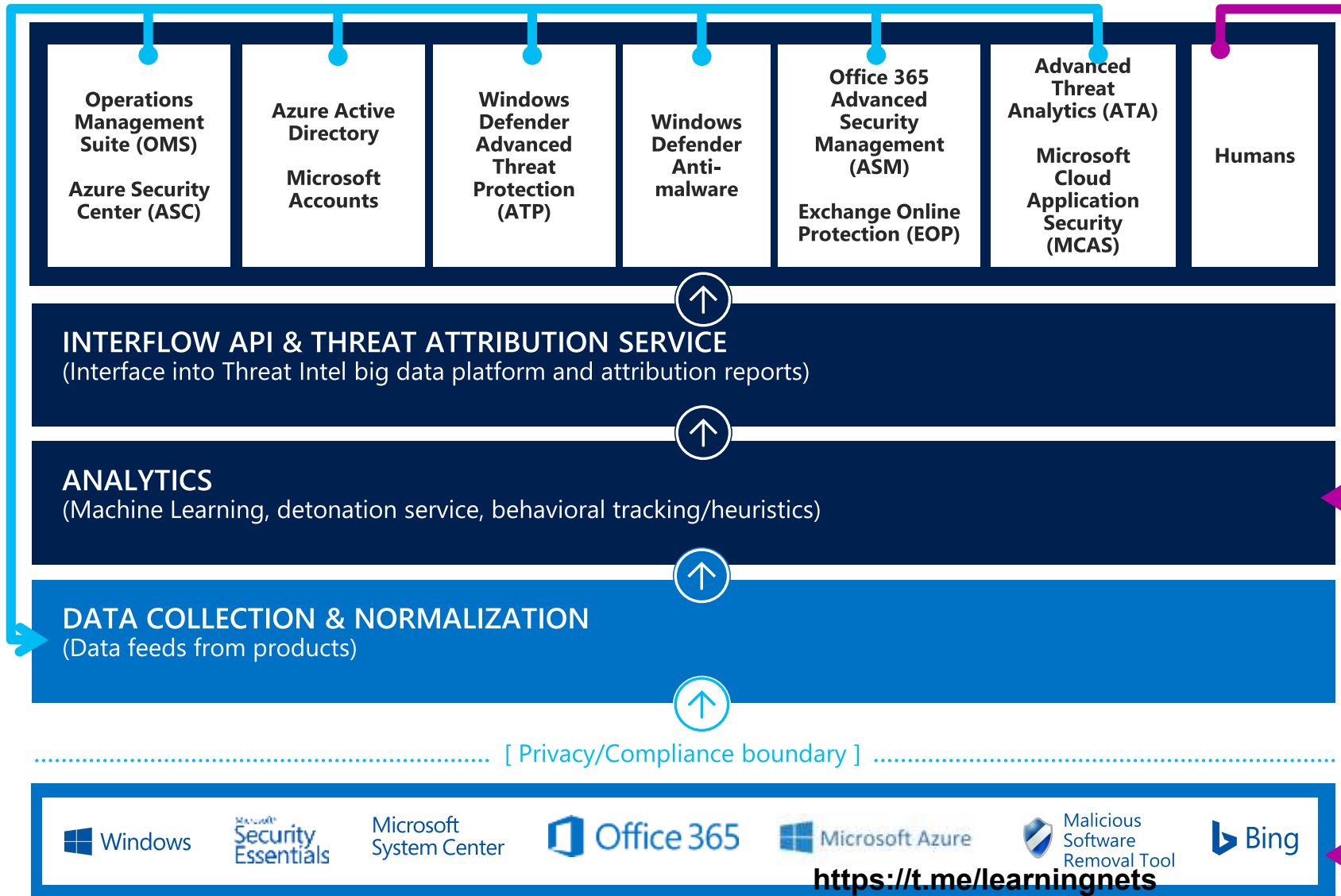
Top 25 Cities by Threat



Microsoft's Security Approach



Inside the Intelligent security graph



- Hunters identify attacks, and improve analytics
- Products generate their own data which feeds back into the graph
- Products use Interflow APIs to access results
- Analytics surfaces findings to help fuel new discoveries
- Data is processed
- Products send data to graph
- Products instrumented with privacy/compliance in mind



- Home
- Alerts
- Permissions
- Security policies
- Data management
- Search & investigation
- Reports
- Service assurance
- Dashboard
- Compliance reports
- Trust documents
- Audited controls**
- Settings

Home > Audited controls

Status of Audited Controls

Use this page to understand the status of audited controls from global information security standards and regulations that Office 365 has implemented. Click on the standards and regulations shown below to view the controls and understand how independent third-party auditors have tested them, and what the test results were.

[Download](#)

<input type="checkbox"/>	Regulation/Standard Name and Description	Last Tested	Controls Tested	Test Results
<input type="checkbox"/>	<p>ISO 27001:2013</p> <p>Office 365 has been accredited to latest ISO 27001:2013 standards. Information under this standard will help you to understand how Office 365 has implemented Information Security Management System (ISMS) to manage and control information security risks. In addition you will gain deep insights into implementation and testing of controls to maintain Confidentiality, Integrity, and availability of your data.</p>	28/10/2015	231	No findings
<input type="checkbox"/>	<p>ISO 27018:2014</p> <p>In line with Office 365's commitment to maintain strict privacy of your data, Office 365 has been accredited to latest ISO 27018:2014 standards. In this section you will see implementation and testing of controls specific to protection of Personally Identifiable Information (PII) and Privacy.</p>	28/10/2015	51	No findings

Trust documents provided by Microsoft

Review white papers, FAQs, end-of-year reports, and other trust-related documents provided by Microsoft.

FAQ and White Papers

View answers to Frequently asked Questions and white papers providing you insights into Office 365 Services Security, Privacy, and Compliance.

- [Auditing and Reporting in Office 365](#)
- [Azure - Financial Services Cloud Security Diagnostic workbook](#)
- [Azure 13 Effective Security Controls for ISO 27001 Compliance](#)
- [Azure A Practical Guide to Designing Secure Health Solutions using Microsoft Azure](#)
- [Azure Active Directory Multi-Tenant Isolation - DRAFT-protected](#)
- [Azure Data-Classification-for-Cloud-Readiness](#)
- [Azure PCI DSS Responsibility Matrix 2016 - v5-readonly](#)
- [CDSA Azure Implementation Guide Final Sept2015](#)
- [Data Encryption Technologies in Office 365](#)
- [Data Resiliency in Office 365](#)
- [Defending Office 365 Against Denial-of-Service Attacks](#)
- [ISO 27001_2013 and ISO 27018_2014 Aligned FAQ](#)
- [Microsoft Azure HIPAA Implementation Guidance](#)
- [Office 365 Customer Security Considerations Preview](#)
- [Office 365 Customer Security Considerations Reference Guide_Use with the workbook](#)
- [Office 365 Mapping of CSA Cloud Control Matrix 3.0.1](#)
- [Office 365 Security Incident Management](#)
- [Tenant Isolation in Office 365](#)

Risk Management Reports

View security assessment and risk management reports on how Office 365 Service manages its risks.

- [Dynamics CRM Online Security Assessment 2014](#)
- [Dynamics CRM Online Security Assessment 2015](#)
- [Microsoft Security Policy](#)
- [MS O365 Risk Environment](#)
- [Office 365 End of Year Security Report 2014](#)
- [Office 365 End of Year Security Report and Pen Test Summary for 2015](#)
- [Office 365 Risk Management Lifecycle](#)
- [Office 365 Security Assessment Summary](#)

Azure Compliance

The largest compliance portfolio in the industry



ISO 27001



SOC 1 Type 2



SOC 2 Type 2



PCI DSS Level 1



Cloud Controls Matrix



ISO 27018



Content Delivery and Security Association



Shared Assessments



FedRAMP JAB P-ATO



HIPAA / HITECH



FIPS 140-2



21 CFR Part 11



FERPA



DISA Level 2



CJIS



IRS 1075



ITAR-ready



Section 508 VPAT



European Union Model Clauses



EU Safe Harbor



United Kingdom G-Cloud



China Multi Layer Protection Scheme



China GB 18030



China CCCPPF



Singapore MTCS Level 3



Australian Signals Directorate



New Zealand GCIO



Japan Financial Services



ENISA IAF

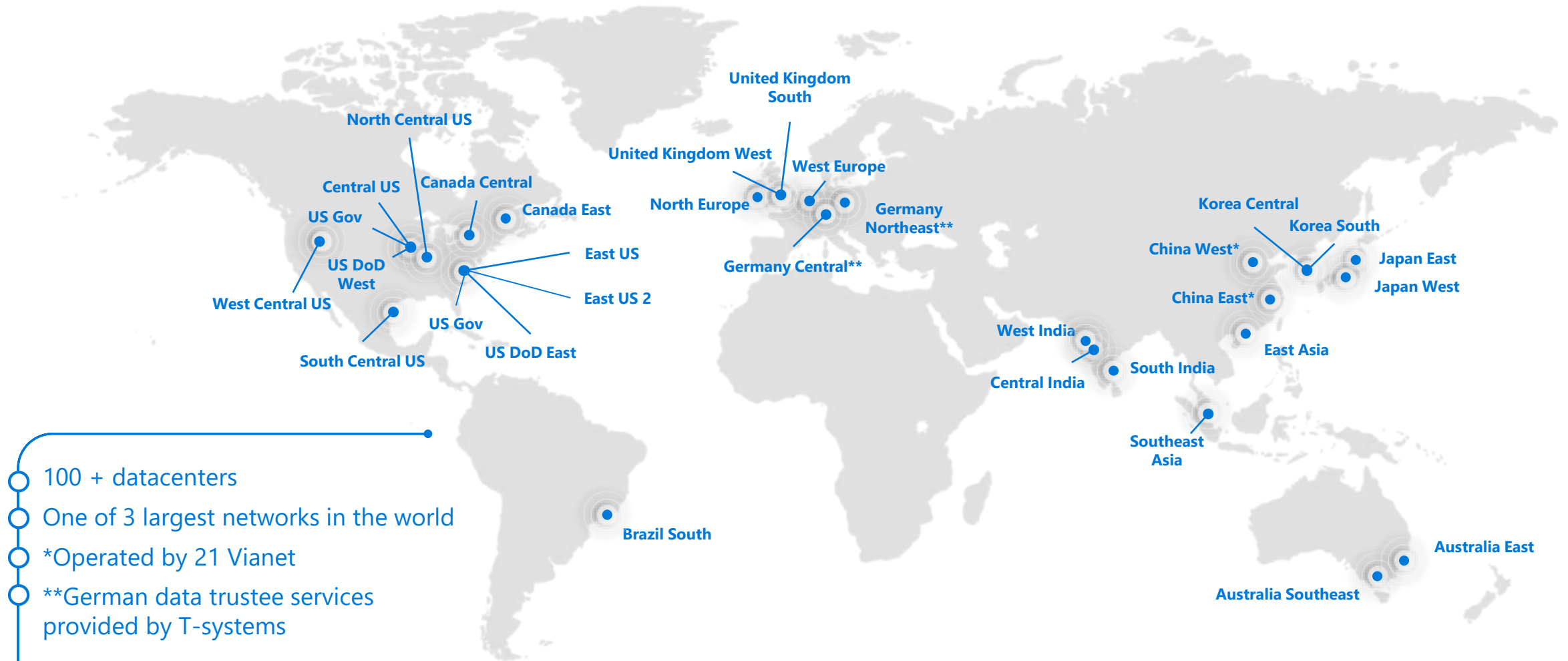
<https://t.me/learningnets>

Scale

- Azure AD Authentications?
- 15,000 authentications
 - Per Day?
 - Per Hour?
 - Per Minute?
- 34 data centres – inc. UK South and UK West

Global opportunity with Azure infrastructure

34 Azure regions worldwide



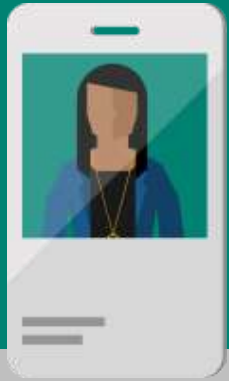
- 100 + datacenters
- One of 3 largest networks in the world
- *Operated by 21 Vianet
- **German data trustee services provided by T-systems

<https://t.me/learningnets>

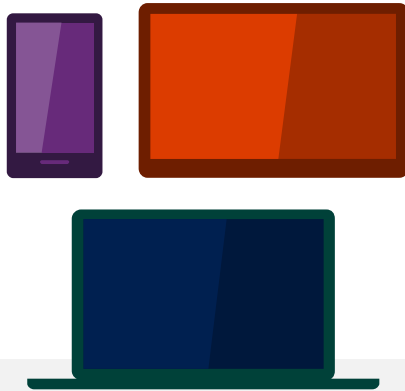
Empowering enterprise mobility

People-centric approach

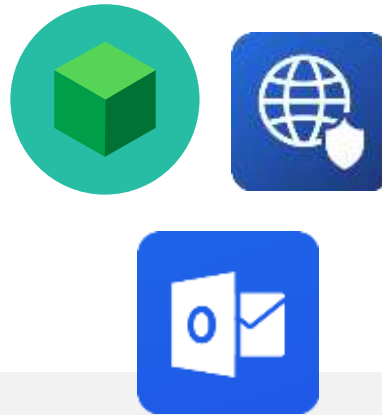
User



Devices



Apps



Data



IT



Enable
your users

Unify your environment

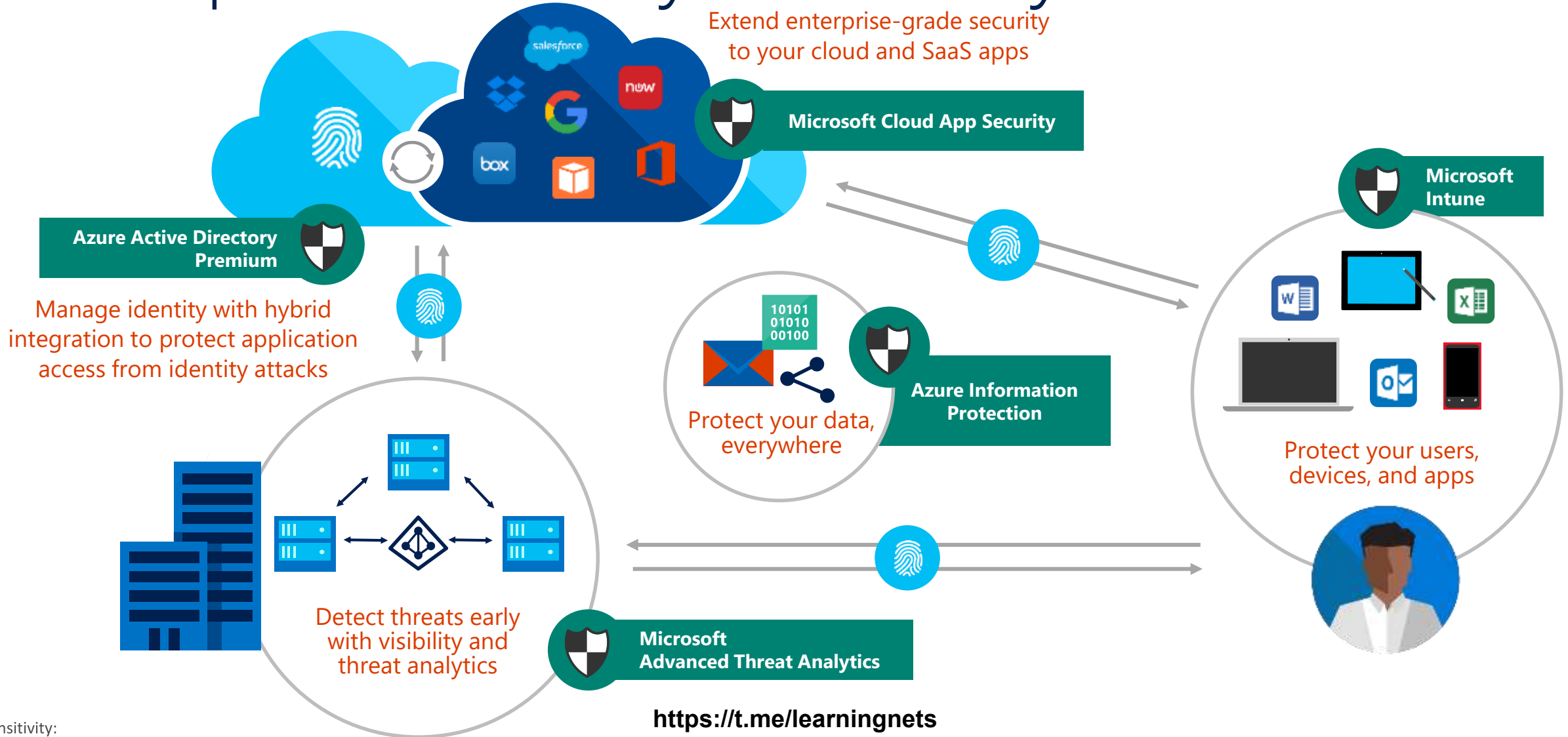
Protect
your data

<https://t.me/learningnets>

A HOLISTIC SOLUTION

Enterprise Mobility + Security

Extend enterprise-grade security to your cloud and SaaS apps



<https://t.me/learningnets>

Enterprise Mobility + Security



Identity and access management

Managed Mobile Productivity

Information Protection

Identity Driven Security

EMS E3

Azure Active Directory Premium P1

Secure Single-Sign on to cloud and On-premises apps. MFA, Conditional Access and advanced security reporting

Microsoft Intune

Mobile device and app management to protect corporate apps and data on any device.

Azure Information Protection Premium P1

Encryption for all files and storage locations. Cloud based file tracking

Microsoft Advanced Threat Analytics

Protection from advanced targeted attacks leveraging user and entity behavioral analytics

Azure Active Directory Premium P2

Identity and Access Management with advanced protection for users and privileged identities
(includes all capabilities in P1)

Azure Information Protection Premium P2

Intelligent classification, & encryption for files shared inside & outside your organization
(includes all capabilities in P1)

Microsoft Cloud App Security

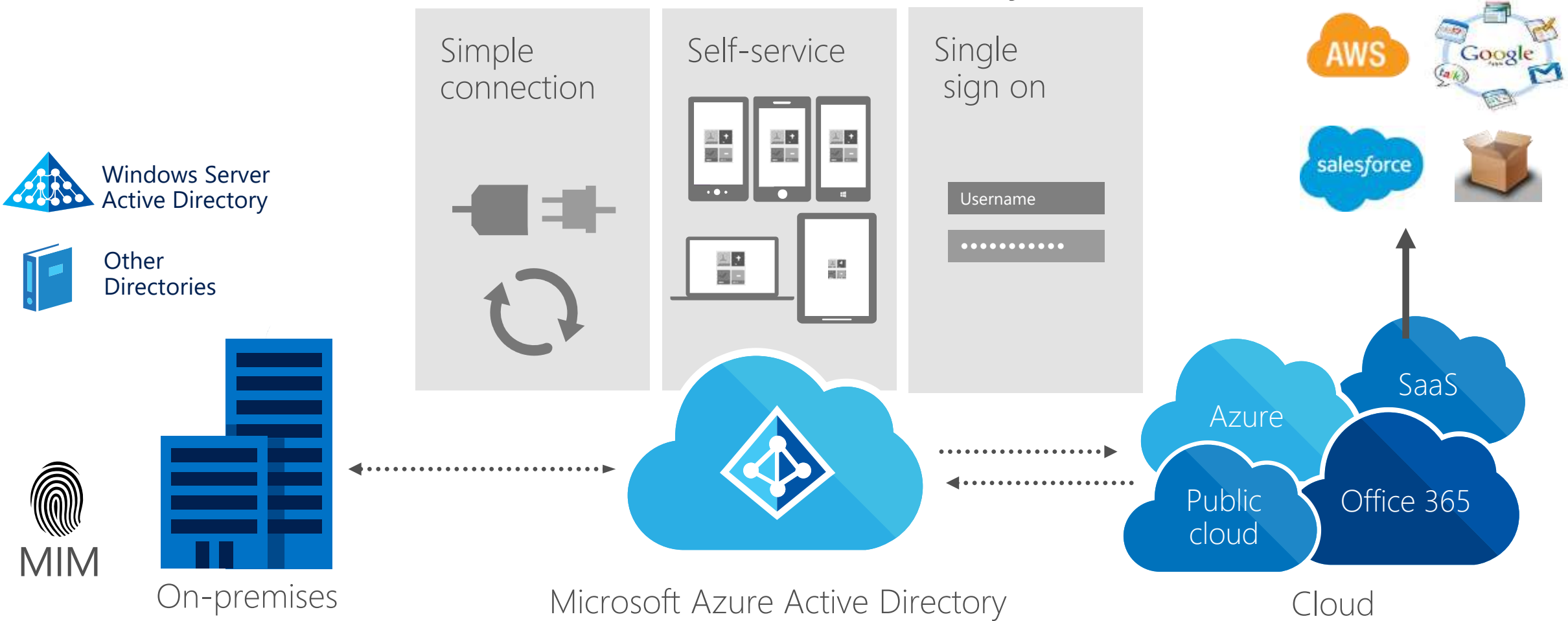
Enterprise-grade visibility, control, and protection for your cloud applications

EMS E5

<https://t.me/learningnets>

Integrated Identity as the control plane

One common identity



<https://t.me/learningnets>



Hilton

HOTELS & RESORTS

A screenshot of the Ashley Madison website. The top left features the "ASHLEY MADISON" logo and the tagline "Life is short. Have an affair." Below this is a form with the text "Get started by telling us your relationship status:" and a dropdown menu labeled "Please Select". A pink button with the text "See Your Matches >" is positioned below the dropdown. At the bottom of the screenshot, it says "Over 43,096,000 anonymous members!". The background of the screenshot is a close-up of a woman's face, with her finger pressed against her lips in a "shh" gesture.



As seen on: BBC News, Reuters, The Sun, The Telegraph, The Times

Ashley Madison is the world's leading married dating service for discreet encounters



Affairs Guaranteed



SSL Secure Site



<https://t.me/learningnets>

Mini Exercise

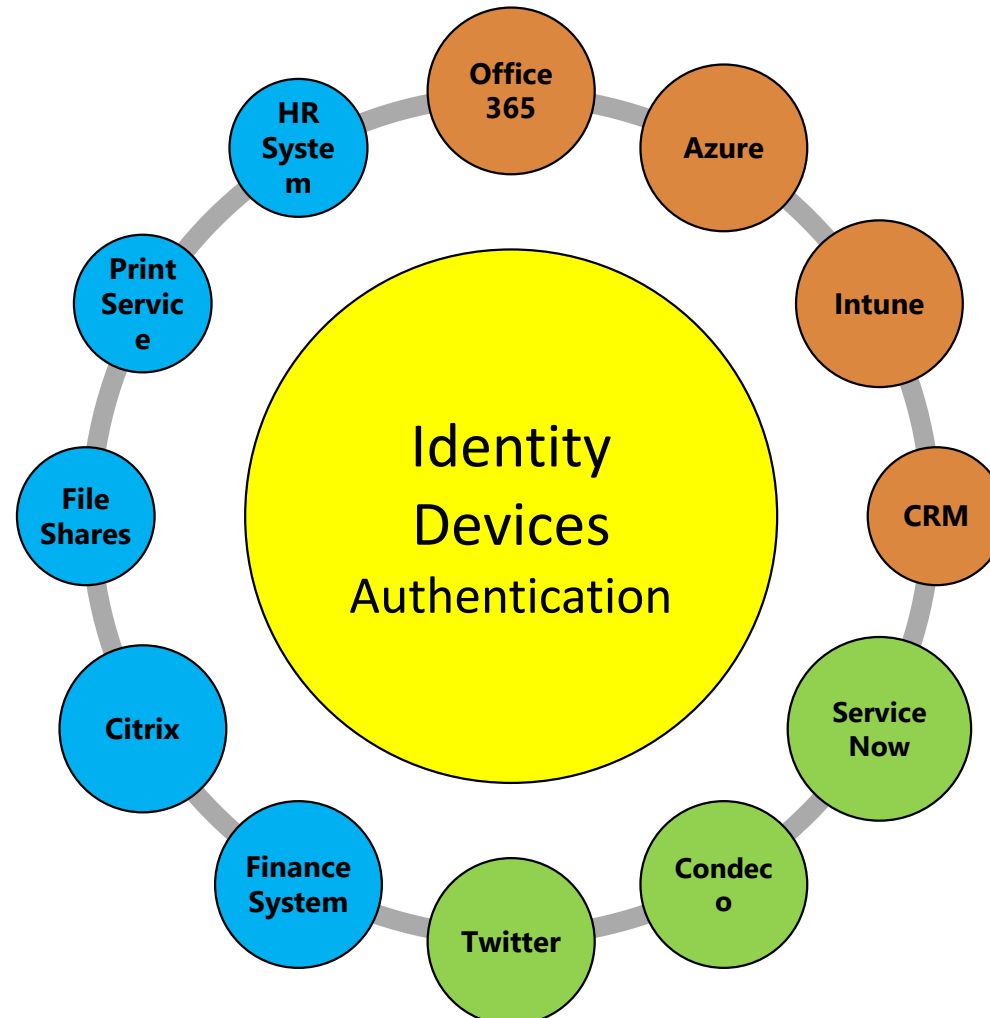
The screenshot shows the homepage of the 'Have I been pwned?' website. The navigation bar includes links for Home, Notify me, Domain search, Who's been pwned, Pastes, API, About, and Donate. The main heading is 'Have I been pwned?' with a subtitle 'Check if you have an account that has been compromised in a data breach'. Below this is a search input field labeled 'email address or username' and a 'pwned?' button. The statistics section displays: 112 pwned websites, 1,070,622,134 pwned accounts, 37,134 pastes, and 28,946,697 paste accounts. The 'Top 10 breaches' section lists the following data:

Rank	Logo	Count	Description
1	myspace	359,420,698	MySpace accounts
2	in	164,611,595	LinkedIn accounts
3	Adobe	152,445,165	Adobe accounts
4	VK	93,338,602	VK accounts
5	tumblr	65,469,298	tumblr accounts
6	Fling	40,767,652	Fling accounts 🔥
7	Ashley Madison	30,811,934	Ashley Madison accounts 🔥
8	mate1	27,393,015	Mate1.com accounts 🔥
9	000webhost	13,545,468	000webhost accounts
10	R2Games	13,186,088	R2Games accounts

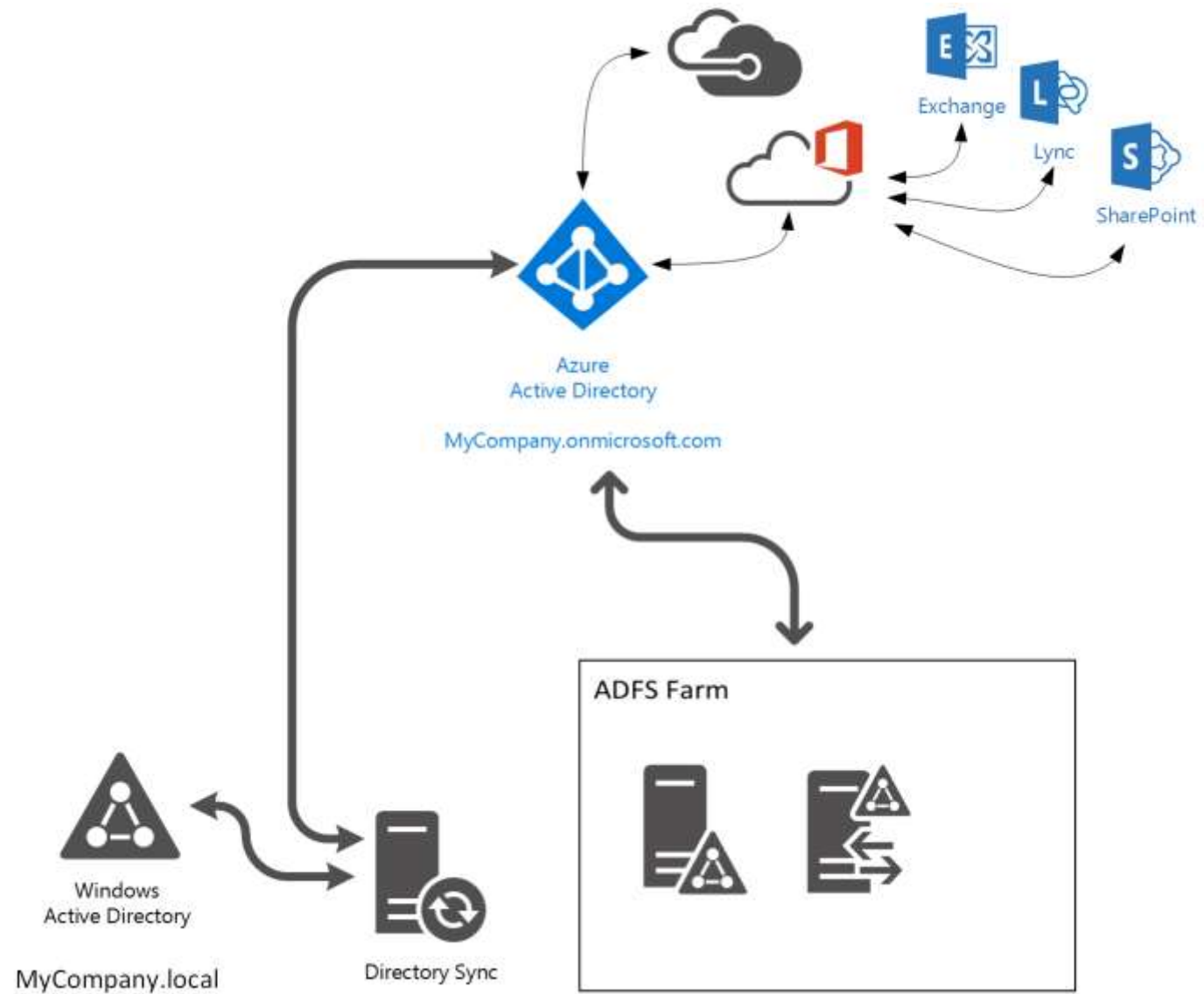
<https://t.me/learningnets>

Traditional Systems and Applications, MS Cloud Services, Other Cloud Services

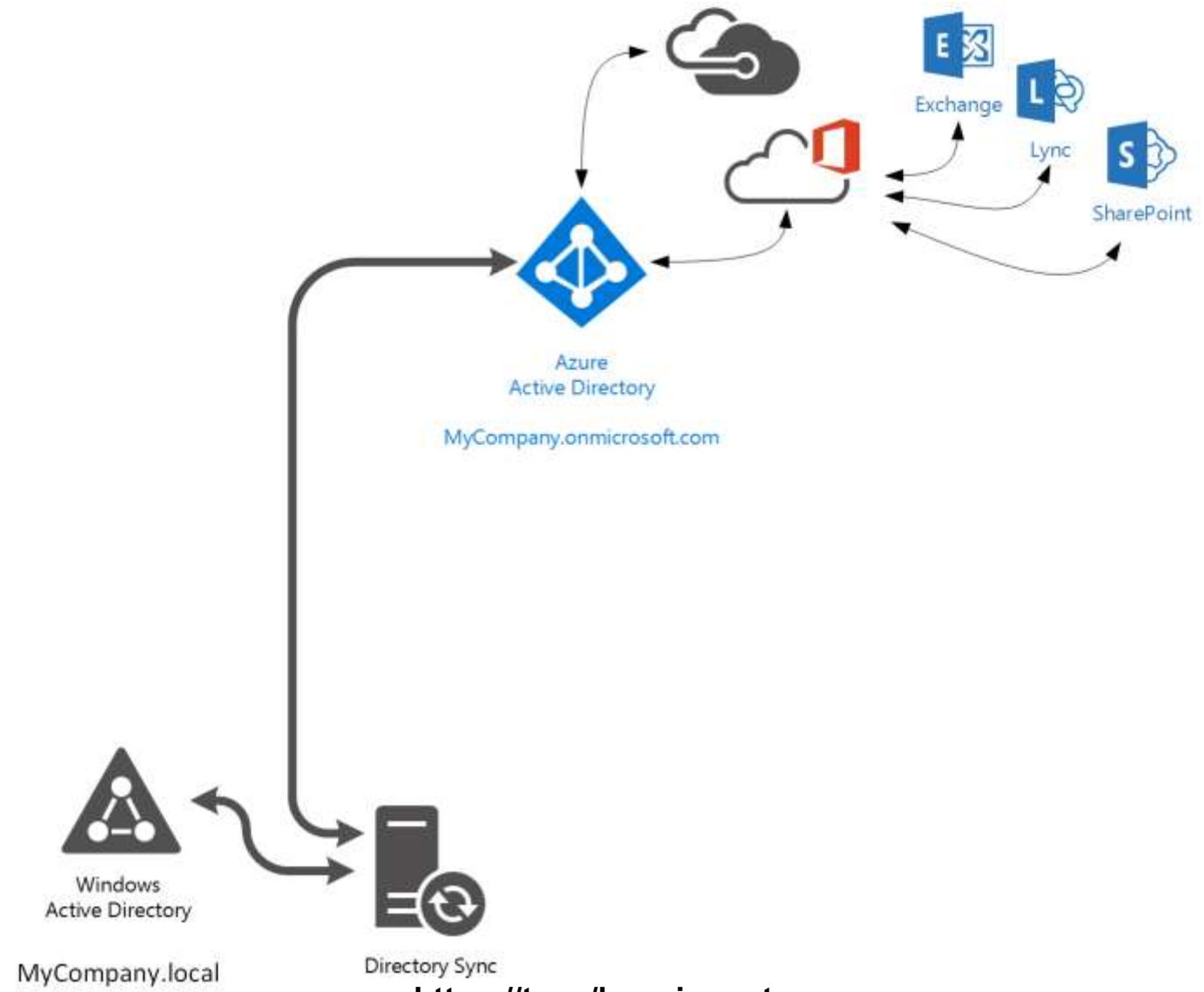
Identity

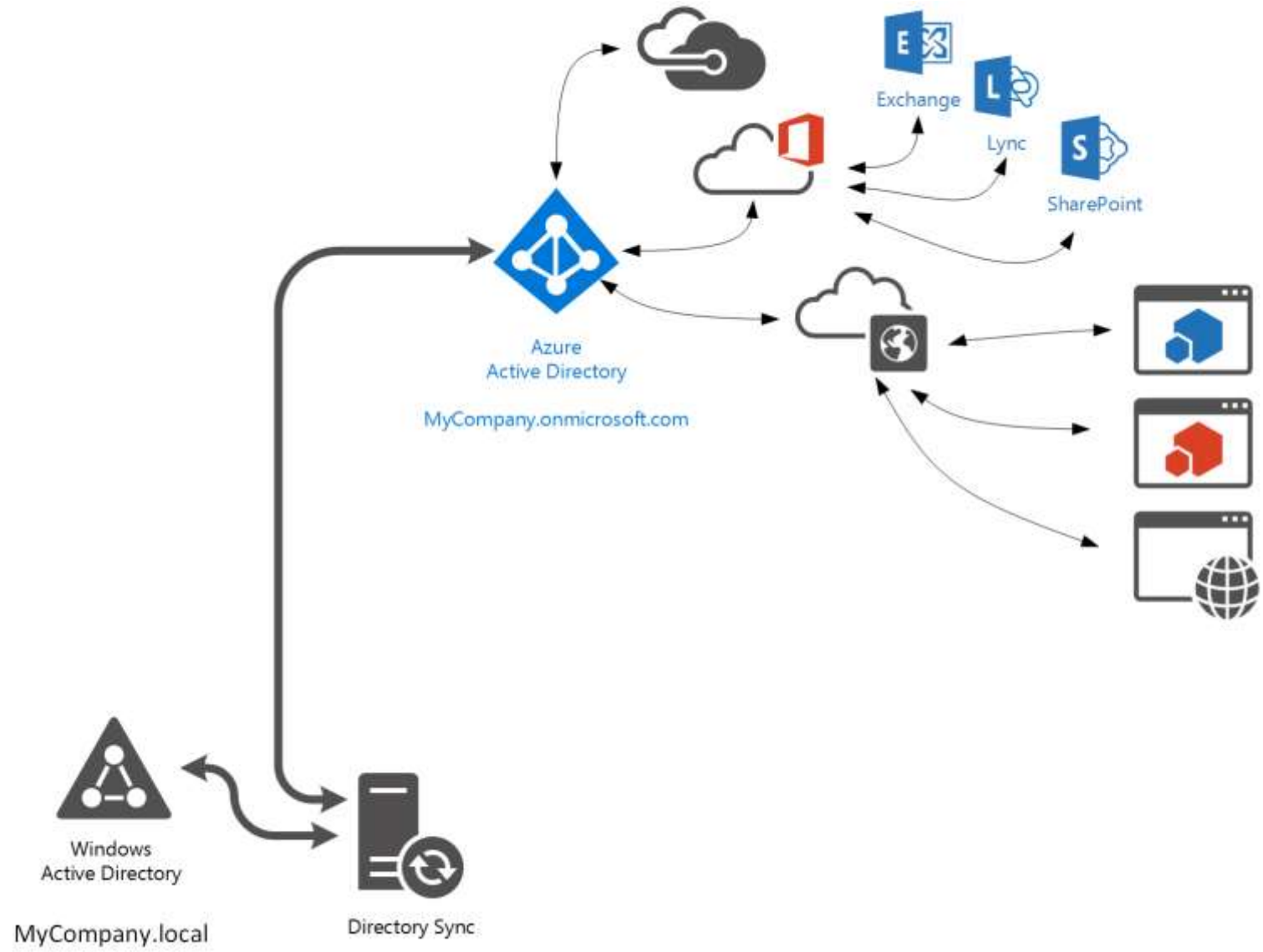


<https://t.me/learningnets>

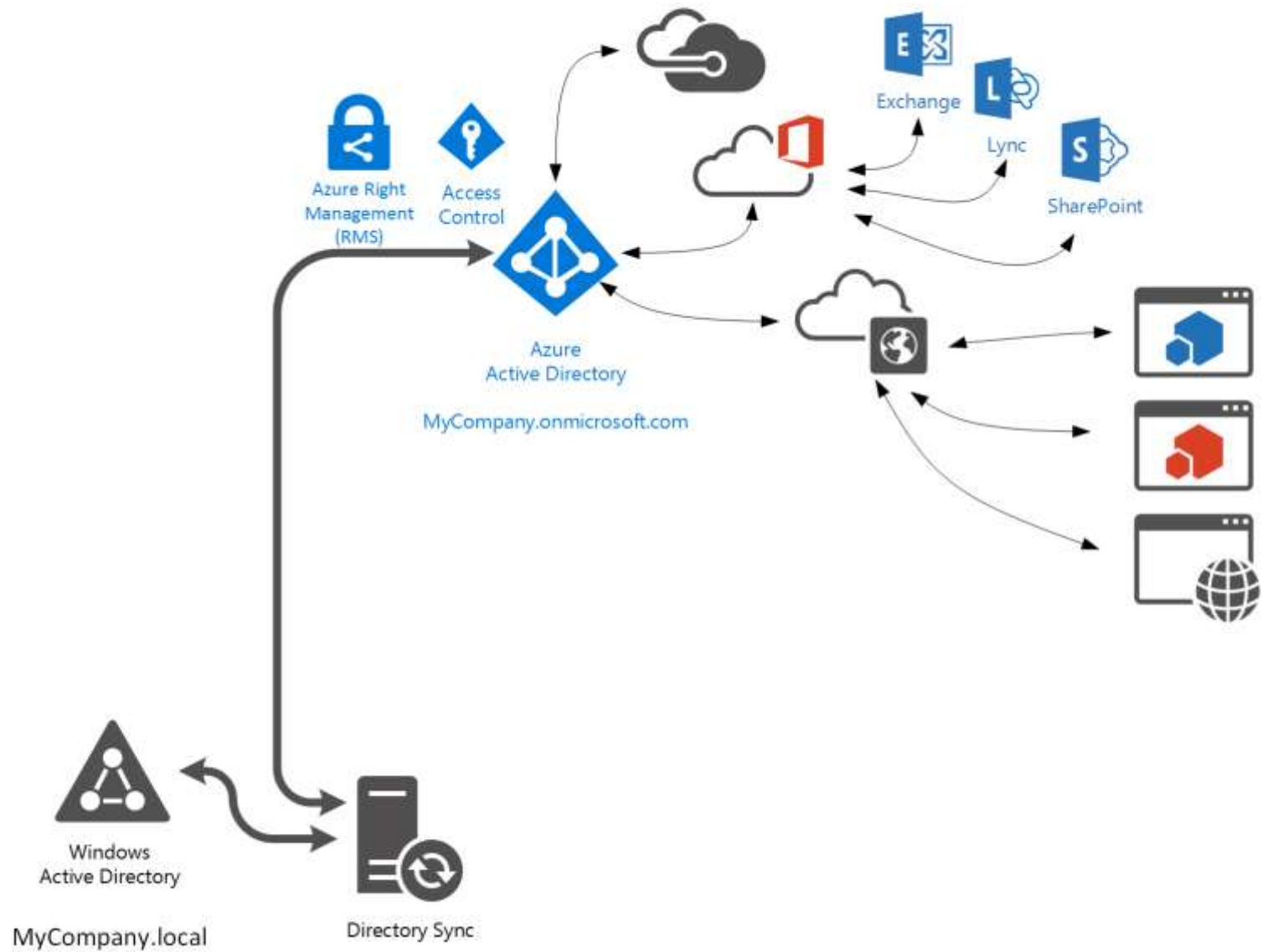


<https://t.me/learningnets>

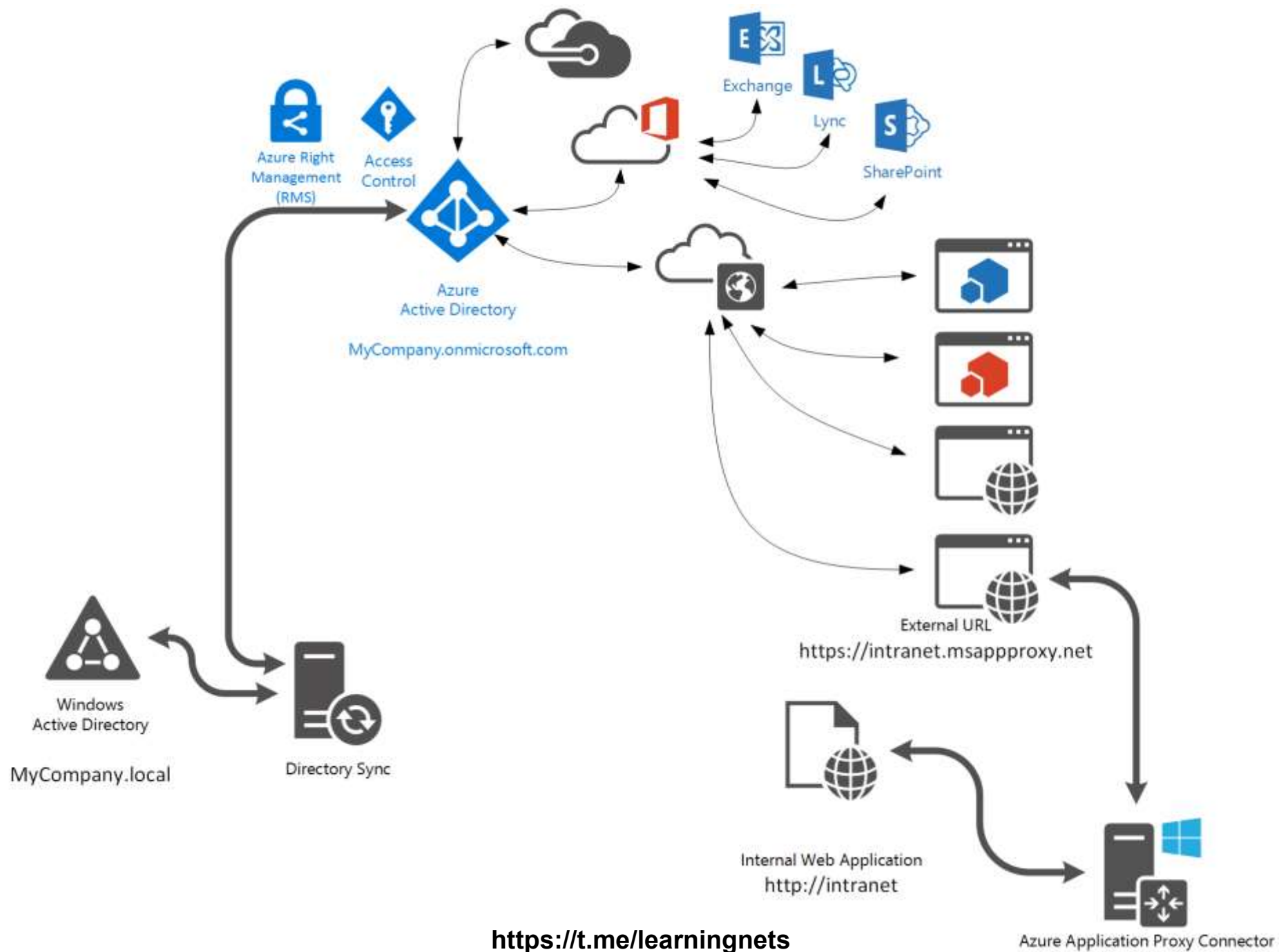




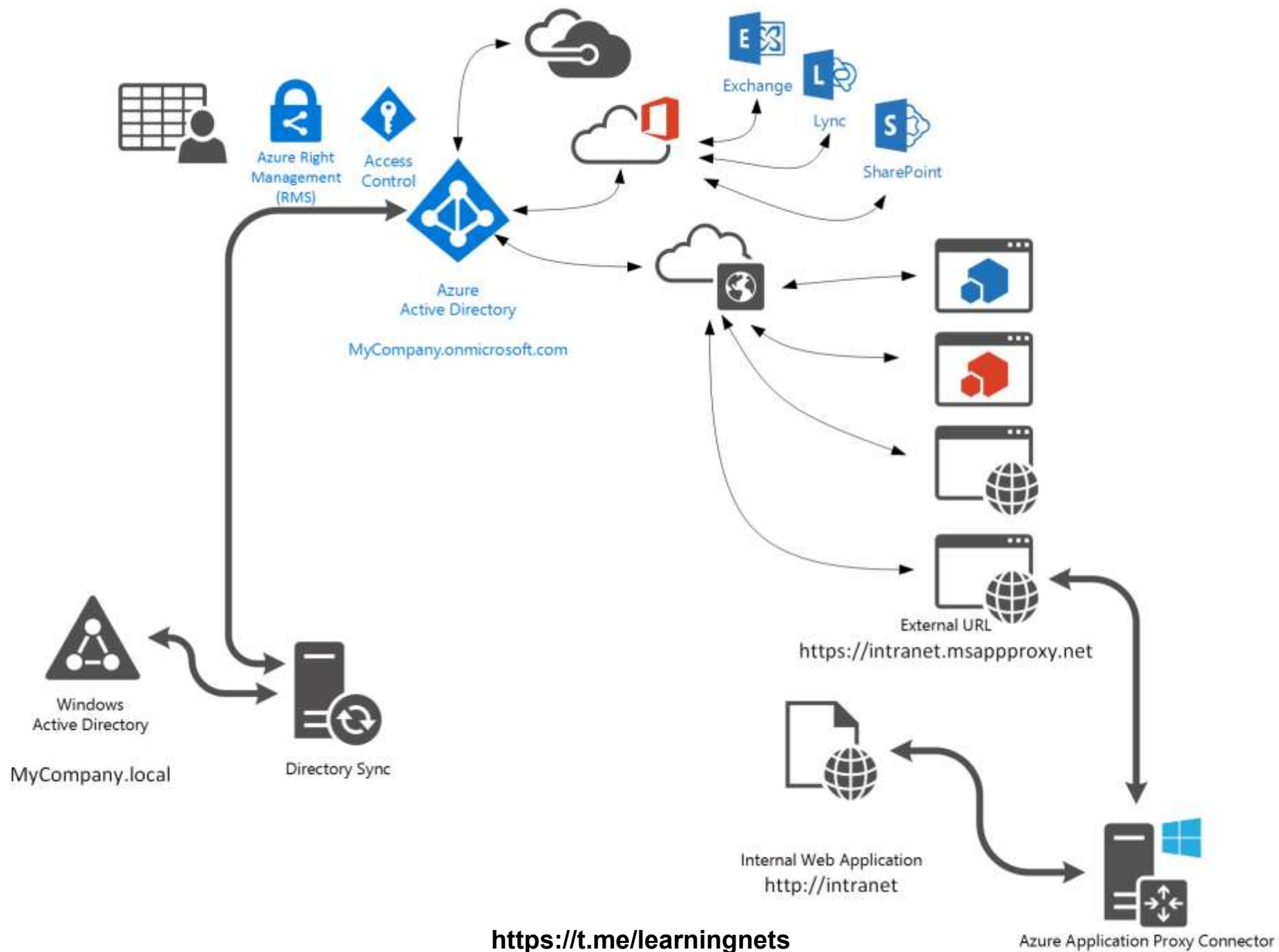
<https://t.me/learningnets>



<https://t.me/learningnets>



<https://t.me/learningnets>



<https://t.me/learningnets>

Azure Application Proxy Connector



1 applications groups approvals profile



Showing 4 of 4

Azure AD Reports

▲ ANOMALOUS ACTIVITY

Sign ins from unknown sources

Sign ins after multiple failures

Sign ins from multiple geographies

Sign ins from IP addresses with suspicious activity

Sign ins from possibly infected devices

Irregular sign in activity

Users with anomalous sign in activity

Users with leaked credentials

▲ ACTIVITY LOGS

Audit report

Password reset activity

Password reset registration activity

Self service groups activity

▲ INTEGRATED APPLICATIONS

Application usage

Account provisioning activity

Password rollover status

Account provisioning errors

▲ RIGHTS MANAGEMENT

RMS usage

Most active RMS users

RMS device usage

RMS enabled application usage

▲ EXTERNAL ACCESS

Invitation summary



PROTECTION

ad

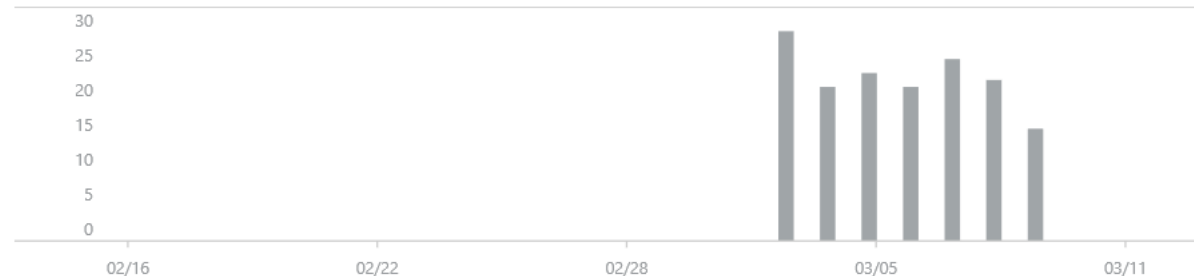
DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	DATE RANGE (UTC)
Real-time	Sign-ins from anonymous IP address(es)	163 of 163	3/3/2016 - 3/9/2016
Real-time	Sign-ins from unfamiliar location(s)	2 of 2	3/9/2016 - 3/10/2016

Sign-ins from anonymous IP addresses

RISK EVENTS

- Last 30 days
- Columns
- Details
- Download

Apply a sign-in risk policy for automatic mitigation. →



ACTIVE 0 CLOSED 163

USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
Candy Dominguez	93.184.66.227	Bratislava, Bratislavsky, SK	▶ 4 instances	Closed (p
Candy Dominguez	37.130.227.133	Redbridge, Greater London,...	▶ 4 instances	Closed (p
Candy Dominguez	66.180.193.219	Los Angeles, California, US	▶ 2 instances	Closed (p
Candy Dominguez	173.254.216.69	Los Angeles, California, US	▶ 2 instances	Closed (p
Candy Dominguez	195.154.56.44	Paris, Paris, FR	▶ 3 instances	Closed (p
Candy Dominguez	171.25.193.78	Stockholm, Stockholms Lan,...	▶ 2 instances	Closed (p

Conditional Access Control

User attributes

- User identity
- Group memberships
- Auth strength (MFA)

Devices

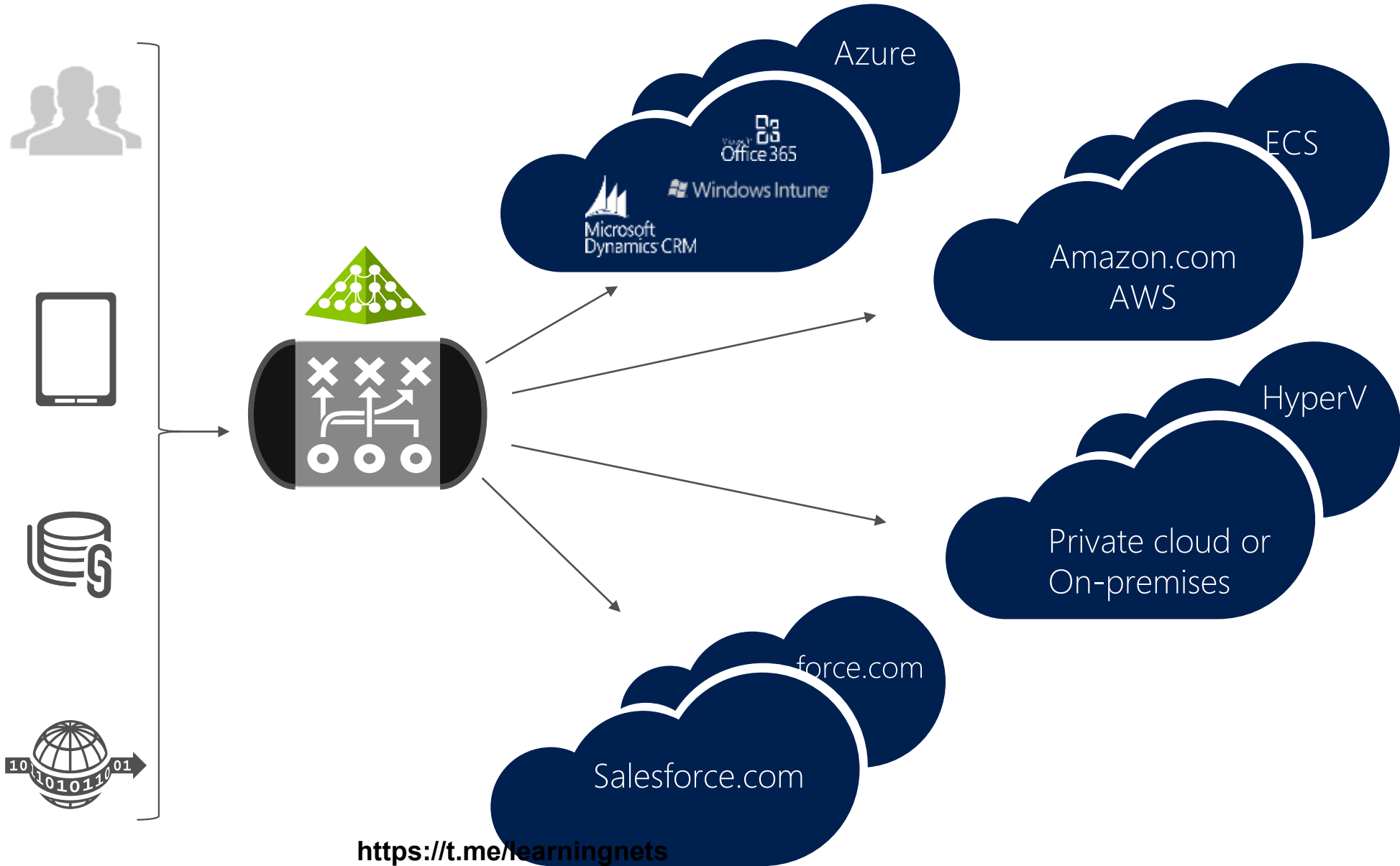
- Known to organization
- MDM Managed (Intune)
- Compliant with policies
- Not lost/stolen

Application

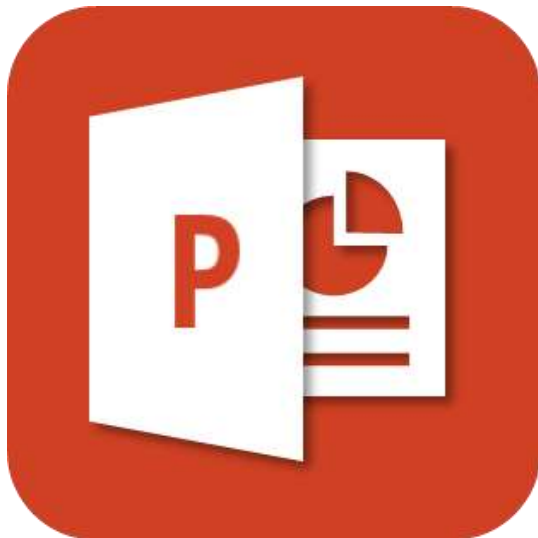
- Business sensitivity

Other

- Inside corp. network
- Outside corp. network
- Risk profile



MDM beyond email



Supported Platforms



Mobile Device Management for Office 365

User-centric approach

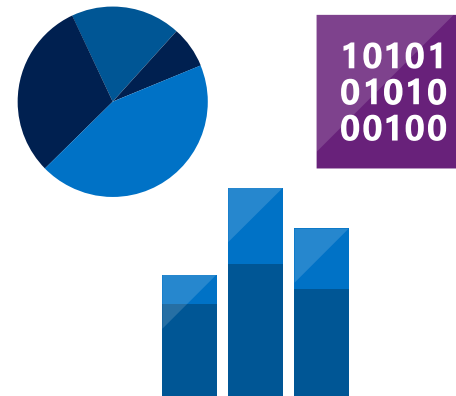
Conditional Access



Device Management



Selective Wipe



Application Management



Built-In

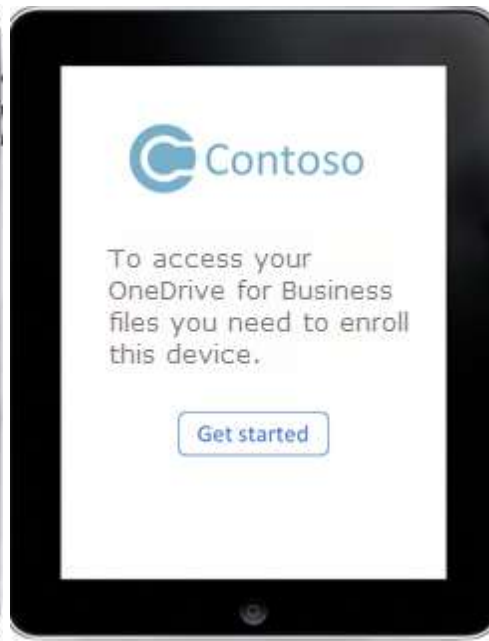
+ Microsoft Intune

Conditional Access

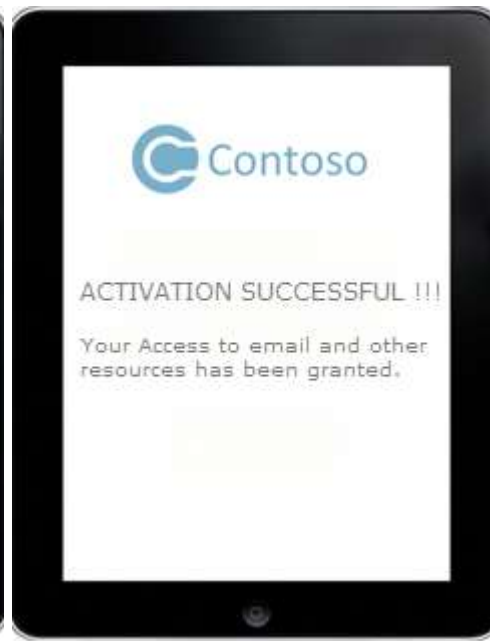
Before mobile devices can access Office 365 data, they must be enrolled and healthy.



1. A user downloads the public OneDrive app on a personal iPad



2. The user is shown a page that directs them to enroll the iPad



3. The user steps through the enrollment process



4. The OneDrive app is now MDM enabled



5. The user is able to access their OneDrive data

Device Management

Device Policies

- Control what mobile devices can connect to Office 365 Data
- Set device configuration policies such as pin lock
- Enforce data encryption on devices

Admin Controls

- Built-In management in Office 365 Admin Center, and PowerShell
- Configure device policies by groups
- Product level granular control

Device Reporting

- Device compliance reports
- Mobile usage and trends in our organization
- API support

The screenshot shows a configuration window titled "New Device Security Policy" with a "Help" link in the top right corner. The main question is "What requirements do you want to have on devices?". The configuration options are as follows:

- Require a password
- Prevent simple password
- Require an alphanumeric password:
Password must include at least character sets
- Minimum password length:
 characters
- Number of sign-in failures before device is wiped
 attempts
- Minutes of inactivity before device is locked:
 minutes
- Password expiration:
 days
- Remember password history and prevent reuse:
Store up to previous passwords
- Require data encryption on devices
- Device cannot be jail broken or rooted

At the bottom of the window, there are three buttons: "back", "next", and "cancel". A vertical scrollbar is visible on the right side of the configuration area.

Selective Wipe

The IT admin can wipe Office 365 data from the user's device. When they trigger the wipe, all of the data cached or stored by the apps will be deleted, while all of the user's personal content remains intact.



1. An employee uses Office 365 apps and data on a mobile device. The employee leaves the company.



2. The IT admin logs into Office 365 Admin Center to perform a selective wipe



3. The Office 365 data is removed from the Office applications leaving personal information intact

Mobile Application Management with Microsoft Intune

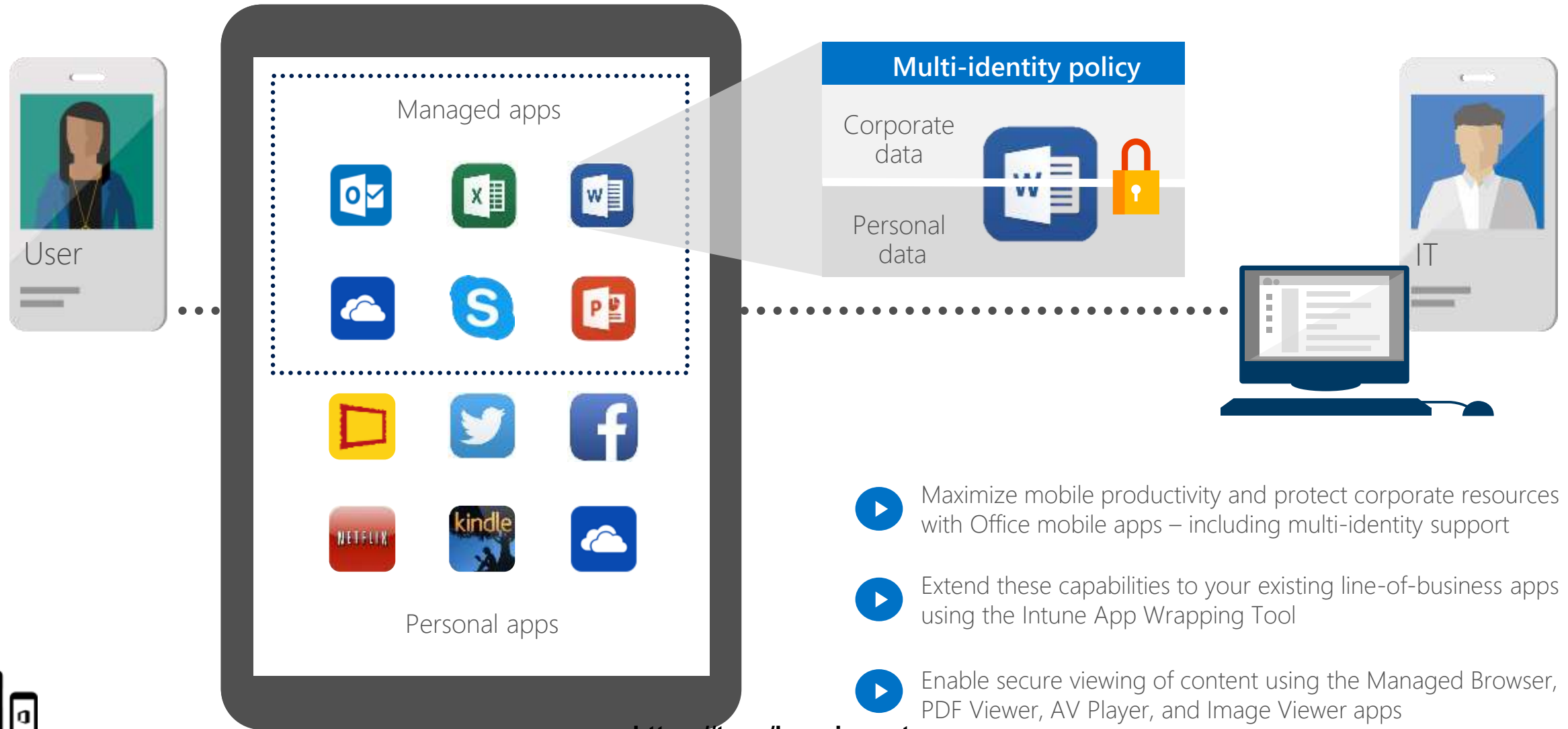


Manage all of your corporate apps and data with Intune's mobile device and application management solution

Complete mobile application management

- Securely access corporate information using Office mobile apps, while preventing company data loss by restricting actions such as copy/cut/paste/save in your managed app ecosystem
- Extend these capabilities to existing line of business apps using the Intune app wrapper
- Enable secure viewing of content using the Managed Browser, PDF Viewer, AV Player, and Image Viewer apps

Mobile application management



- ▶ Maximize mobile productivity and protect corporate resources with Office mobile apps – including multi-identity support
- ▶ Extend these capabilities to your existing line-of-business apps using the Intune App Wrapping Tool
- ▶ Enable secure viewing of content using the Managed Browser, PDF Viewer, AV Player, and Image Viewer apps



Office Managed Applications Walkthrough



OWA



Word



Managed Br...



Excel



PowerPoint



Messages



Mail



Safari



Music

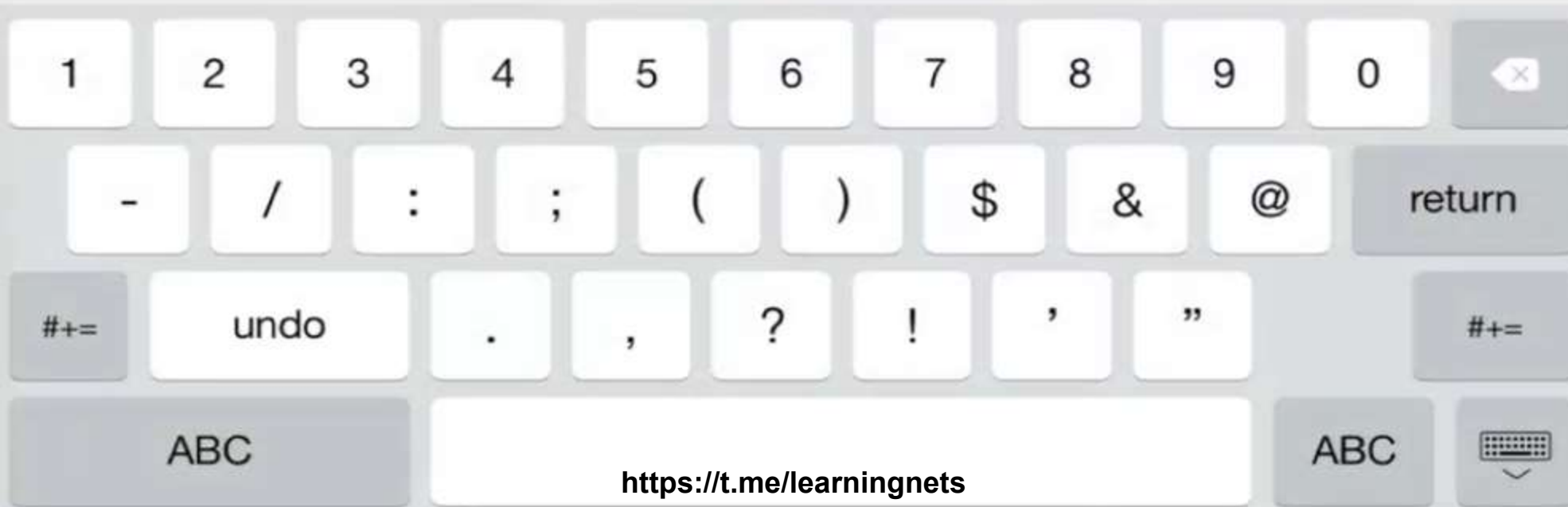
<https://t.me/learningnets>



Managed by your company

Enter your PIN

[Forgot your PIN?](#)





Managed by your company

Enter your PIN

[Forgot your PIN?](#)



<https://t.me/learningnets>

INBOX
all unread to me flagged

LAST MONTH
»
Daniel Emerson
App Store Report Info 6/13/2014
Please see the latest data with the curre...

App Store Report Info



 Daniel Emerson <Daniel.Emerson@microsoft.com>
Fri 6/13/2014 1:49 PM

To: Arianna Moshary;



1 attachment

 App Store reports.xlsx
478 KB

478 KB

Action Items

Please see the latest data with the current app store information.

-Daniel

Connecting...



Office





Managed by your company

Enter your PIN

[Forgot your PIN?](#)

1 2 3 4 5 6 7 8 9 0

- / : ; () \$ & @ return

#+= undo . , ? ! ' " #+=

ABC <https://t.me/learningnets> ABC



Managed by your company

Enter your PIN

[Forgot your PIN?](#)

1 2 3 4 5 6 7 8 9 0

- / : ; () \$ & @ return

#+= undo . , ? ! ' " #+=

ABC <https://t.me/learningnets> ABC

Arianna

New

Recent

Open

New Blank Workbook

Annual Financial Report

Calendar

Channel Marketing Budget

Expense Report

General Ledger

Household Budget

Inventory List

Invoice

Mortgage Loan Calculator

Movie List

Opening...
attachmentBFC07032

Cancel

iPad 1:20 PM attachmentBFC07032 89%

HOME INSERT FORMULAS REVIEW VIEW

Calibri 11 B I U

Read-Only To edit, tap Duplicate and change the resulting copy. Duplicate

fx Germany

Categories		Top Charts		Downloads by Country (Top 10)	
Paid	Top Grossing	Free		Country	Downloads
1	Minecraft - Pocket Edition	\$6.99	1	U.S.A.	12,551,290
2	Loopy HD	\$2.99	2	U.K.	3,296,331
3	Doc McStuffins Paint and Play	\$4.99	3	China	3,060,986
4	Block Iron 3D (original) - Mini Survival FPS Craft...	\$0.99	4	Mexico	1,427,828
5	Surgeon Simulator	\$5.99	5	Germany	1,242,704
6	Skyblock - Survival Game Mission Flying Island	\$2.99	6	Russia	1,181,069
7	Angry Birds Star Wars II	\$0.99	7	Canada	1,122,512
8	foodgawker for iPad	\$1.99	8	Brazil	1,121,363
9			9	Australia	1,114,262
10			10	France	936,482

Numbers are for illustration purposes only

Downloads by Coun... Downloads by Product

Sum : 0

<https://t.me/learningnets>

Read-Only To edit, tap Duplicate and change the resulting copy. Duplicate

Country

C D E F G H I J K L M

Cut Copy Paste Clear Delete Wrap

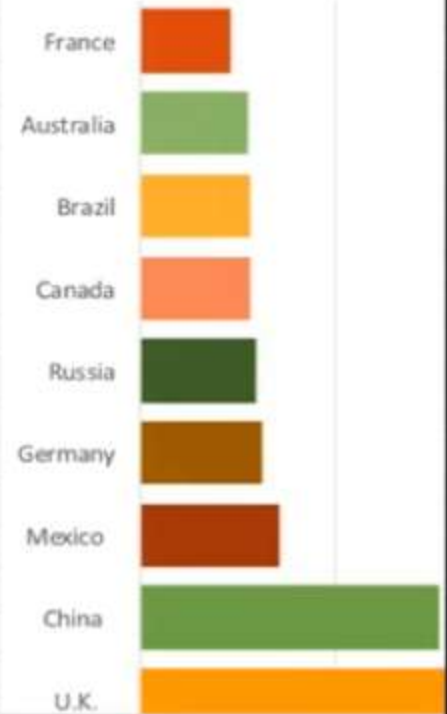
Top Charts

Free

- 1 Microsoft Word for iPad Productivity
- 2 Microsoft Excel for iPad Productivity
- 3 Microsoft PowerPoint for iPad Productivity
- 4 Microsoft OneNote for iPad Productivity
- 5 Boom Beach Games
- 6 2048 Games
- 7 Smash Hit Games
- 8 Star Wars: Assault Team Games

Country	Downloads
U.S.A.	12,551,290
U.K.	3,296,331
China	3,060,986
Mexico	1,427,828
Germany	1,242,704
Russia	1,181,069
Canada	1,122,512
Brazil	1,121,363
Australia	1,114,262
France	936,482

Numbers are for illustration purposes only



iPad 1:20 PM attachmentBFC07032 89%

HOME INSERT FORMULAS REVIEW VIEW TABLE

Calibri 11 B I U A ABC 123 General Normal

Read-Only To edit, tap Duplicate and change the resulting copy. Duplicate

Country

Country	Downloads
U.S.A.	12,551,290
U.K.	3,296,331
China	3,060,986
Mexico	1,427,828
Germany	1,242,704
Russia	1,181,069
Canada	1,122,512
Brazil	1,121,363
Australia	1,114,262
France	936,482

Downloads by Country (Top 10)

Numbers are for illustration purposes only

Sum : 27054825.2



OWA



Word



Managed Br...



Excel



PowerPoint



Messages



Mail



Safari



Music

<https://t.me/learningnets>



FaceTime



Calendar



Photos



Camera



Contacts



Clock



Maps



Videos



Notes



Reminders



Photo Booth



Game Center



Newsstand



iTunes Store



App Store



Settings



Messages



Mail



Safari



Music

<https://t.me/learningnets>



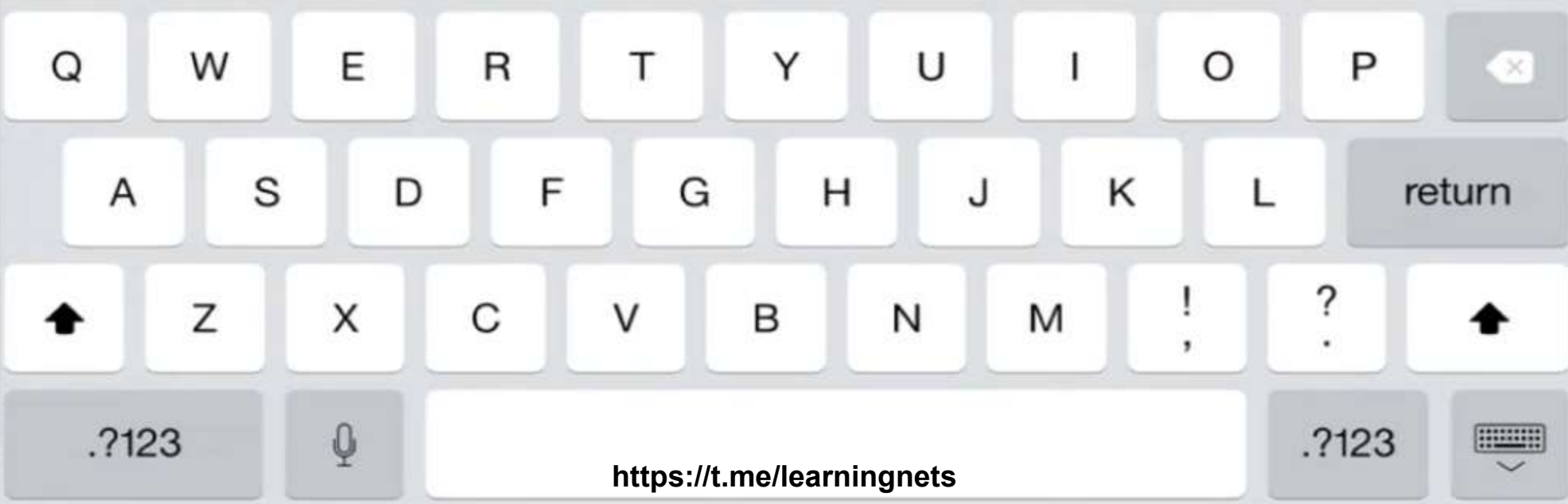
Search

July 29, 2014, 1:21 PM

New Note

Blank lined area for note content

Blank text area for note content



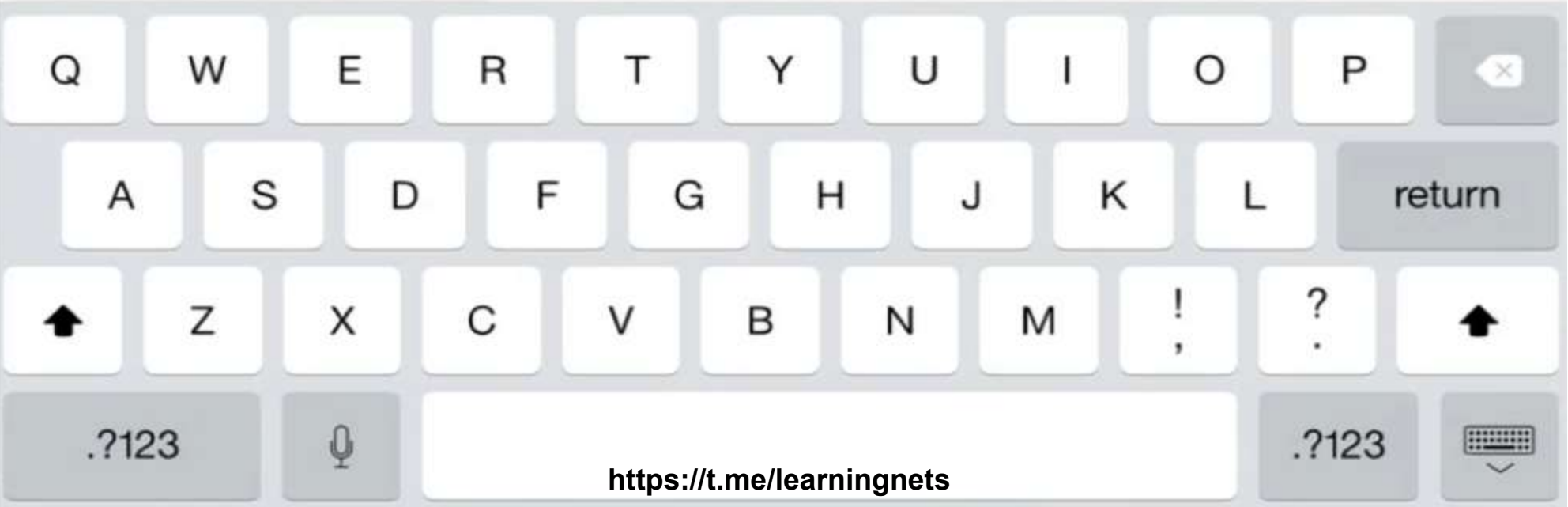
<https://t.me/learningnets>



Search

July 29, 2014, 1:21 PM

New Note





OWA



Word



Managed Br...



Excel



PowerPoint



Messages



Mail



Safari



Music

<https://t.me/learningnets>



Managed by your company

<https://t.me/learningnets>



App Data Report:

Additional references:

<http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1>

iPad 1:21 PM Report 89%

HOME INSERT LAYOUT REVIEW VIEW

Calibri 21 B I U A.. A

Select Select All Paste Insert...

App data report:

Additional references:

<http://windows.microsoft.com/is-IS/windows->

Q W E R T Y U I O P

A S D F G H J K L return

↑ Z X C V B N M ! ?

.?123 .?123

<https://t.me/learningnets>

U.K.	3,296,331
China	3,060,986
Mexico	1,427,828
Germany	1,242,704
Russia	1,181,069
Canada	1,122,512
Brazil	1,121,363
Australia	1,114,262
France	936,482



iPad 1:21 PM Report 89%

HOME INSERT LAYOUT REVIEW VIEW

Calibri 21 B I U A.. A

Additional references:
<http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1>

Q W E R T Y U I O P
A S D F G H J K L return
↑ Z X C V B N M ! ?
.?123 .?123

<https://t.me/learningnets>



HOME INSERT LAYOUT REVIEW VIEW

Calibri 21 B [font icons]

Hyperlink

<http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1>

Open

Copy

Edit >

Additional r
<http://wind>
<8/apps#Ca>

<IS/windows->



<https://t.me/learningnets>



Managed by your company



<https://t.me/learningnets>



Managed by your company

Enter your PIN

[Forgot your PIN?](#)

1 2 3 4 5 6 7 8 9 0

- / : ; () \$ & @ return

#+= undo . , ? ! ' " #+=

ABC <https://t.me/learningnets> ABC



Managed by your company

Enter your PIN

[Forgot your PIN?](#)





http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1%25EE%2583%259C%25E3%25A8%25...



Loading



Loading

[MEET WINDOWS](#) [PCs+TABLETS](#) [DOWNLOADS](#) [HOW-TO](#)[Sign in](#)[Features](#) [Apps](#) [Compare](#) [Top questions](#)

Apps for Windows

Popular apps



Halo: Spartan Assault

A new touch-based shooter exclusively for Windows 8 and Windows Phone 8.



Facebook

The official app. Stay in touch, get updates, and chat.



Castles of Illusion Starring Mickey Mouse

A fantastical reimagining of the Sega



writr

An interactive journal and calendar for personal growth.

iPad 1:22 PM 89%

http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1

Cut Copy Paste Define

MEET WINDOWS PCs+TABLETS DOWNLOADS HOW-TO Sign in

Features Apps Compare Top questions

Apps for Windows

Q W E R T Y U I O P

A S D F G H J K L Go

↑ Z X C V B N M , . ↑

.?123 : / - .com .?123

<https://t.me/learningnets>



http://blocked.com



Loading

MEET WINDOWS PCs+TABLETS DOWNLOADS HOW-TO

Sign in

Features Apps Compare Top questions

Apps for Windows

Alert

Access to this website has been blocked.

Contact your IT administrator if you feel you should have access to this resource.

[Close](#) [Learn more](#)

Popular apps



Halo: Spartan Assault
 A new touch-based shooter exclusively for Windows 8 and Windows Phone 8.



Facebook
 The official app. Stay in touch, get updates, and chat.



Castles of Illusion Starring Mickey Mouse
 A fantastical reimagining of the Sega Genesis classic.



writr
 An interactive journal and calendar for personal growth.

End User Enrollment Walkthrough

Enrolling in Office 365 MDM

Connect through Office Apps

Connect to email via
Built-In Email Client

Office
apps

Enrolling in Office 365 MDM

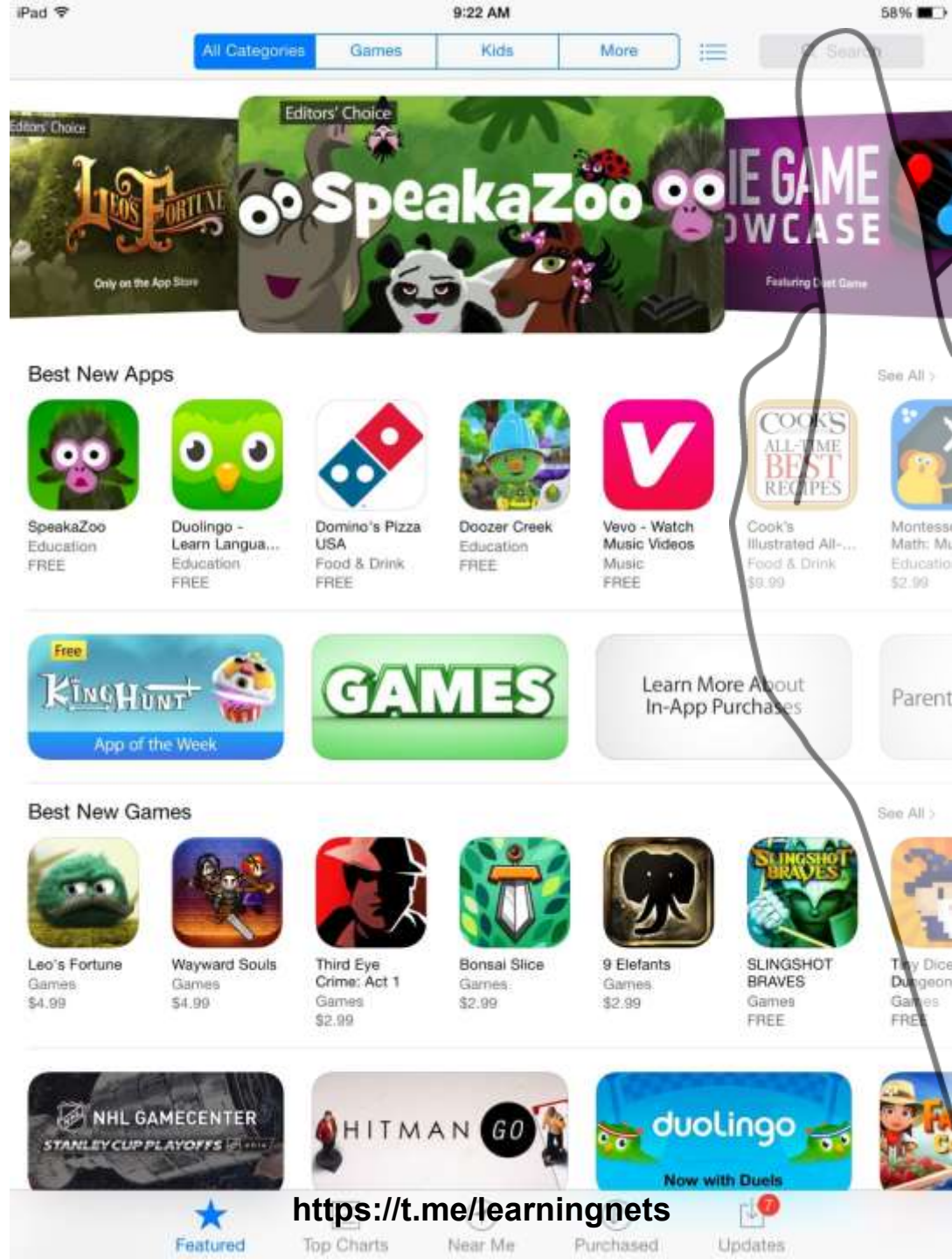


Download & sign into Office
applications

Connect to email via
Built-In Email Client

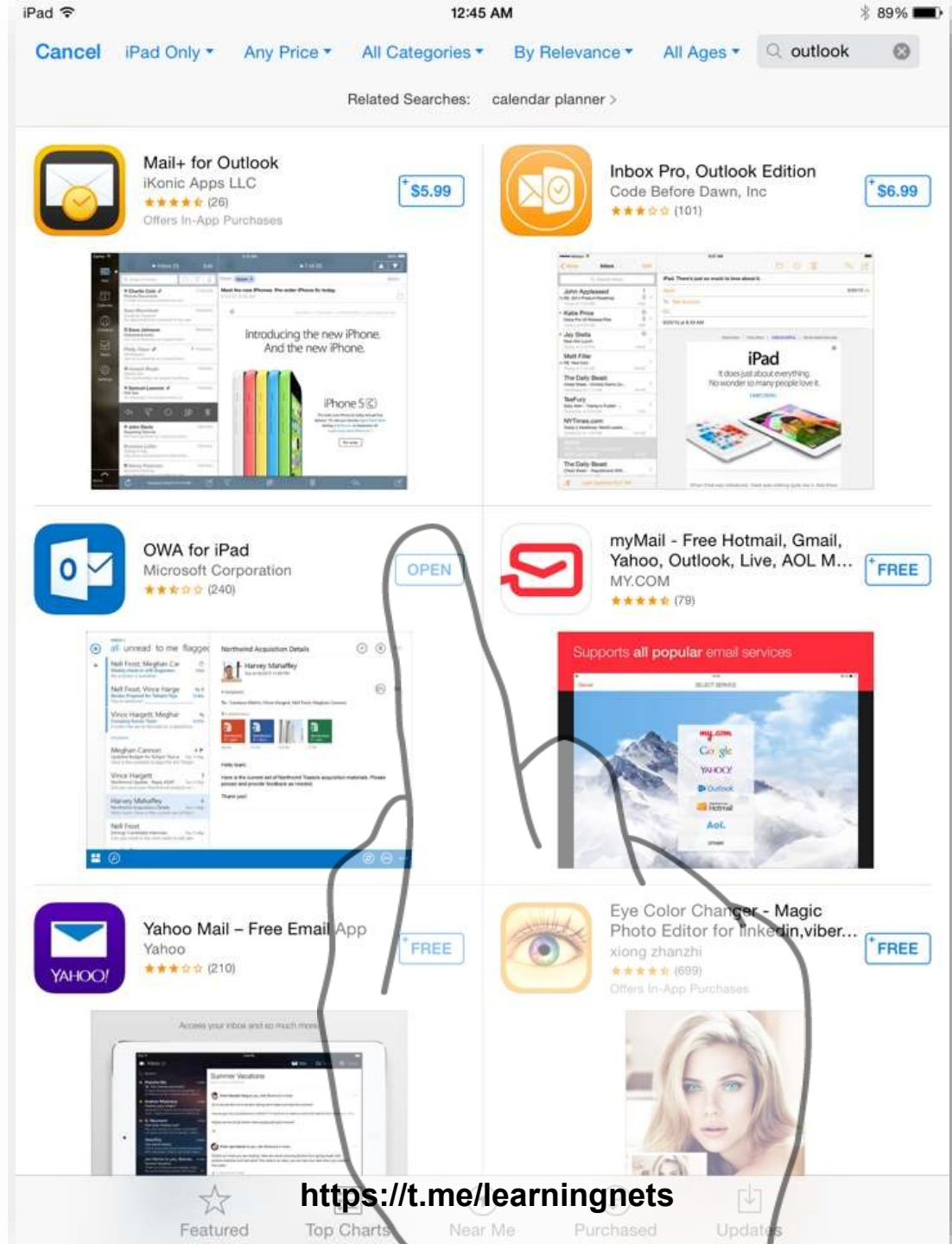
<https://t.me/learningnets>

Office apps

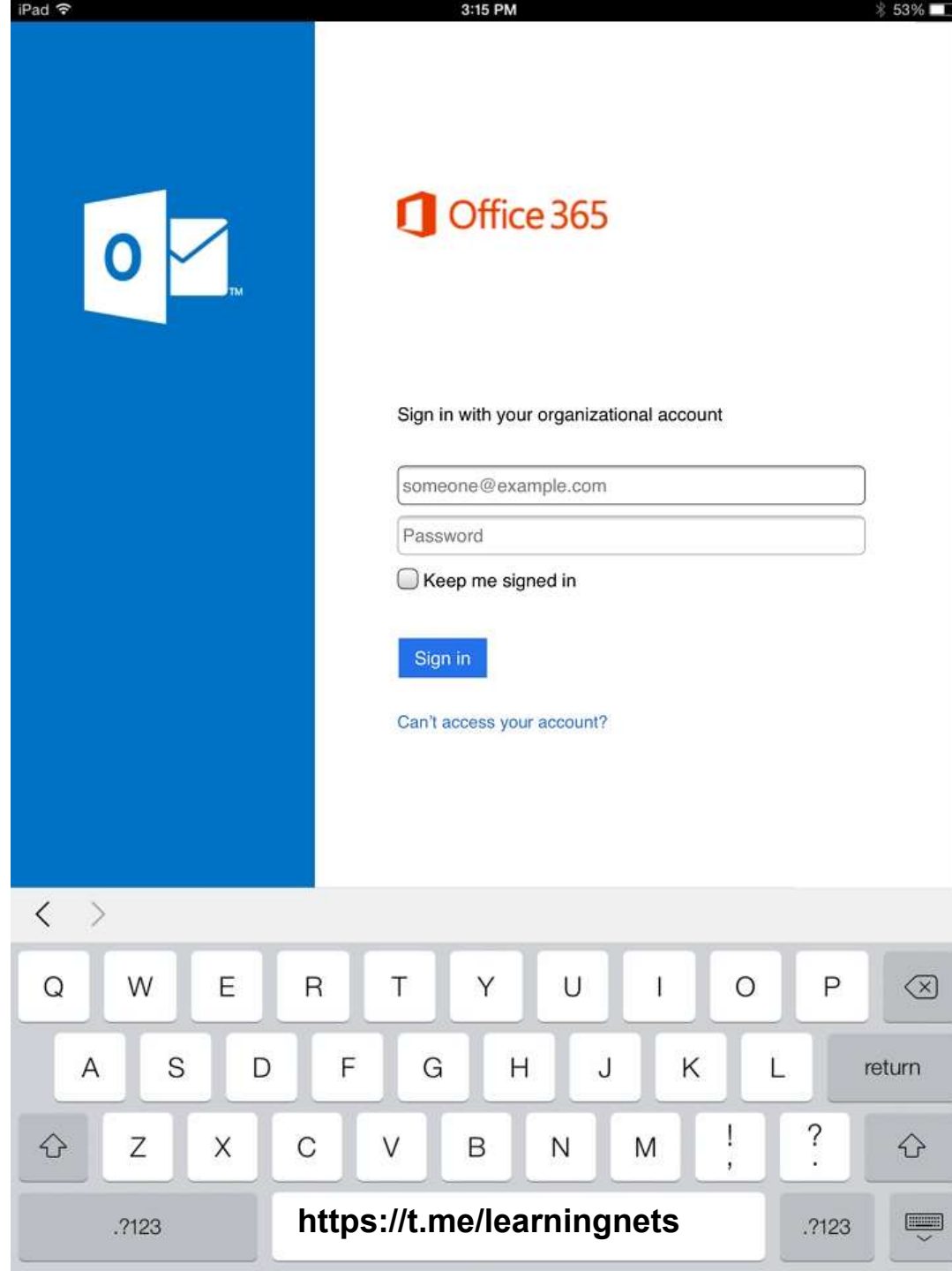


<https://t.me/learningnets>

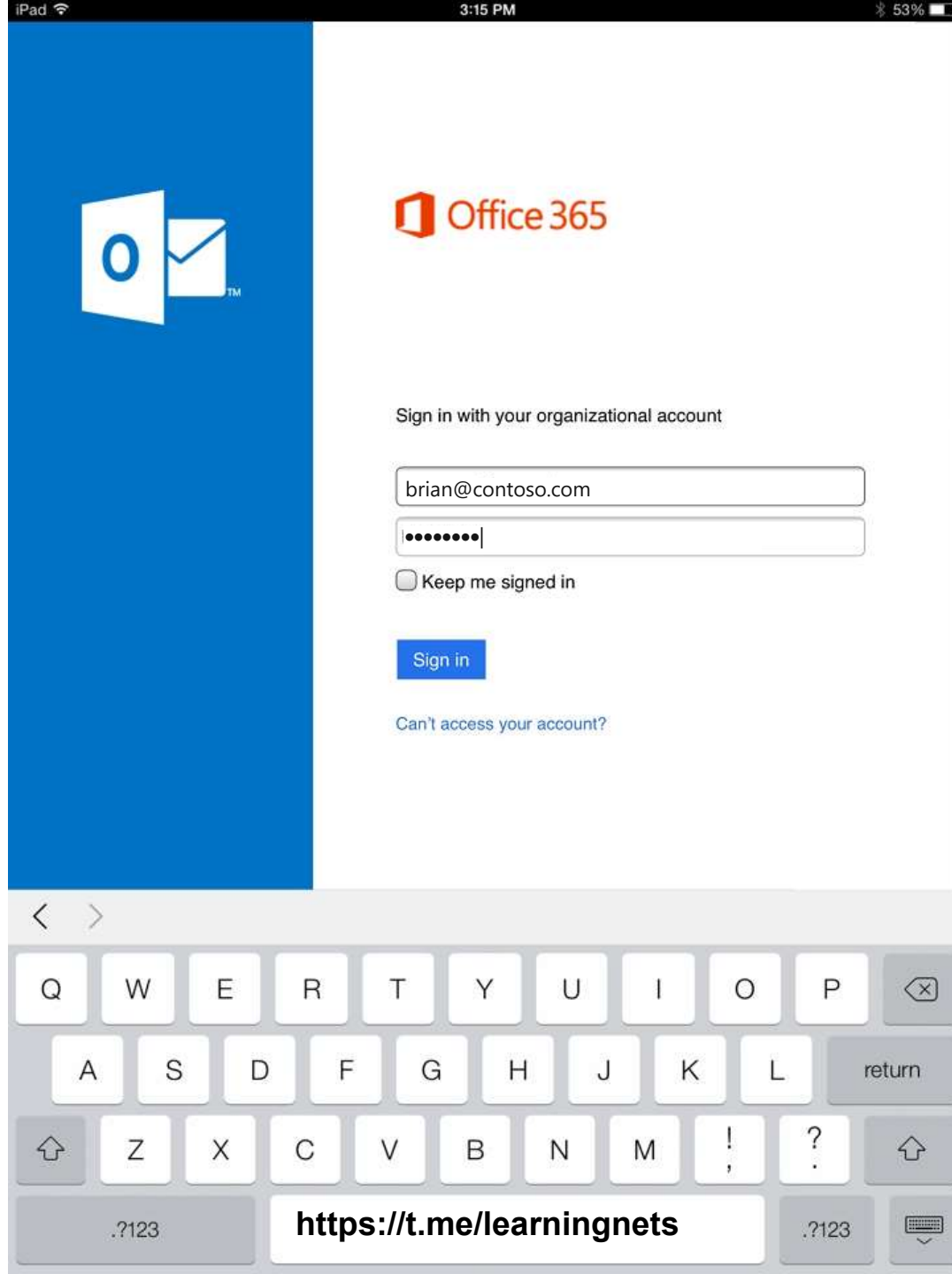
Office apps



Office
apps



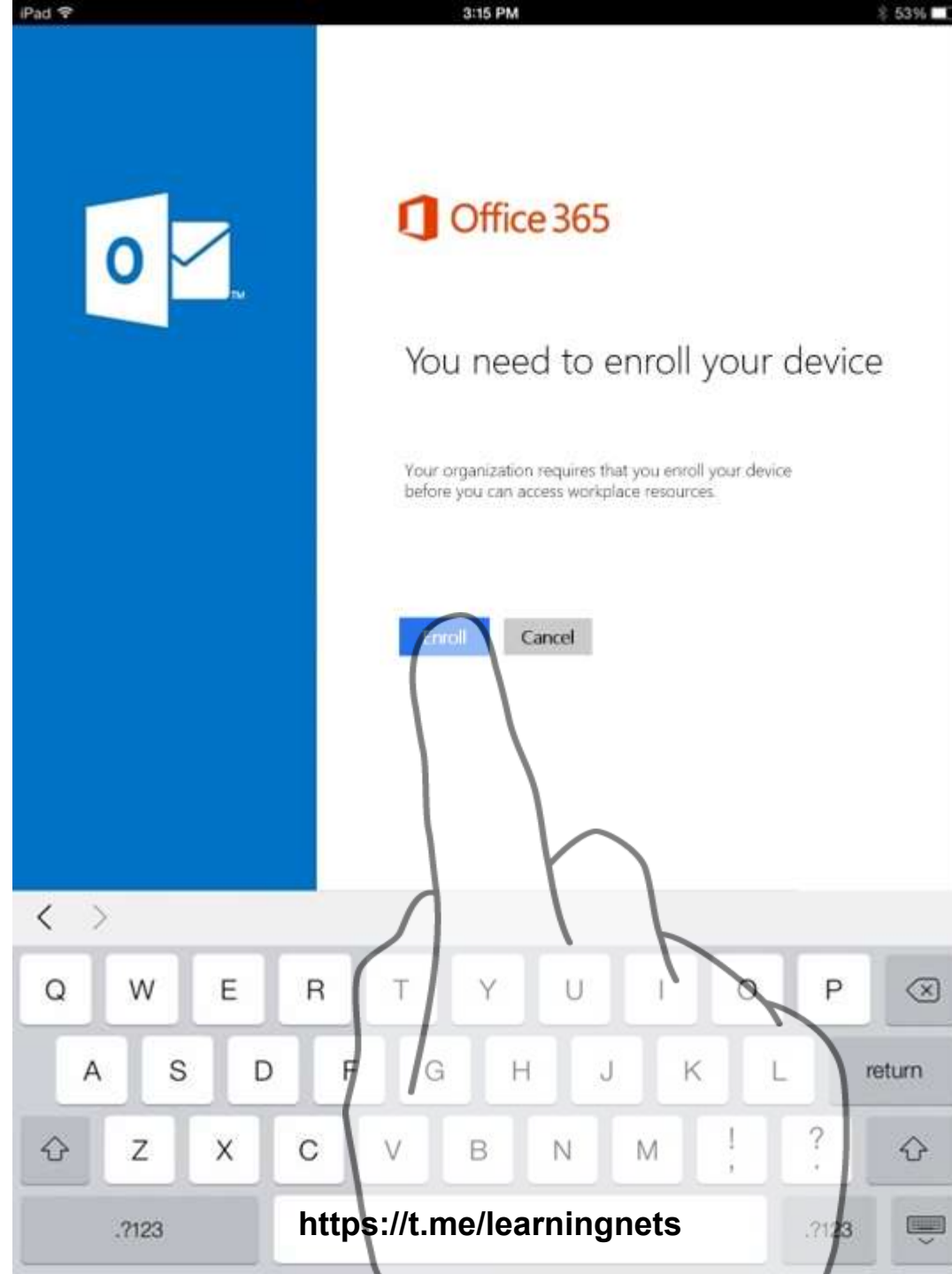
Office
apps



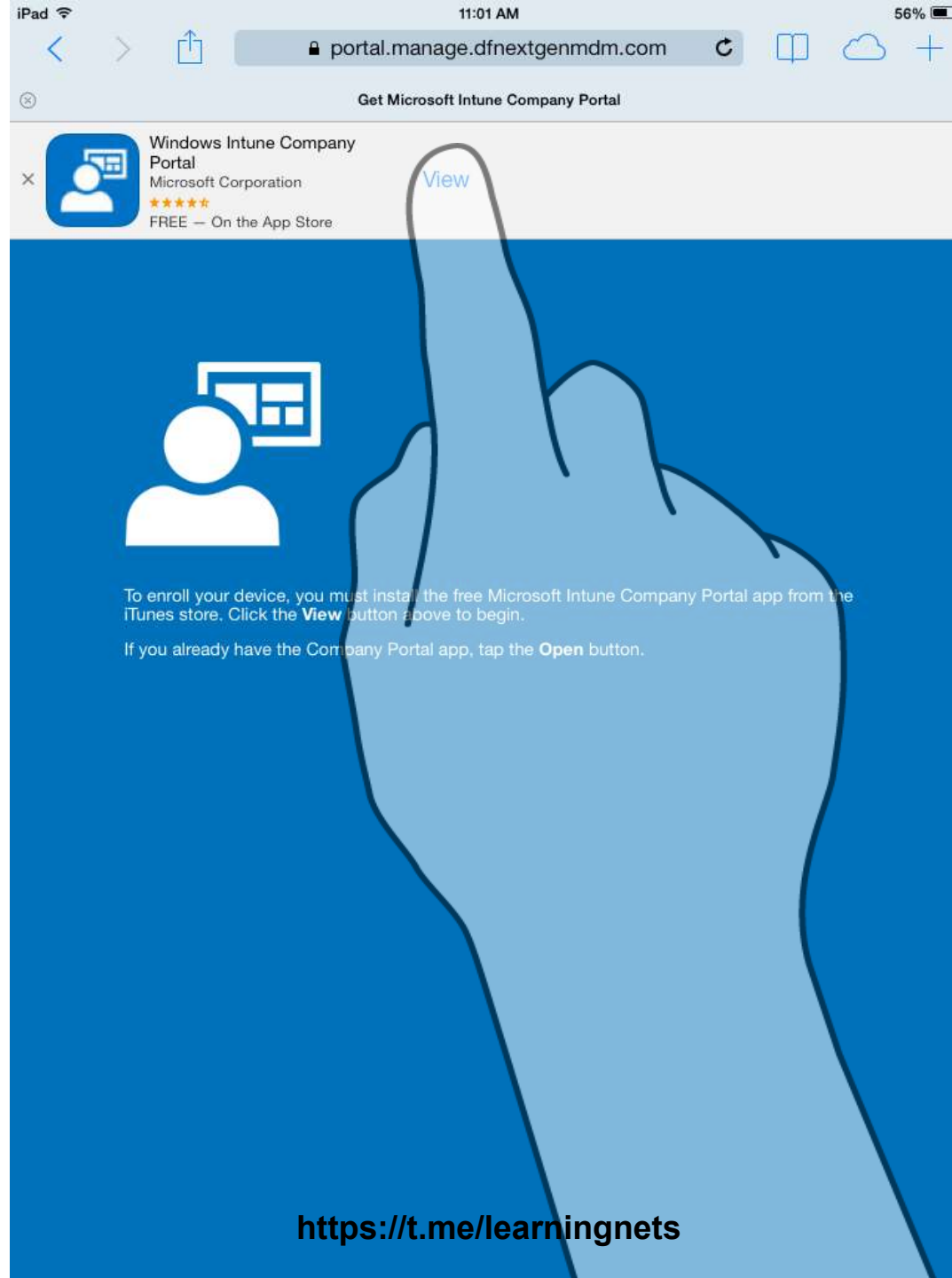
Office apps



Office
apps



Office apps



<https://t.me/learningnets>

Office apps

iPad 11:02 AM 56%

☰ Search

Windows Intune Company Portal

Microsoft Corporation >

★★★★☆

OPEN

Details Reviews Related

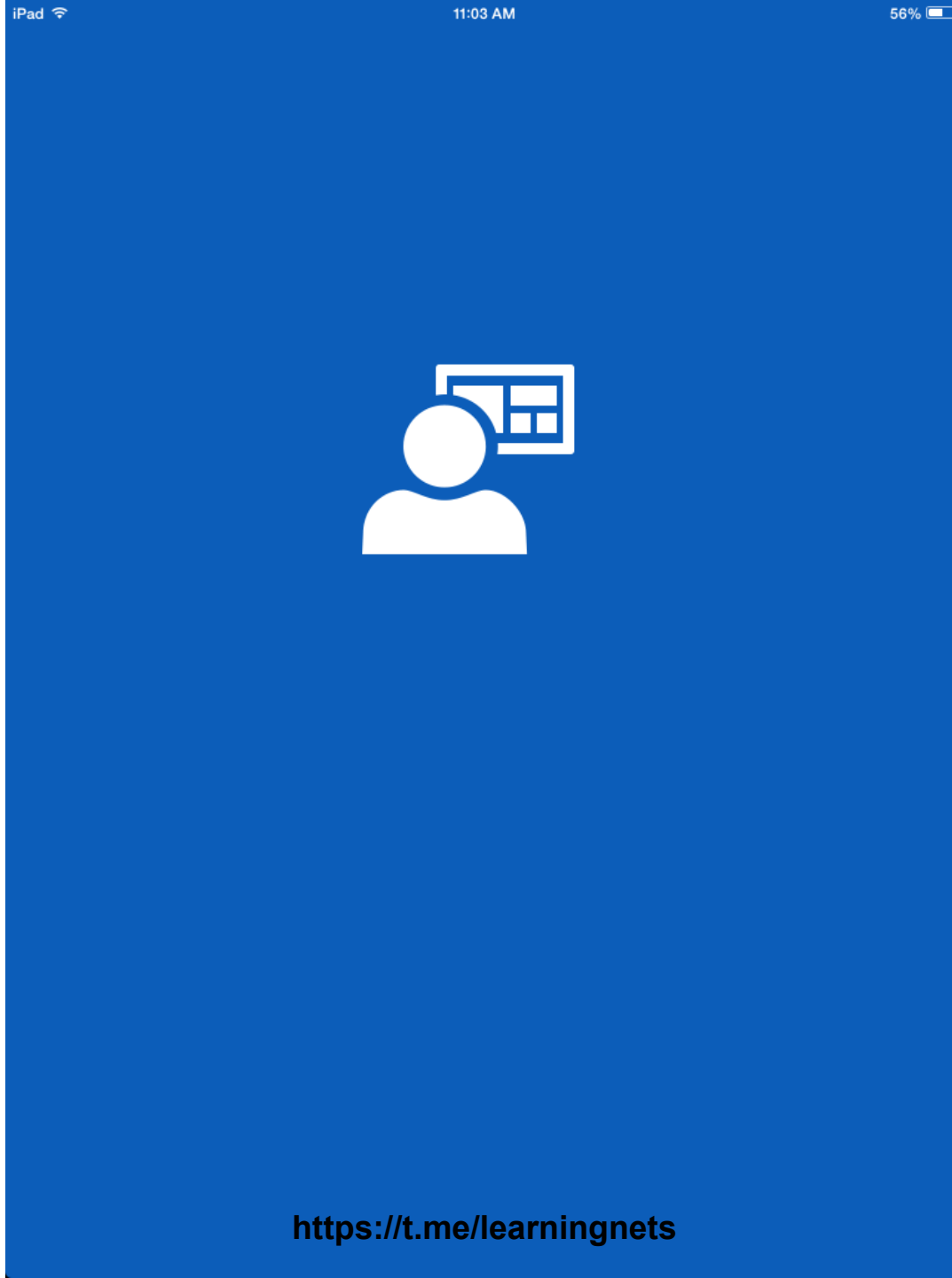
Description

The Company Portal app helps you search, browse and install apps made available to you by your organization through the Windows Intune online service. Apps can be installed without requiring a connection to your

<https://t.me/learningnets>

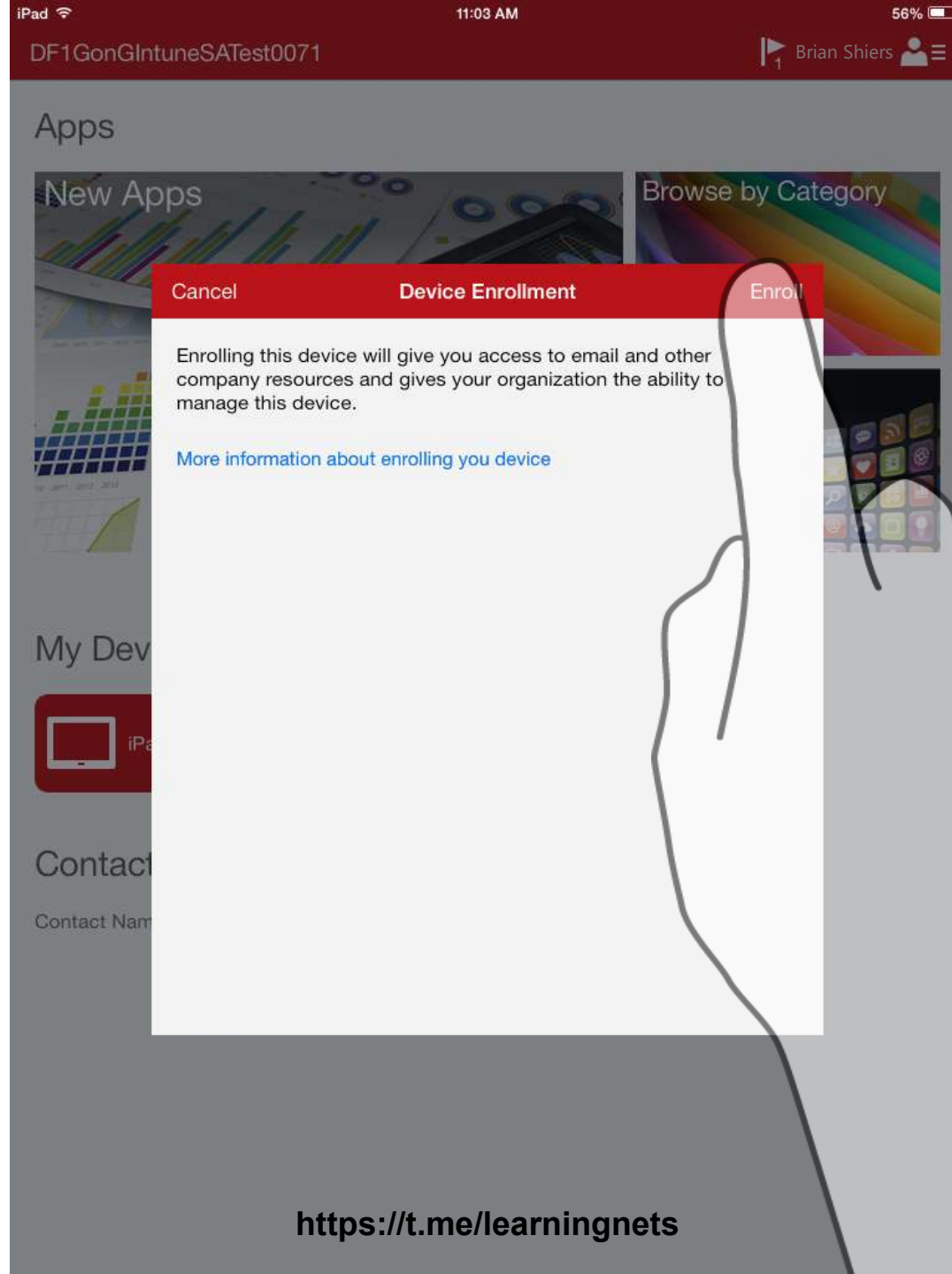
Featured Top Charts Near Me Purchased Updates

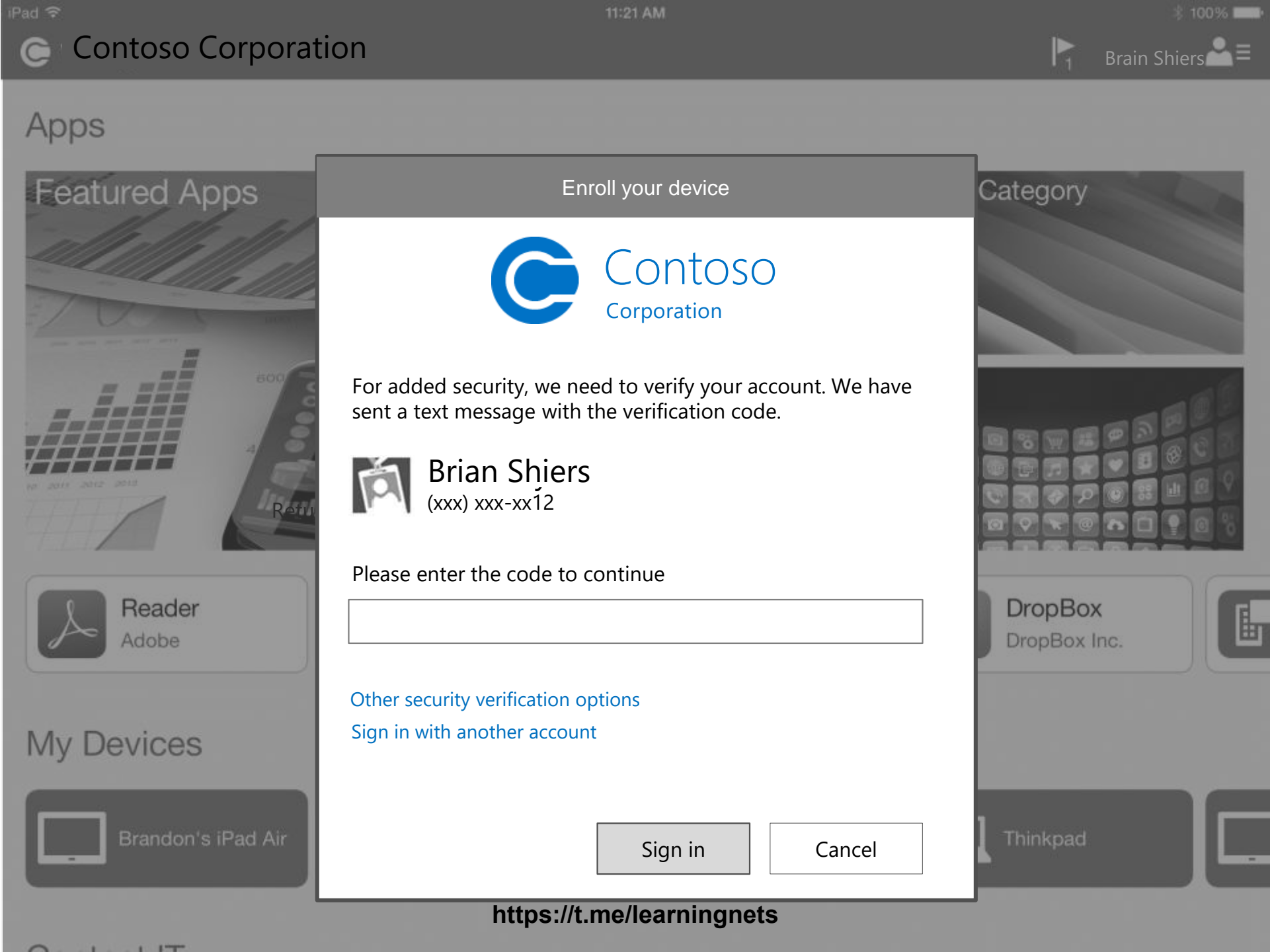
Office
apps



<https://t.me/learningnets>

Office apps





Apps

Featured Apps



My Devices



Enroll your device



For added security, we need to verify your account. We have sent a text message with the verification code.

 **Brian Shiers**
(xxx) xxx-xx12

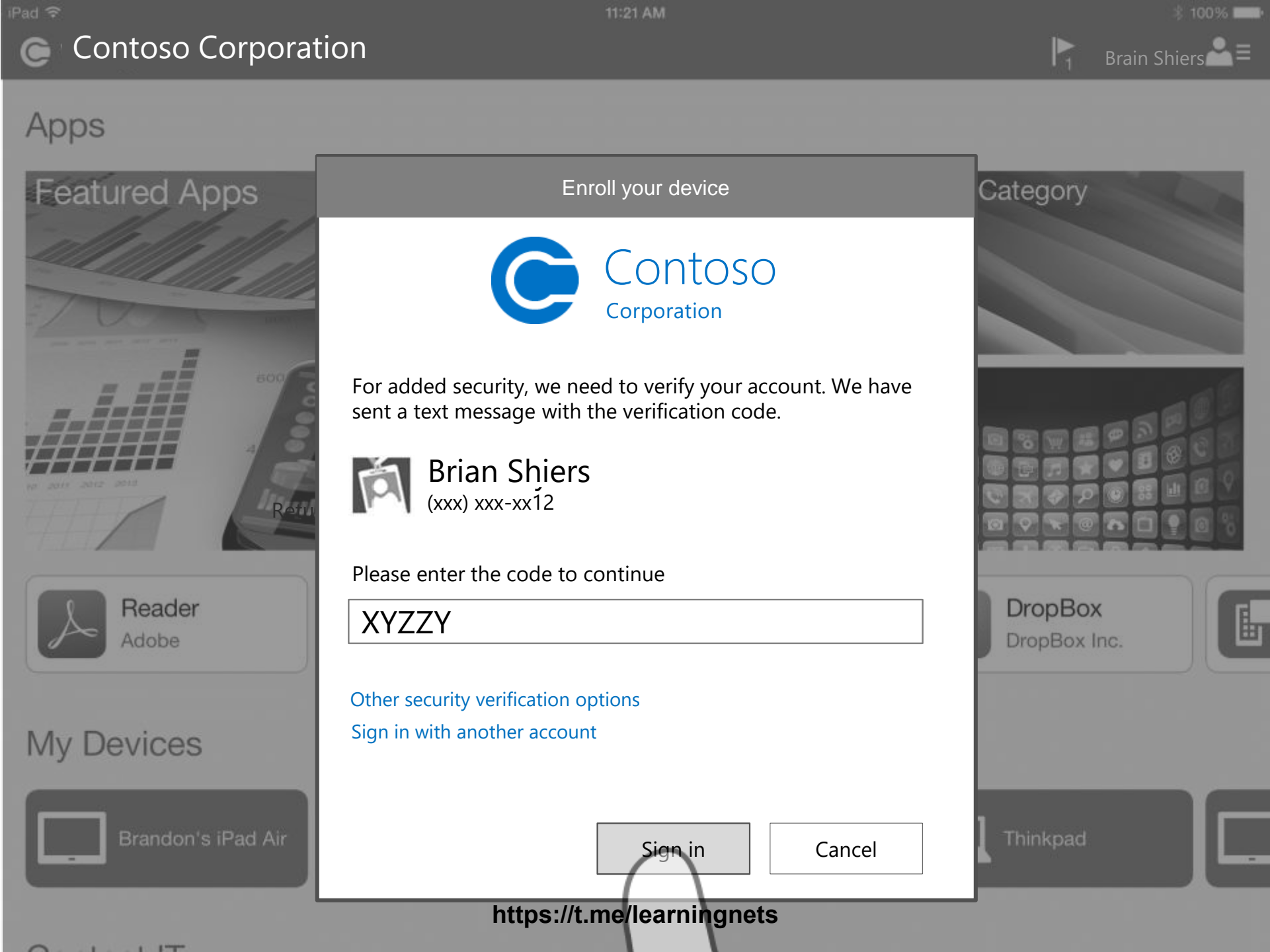
Please enter the code to continue

[Other security verification options](#)
[Sign in with another account](#)

Sign in

Cancel



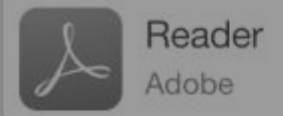
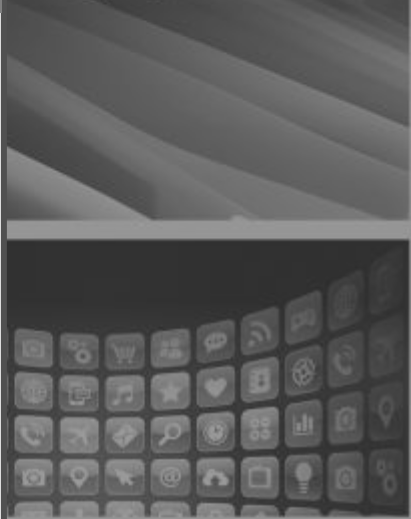


Apps

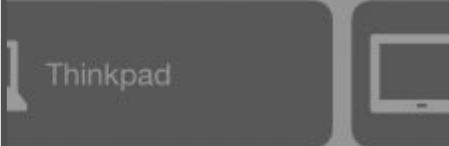
Featured Apps



Category



My Devices



Enroll your device



For added security, we need to verify your account. We have sent a text message with the verification code.

 **Brian Shiers**
(xxx) xxx-xx12

Please enter the code to continue

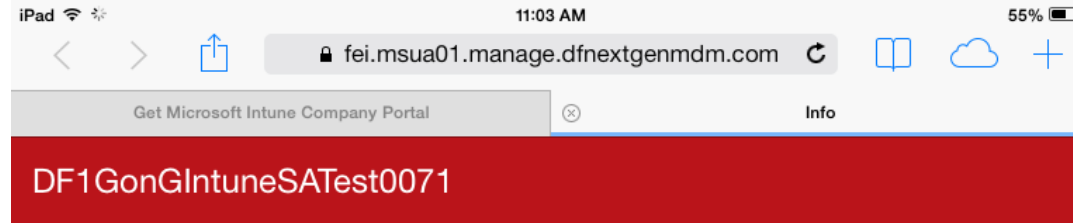
[Other security verification options](#)
[Sign in with another account](#)

Sign in

Cancel



Office
apps



Adding Device...

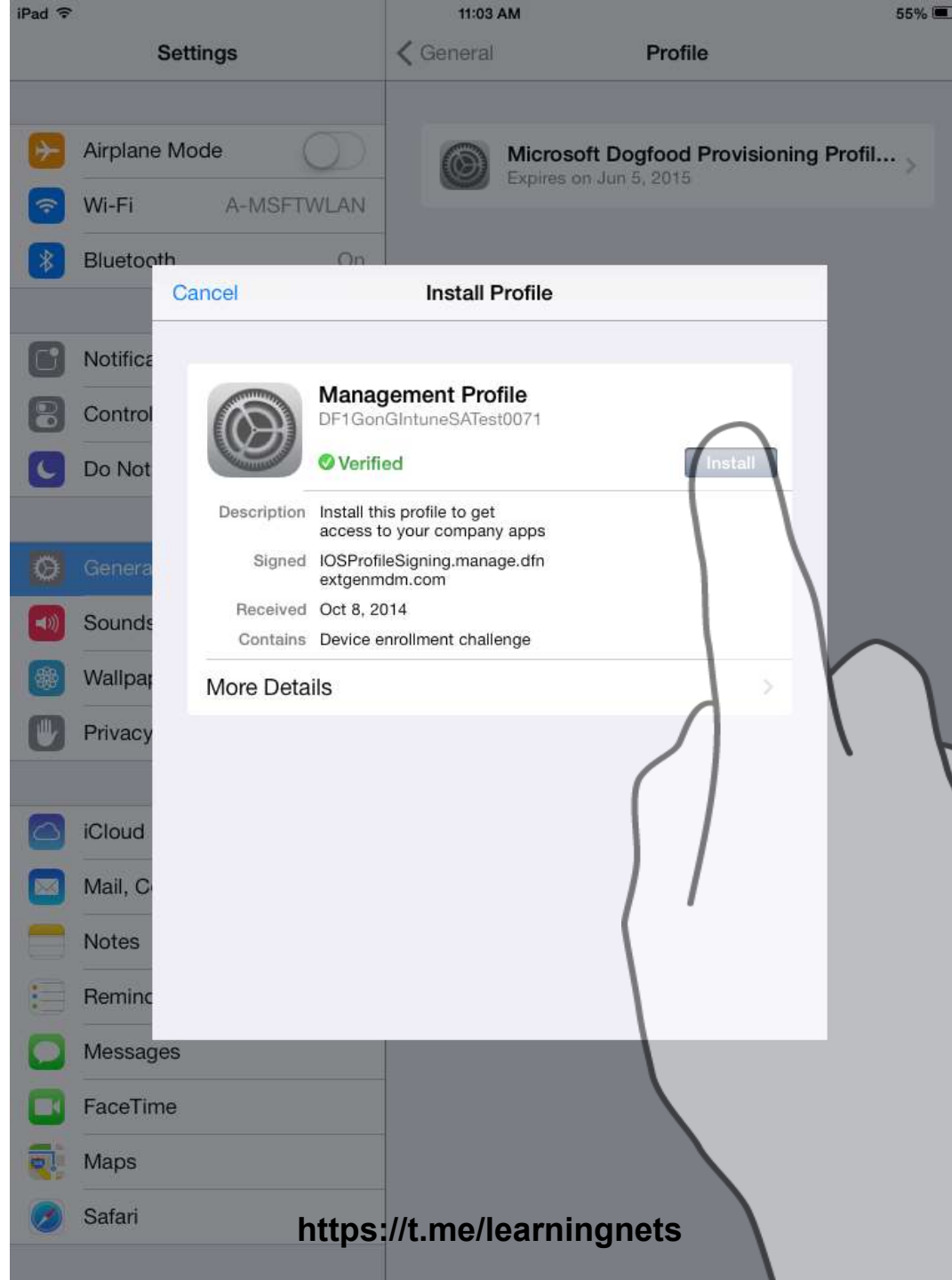
<https://timelearning.net>

[Privacy & Cookies](#)

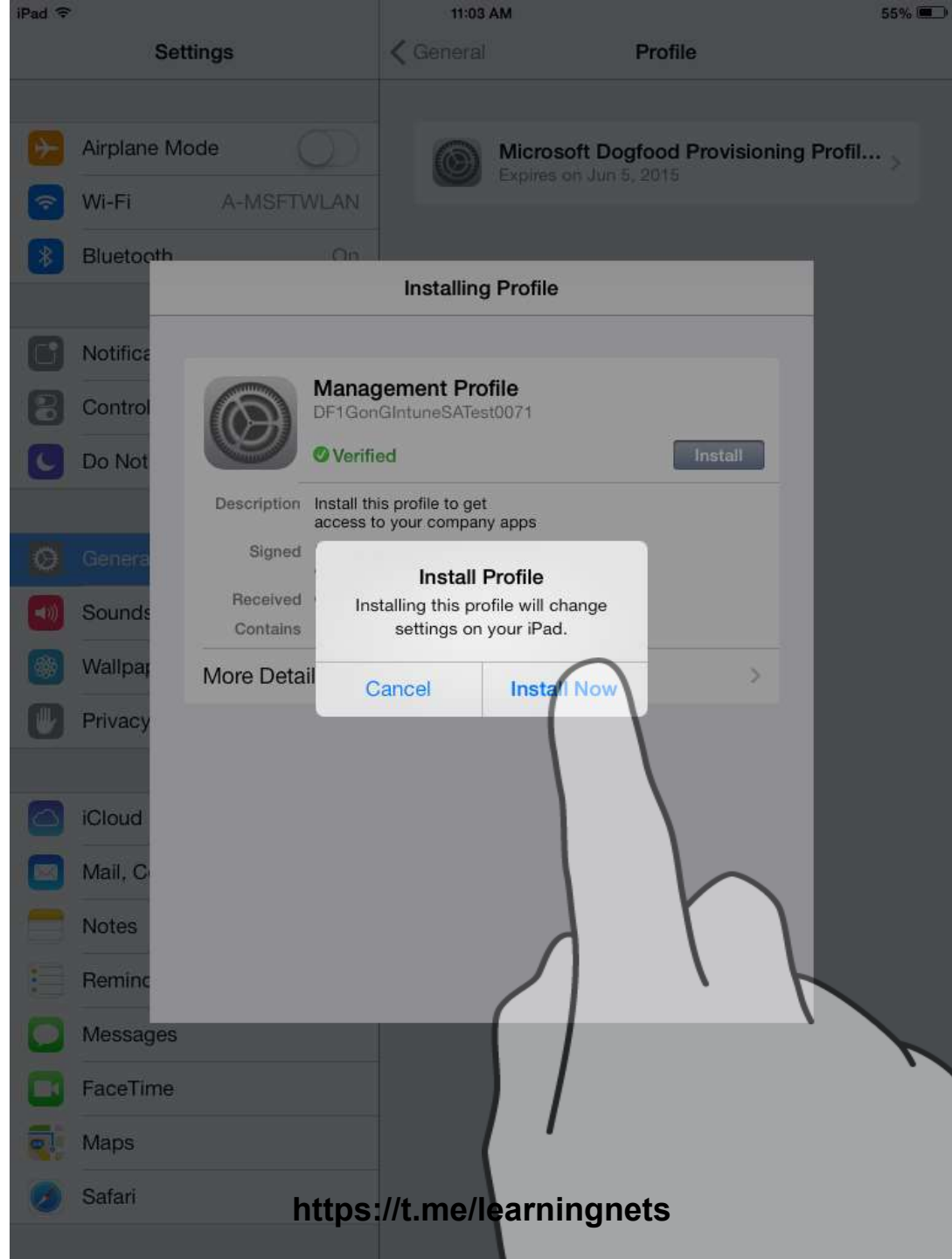
[Terms and conditions](#)

Microsoft Intune © Microsoft 2014

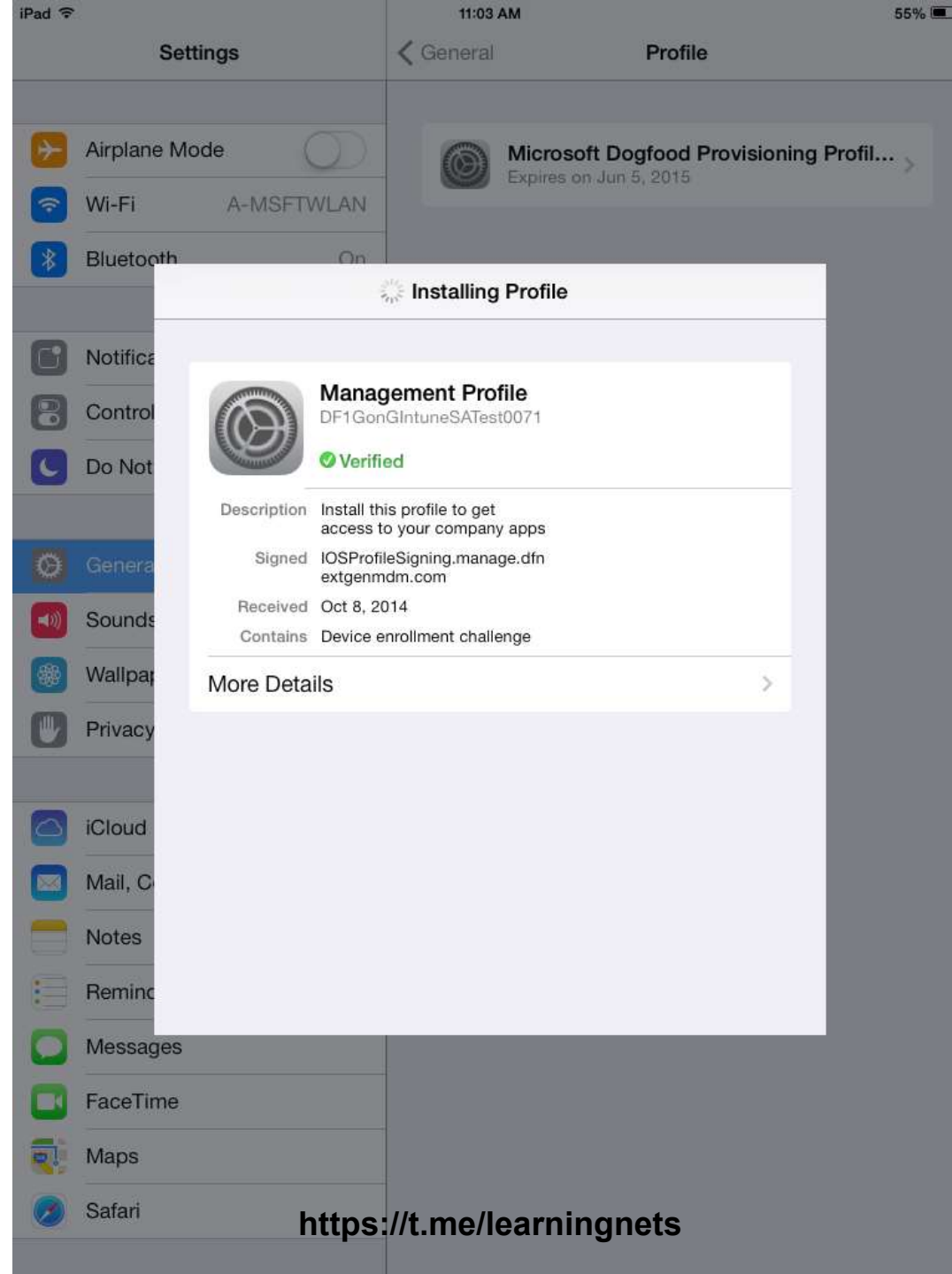
Office apps



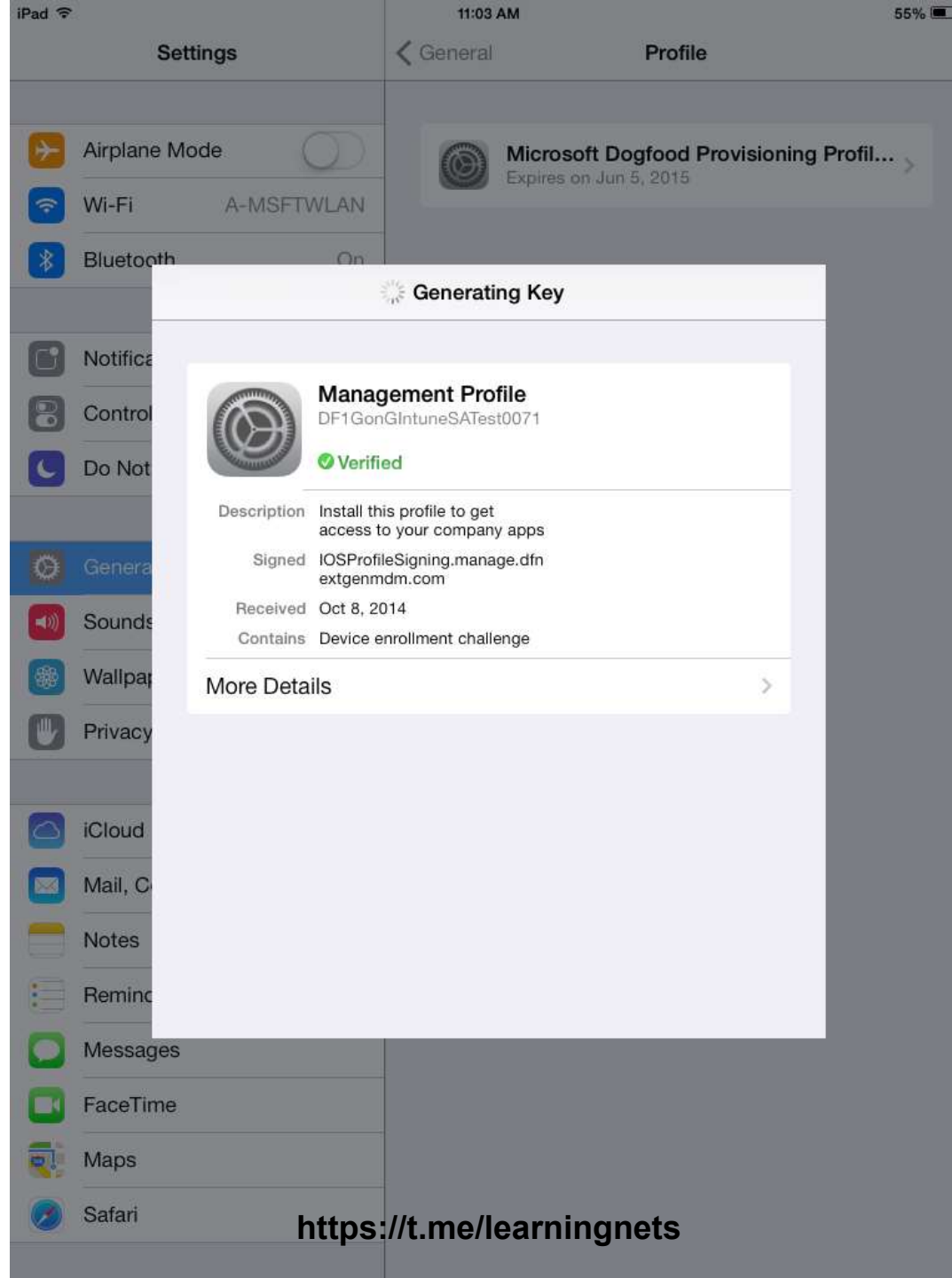
Office apps



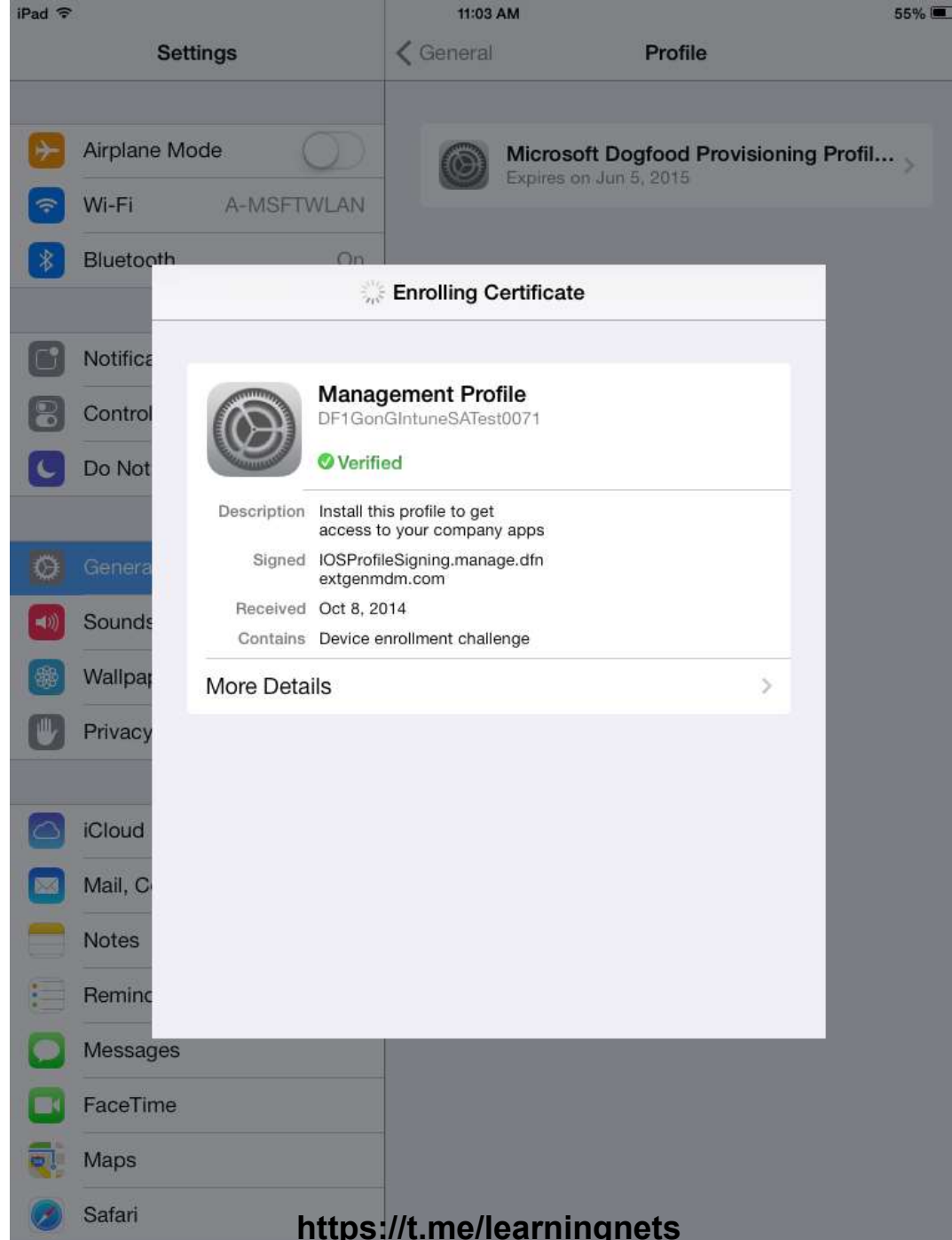
Office apps



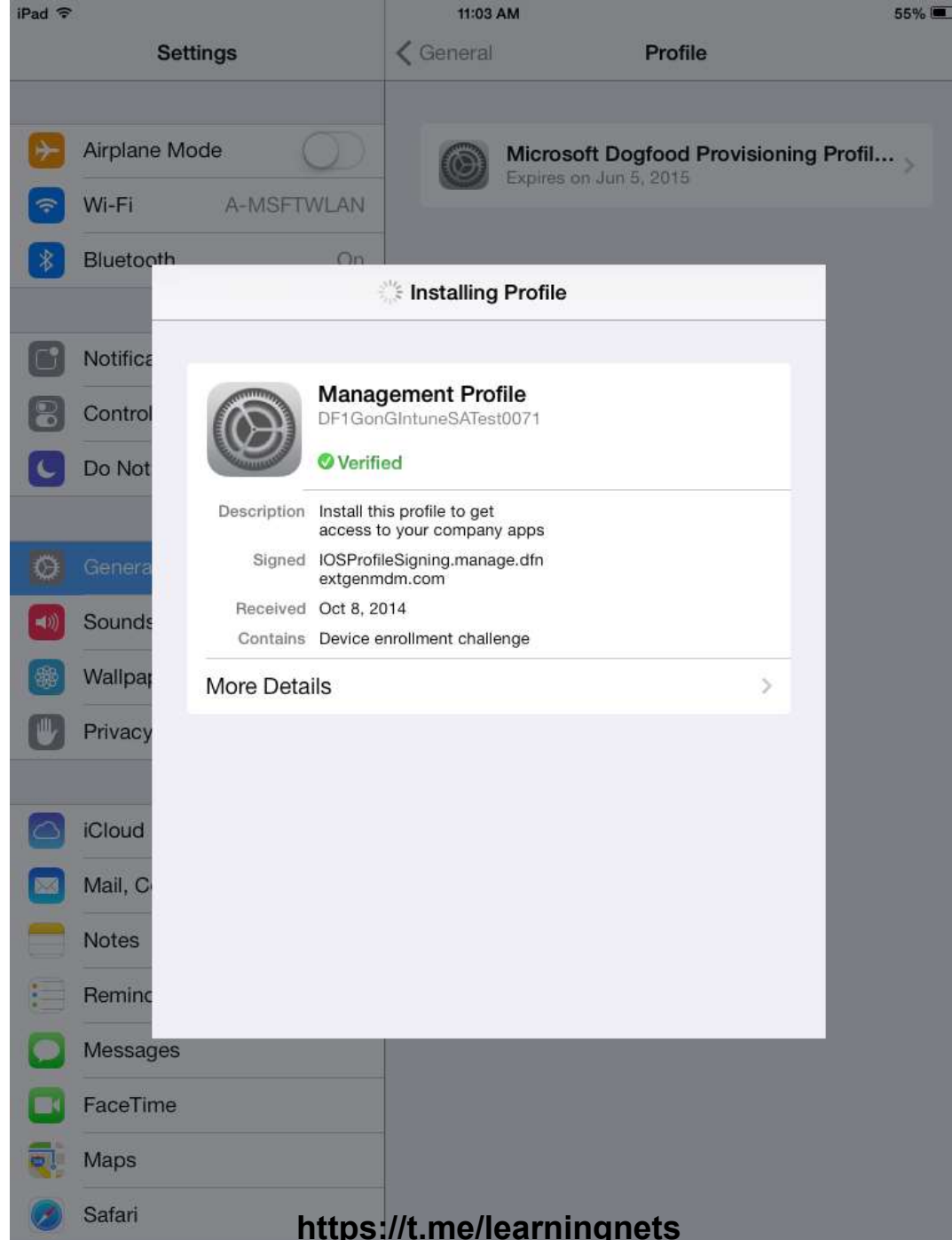
Office apps



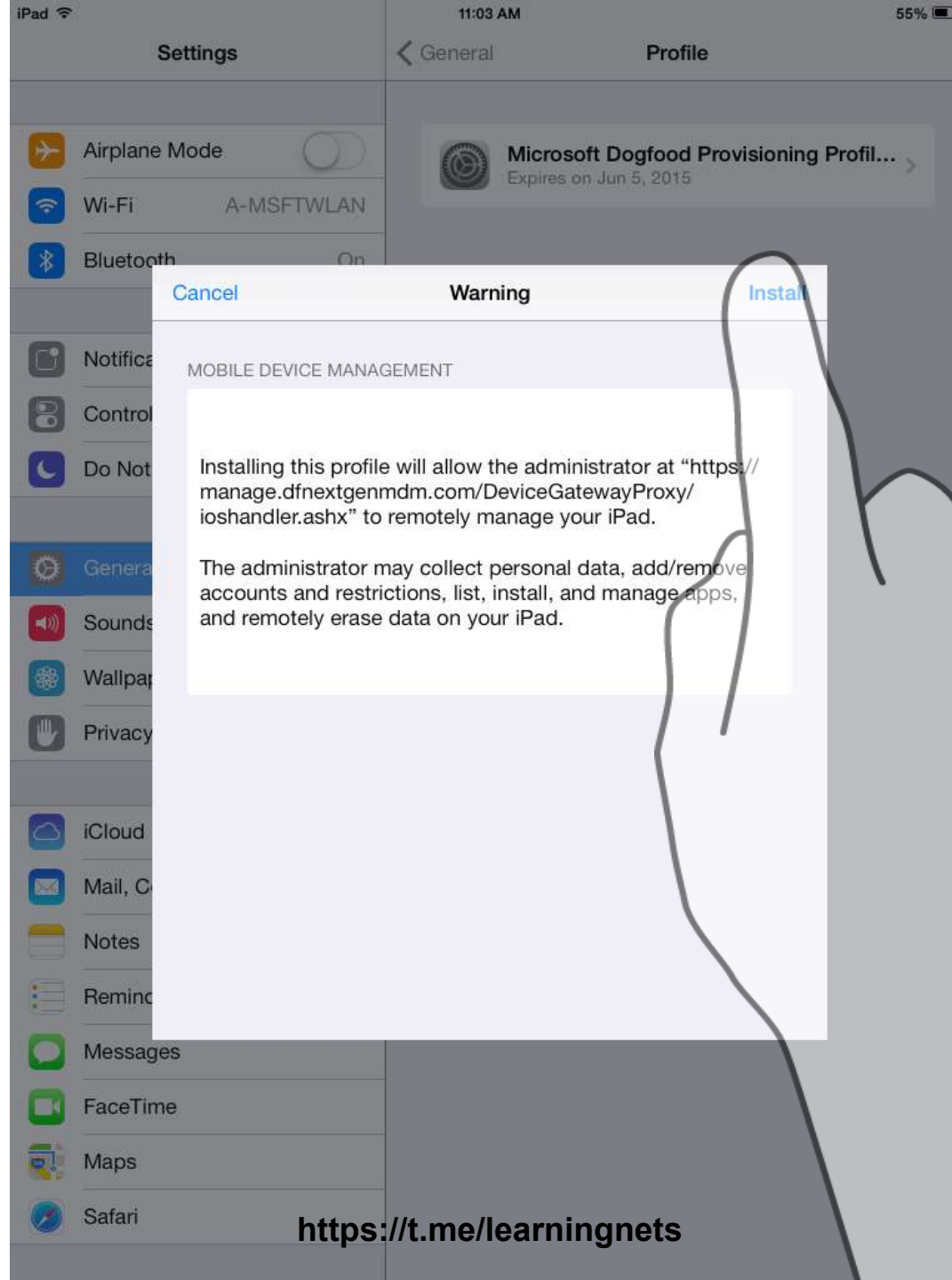
Office apps



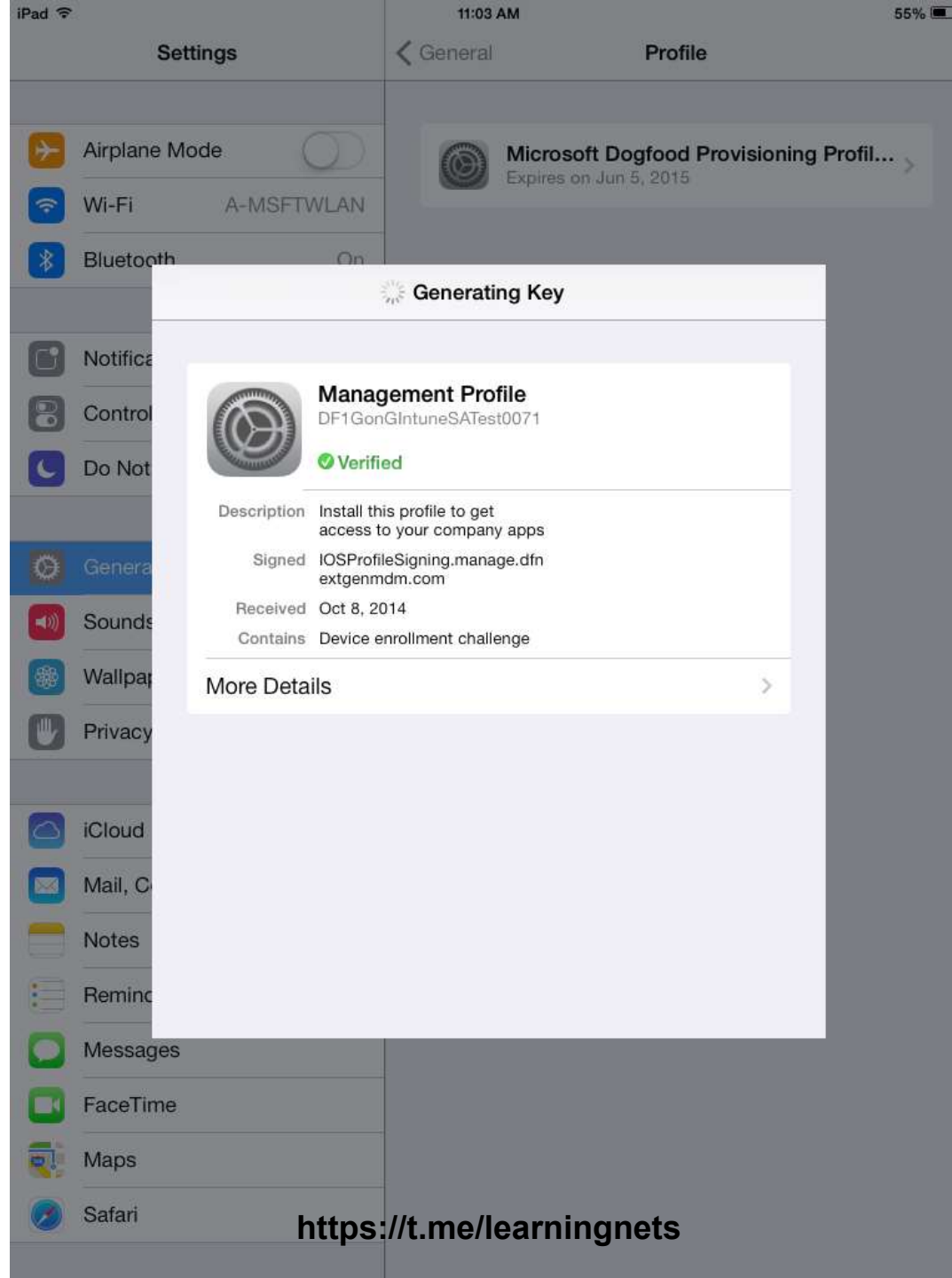
Office apps



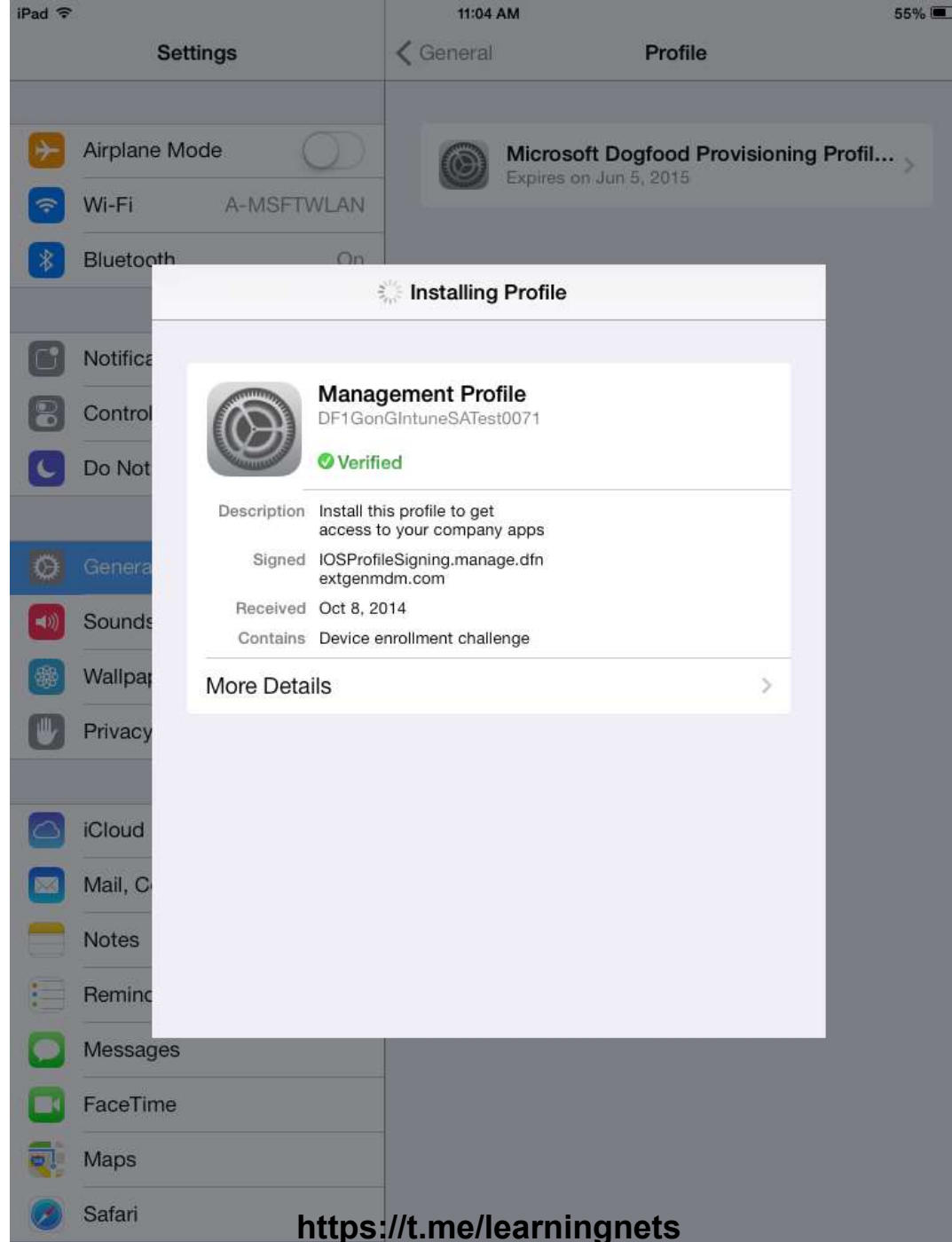
Office apps



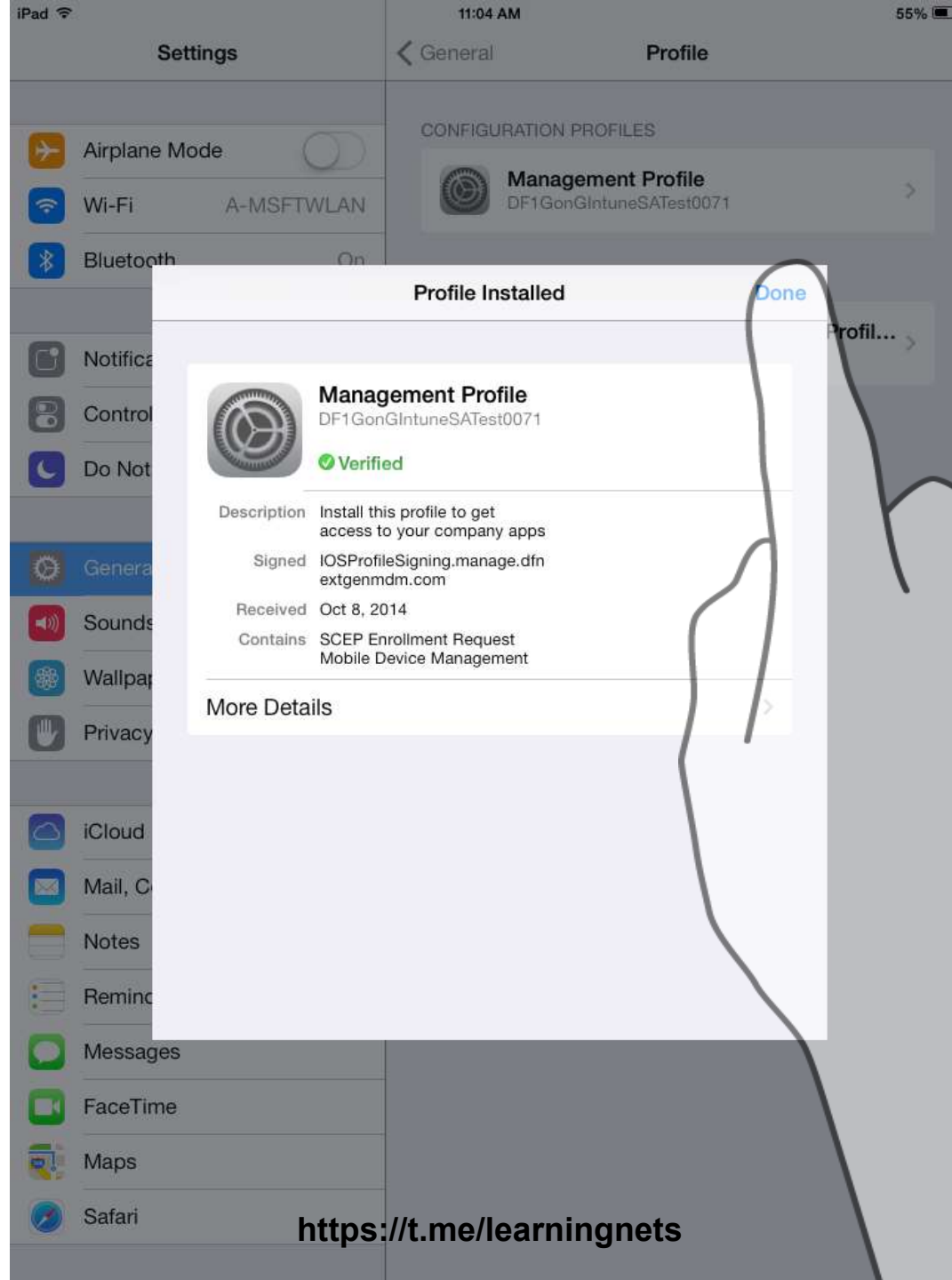
Office apps



Office apps



Office apps



The screenshot shows an iPad interface with an email inbox on the left and a selected email on the right. The top status bar shows 'iPad', signal strength, Wi-Fi, time '12:13 AM', and battery '92%'. The inbox header is 'INBOX 57' with filters 'All Unread To me Flagged'. The selected email is from 'Katie Jordan from Marketir' with subject 'Adobe vision video', dated 'Thu 10/30/2014 12:33 PM'. The email body contains a list of recipients, a 'To' field with 'Marketing Campaigns; Alex Darrow; Sara Davis', and a 'Subject' field with 'Adobe vision video'. The main text of the email says 'this was great' and includes a link to a YouTube video: 'https://www.youtube.com/watch?v=PILR9ANGsOo'. The bottom dock shows the Start button, a search icon, the URL 'https://t.me/learningnets', and other navigation icons.

INBOX 57
All Unread To me Flagged

TWO WEEKS AGO

Katie Jordan
Adobe vision video 10/30/2014
Agreed, things are moving quickly. _____

Katie Jordan
Trip Expenses? 10/30/2014
What is the IO code we should use for t...

[Draft] Katie Jordan
Expense Summary 10/30/2014
2014 Expenses.xlsx Shared via OneDrive...

Katie Jordan
Sharing the latest 10/30/2014
Sara/Alex- Attached is the latest versio...

Katie Jordan
Who is covering for Garth? 10/30/2014
Sara- Any ideas? I have an urgent invo...

Sara Davis
Customer data 10/29/2014
Here you go (attached).

Katie Jordan
Tracking info 10/28/2014
Tracking information: Ship Carrier: FedE...

Alex Darrow
Support org changes 10/28/2014
Hi Sara, I'd love to chat with you some...

Garth Fort
Review meeting 10/28/2014
Can you set up a review meeting with B...

Garth Fort
Lunch today? 10/28/2014
How does your schedule look? Would L...

Adobe vision video

Katie Jordan from Marketir
Thu 10/30/2014 12:33 PM

3 recipients

To: Marketing Campaigns; Alex Darrow; Sara Davis;
Agreed, things are moving quickly.

From: Marketing Campaigns on behalf of Sara Davis
Sent: Tuesday, October 28, 2014 7:57:38 AM
To: Marketing Campaigns; Alex Darrow
Subject: Adobe vision video

this was great

From: Alex Darrow
Sent: Thursday, October 9, 2014 12:56:11 PM
To: Marketing Campaigns; Marketing Campaigns
Subject: Adobe vision video

Totally unrelated to what we are doing, but pretty cool i think.

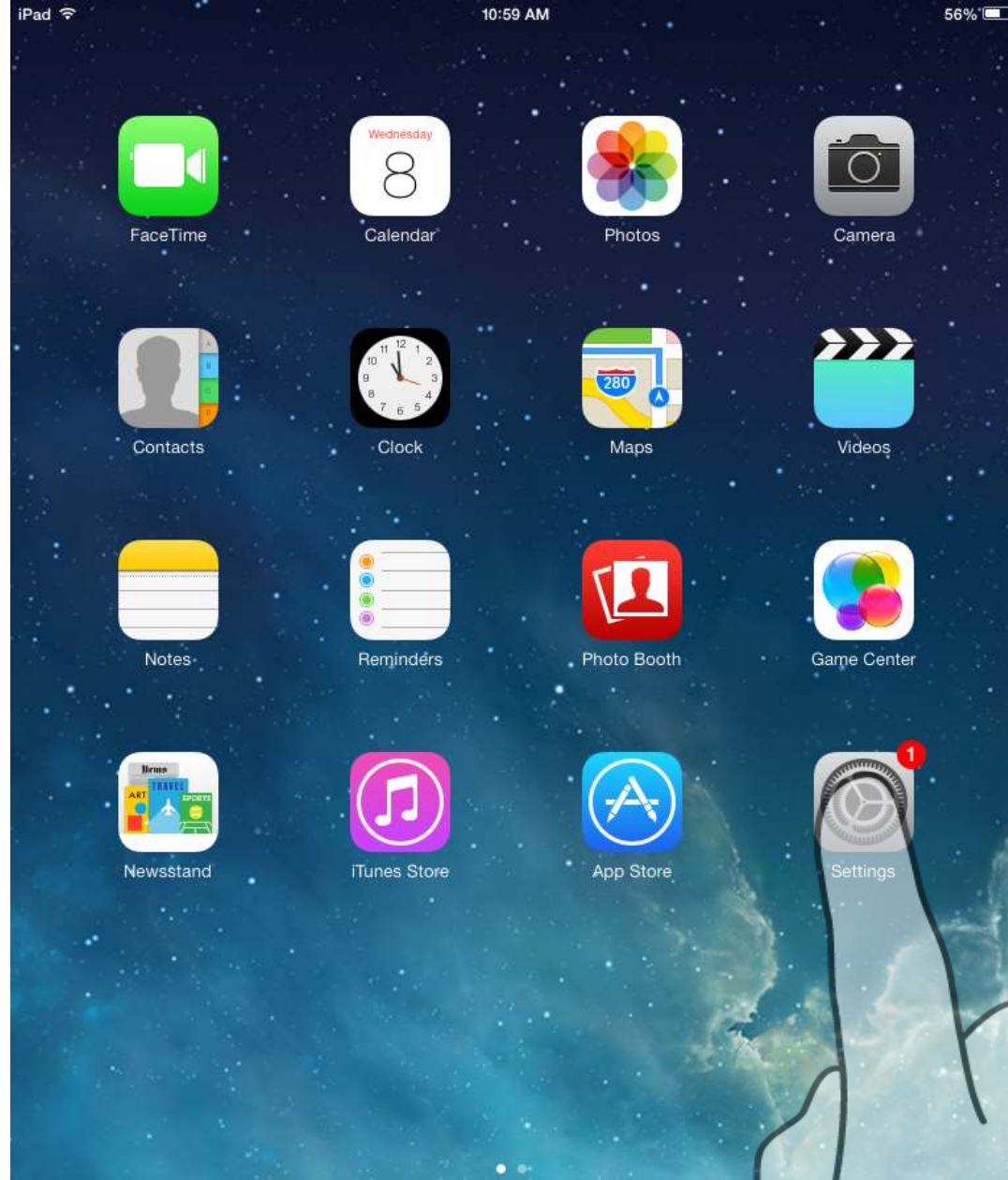
<https://www.youtube.com/watch?v=PILR9ANGsOo>

<https://t.me/learningnets>

Enrolling in Office 365 MDM

Download & sign into Office applications

Connect to email via Built-In Email App



FaceTime



Calendar



Photos



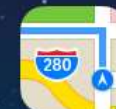
Camera



Contacts



Clock



Maps



Videos



Notes



Reminders



Photo Booth



Game Center



Newsstand



iTunes Store



App Store



Settings



Messages



Mail



Safari

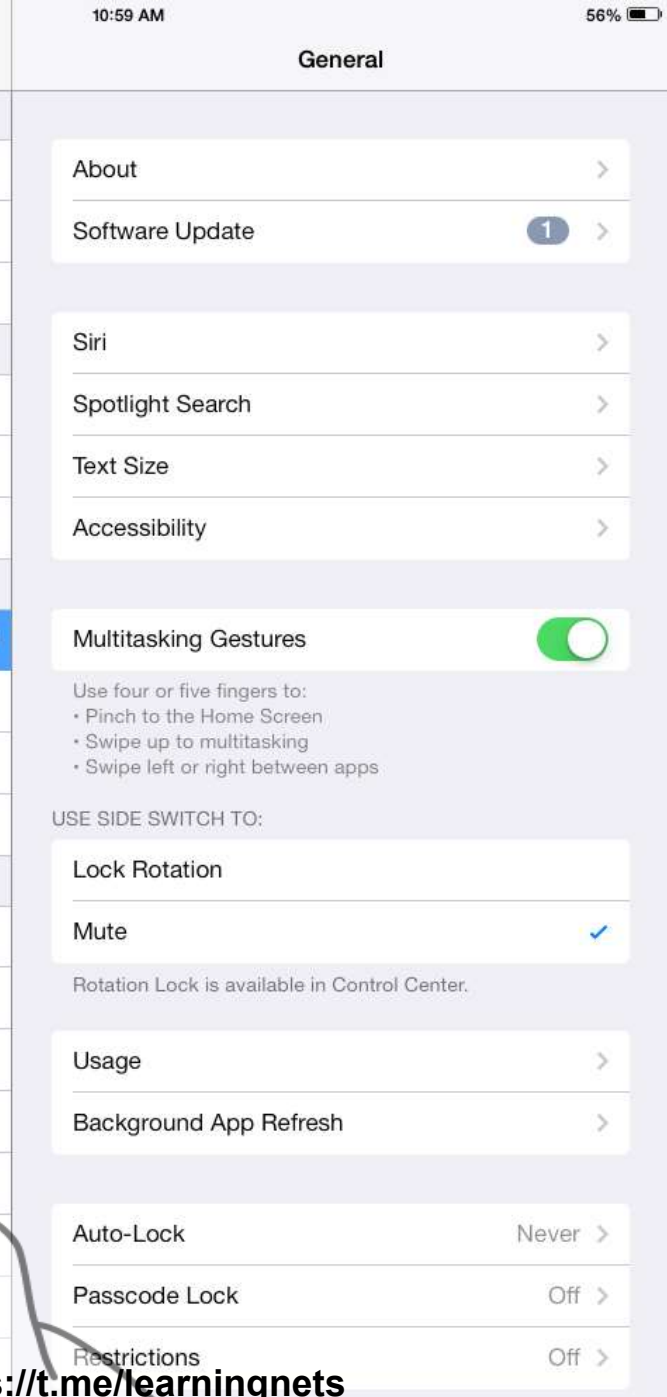
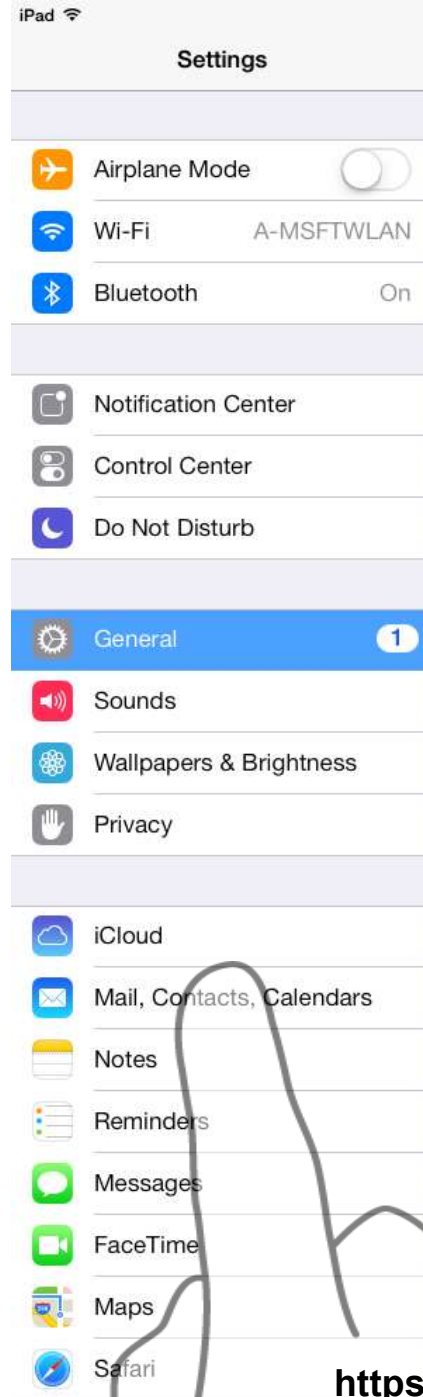


Music

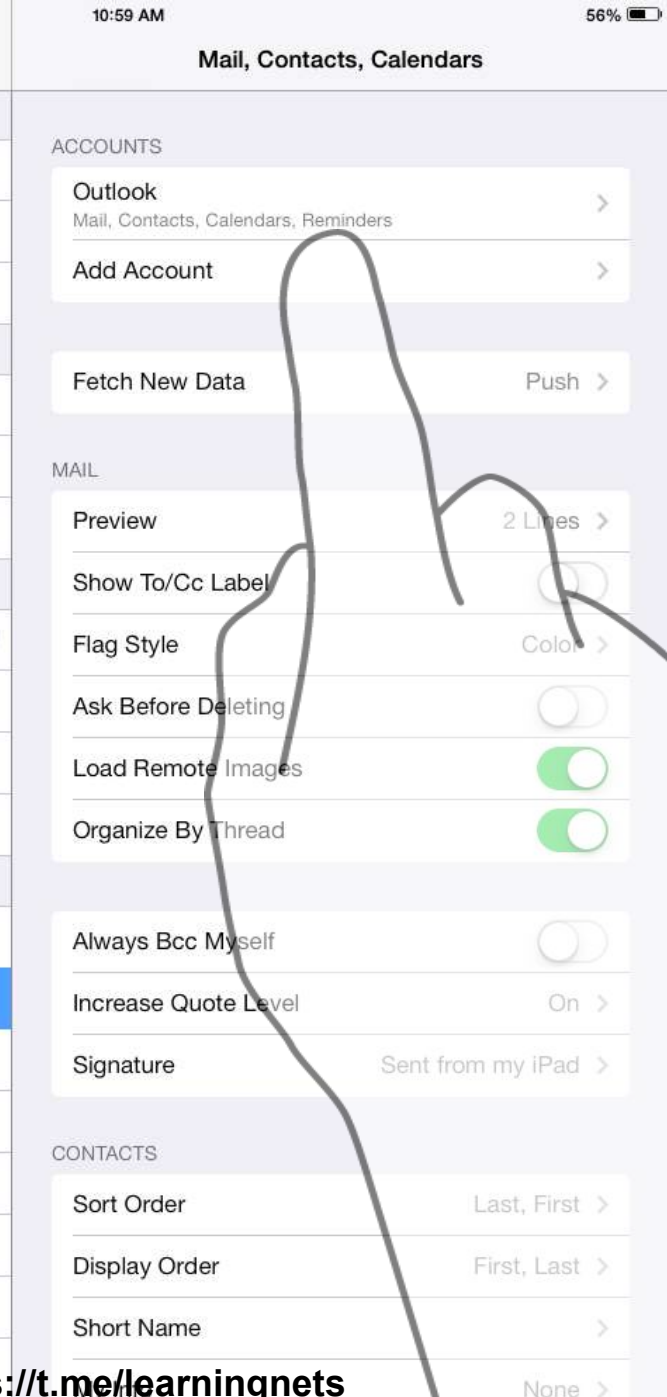
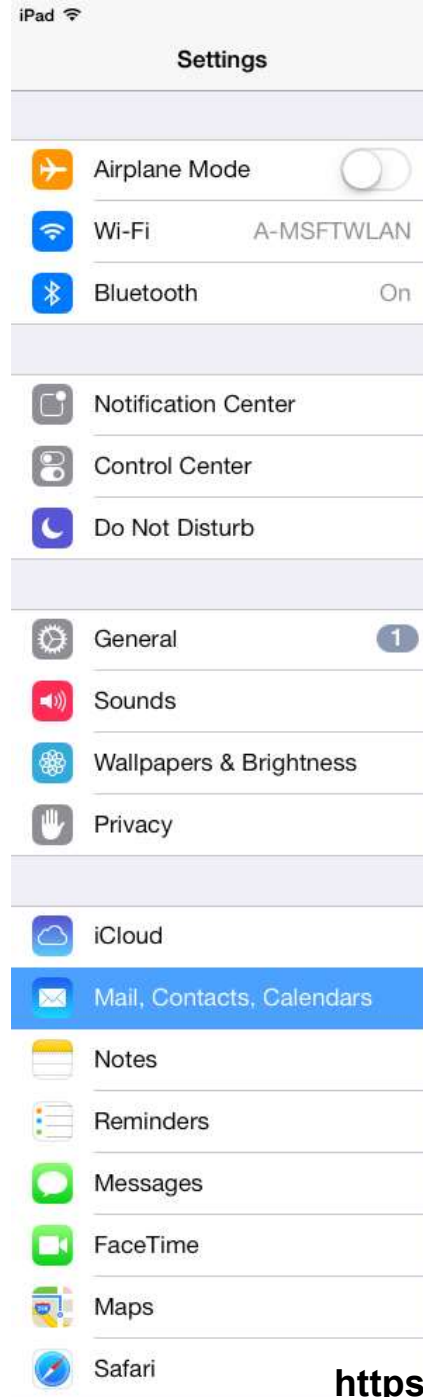
<https://t.me/learningnets>



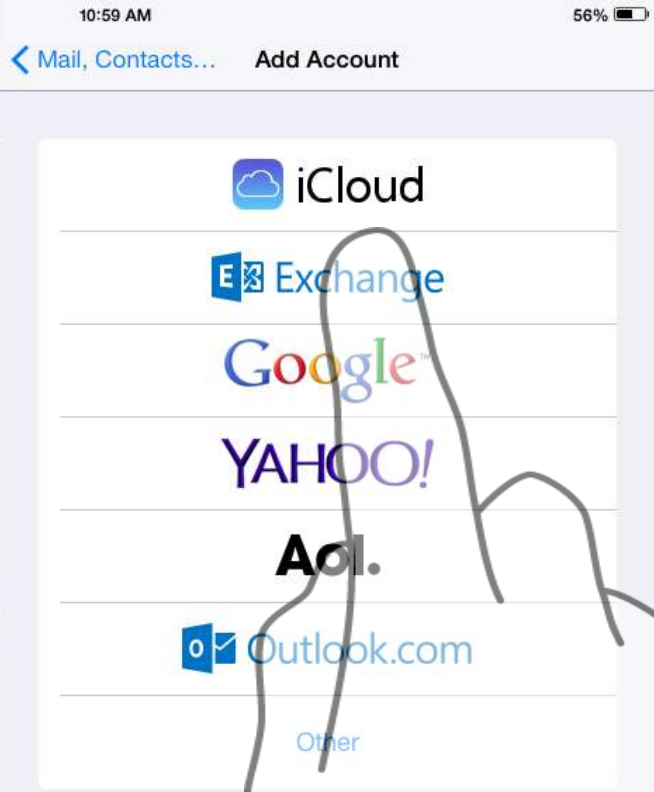
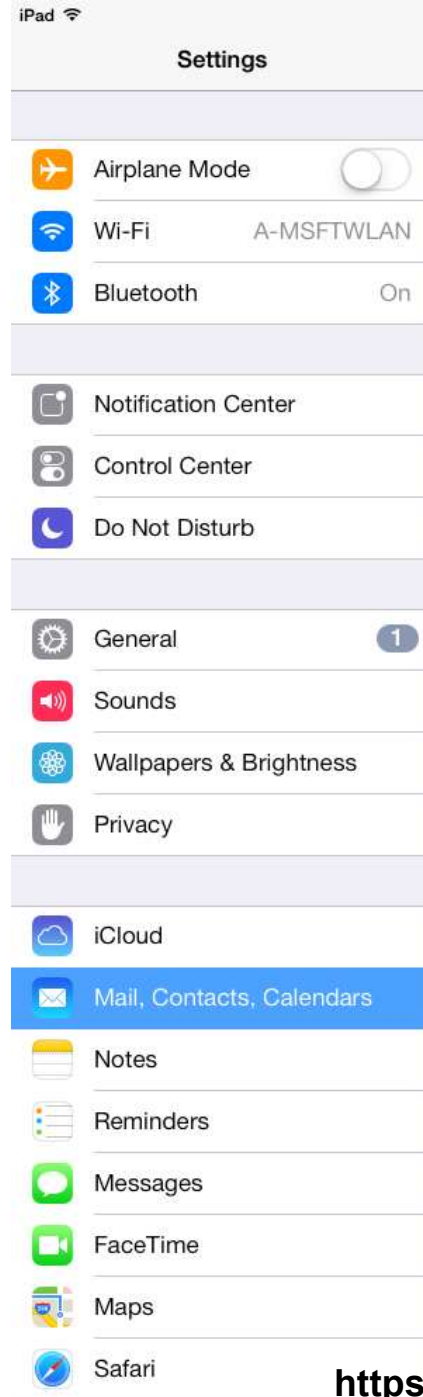
EAS



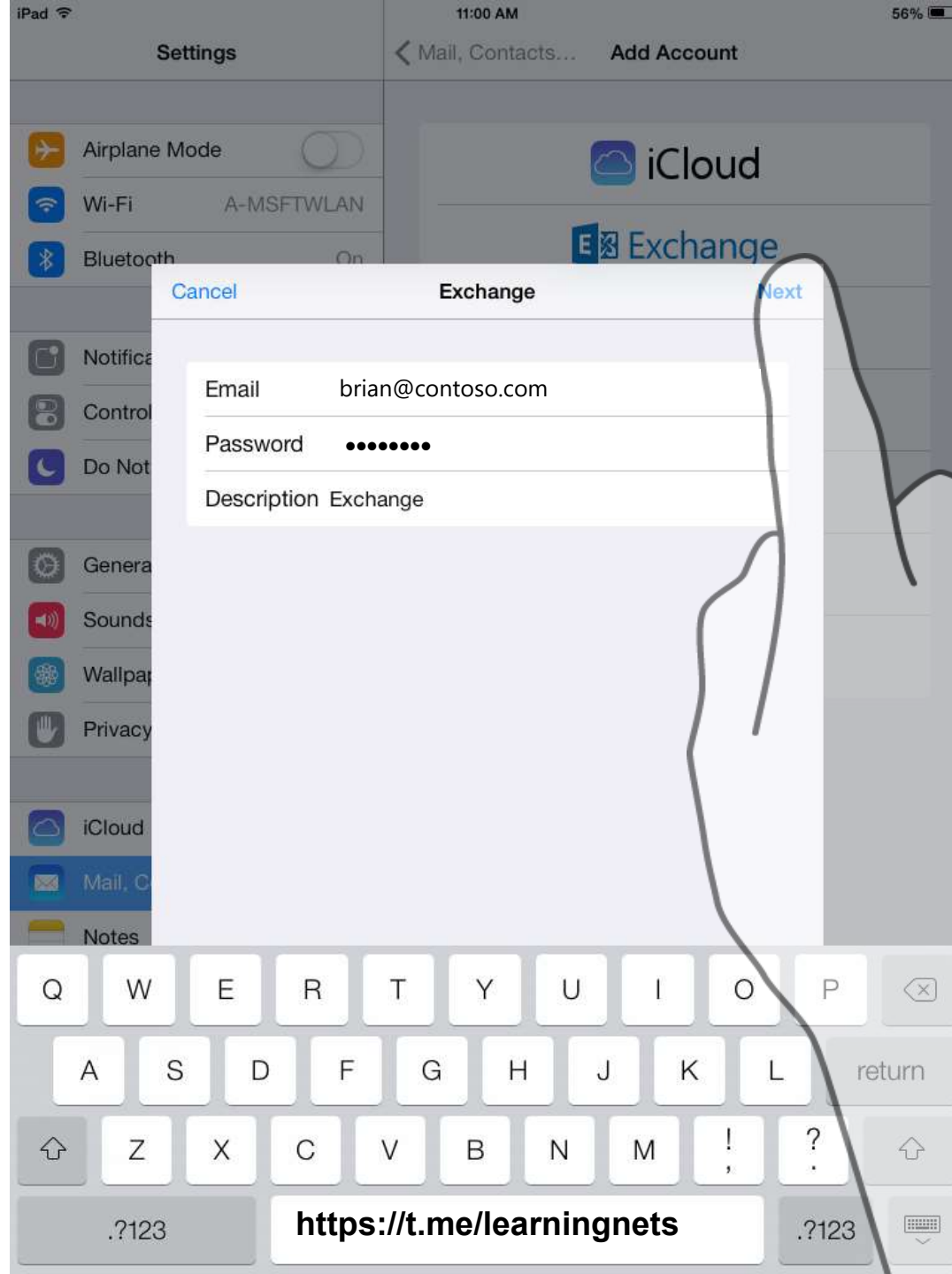
<https://t.me/learningnets>

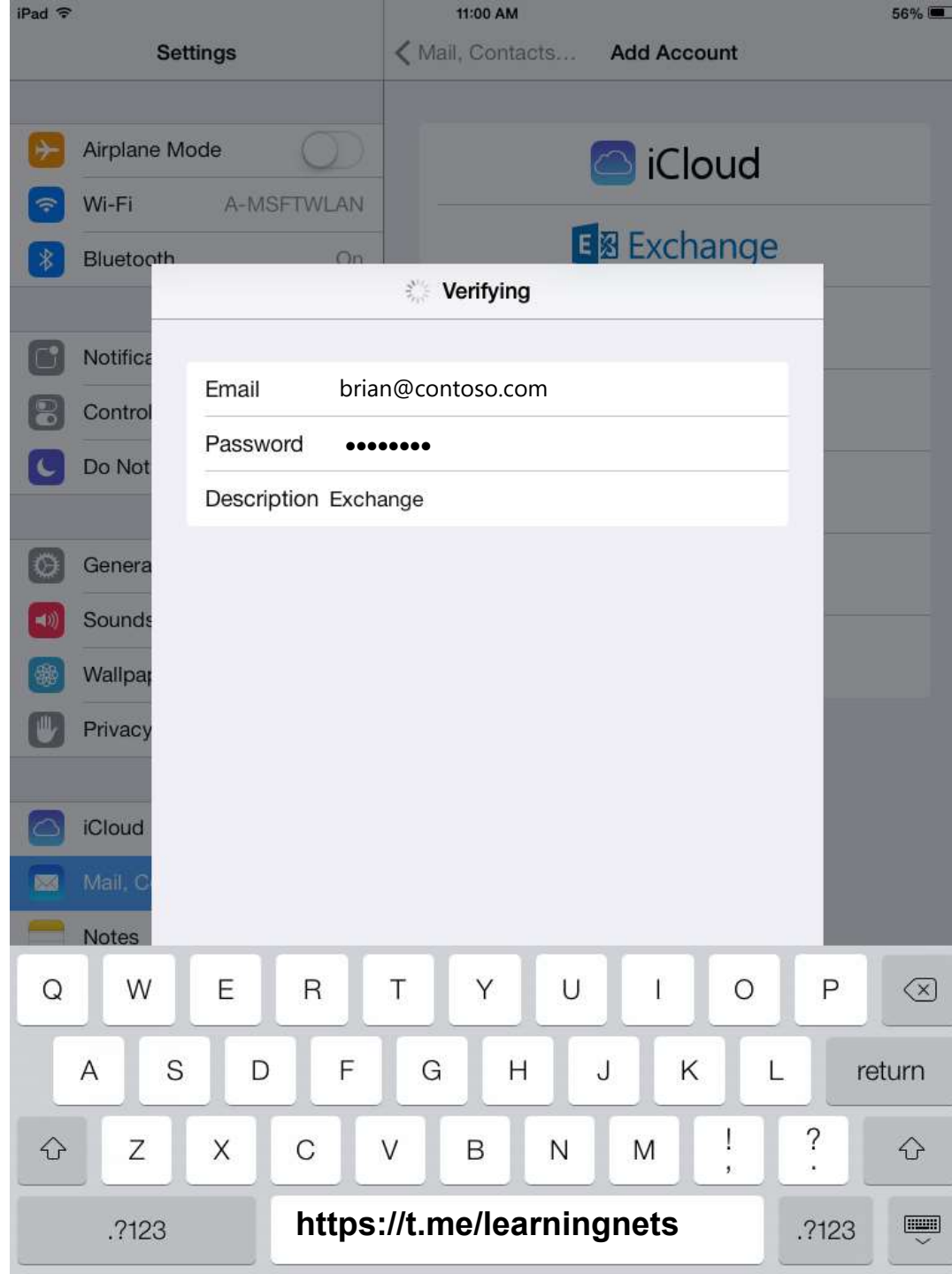


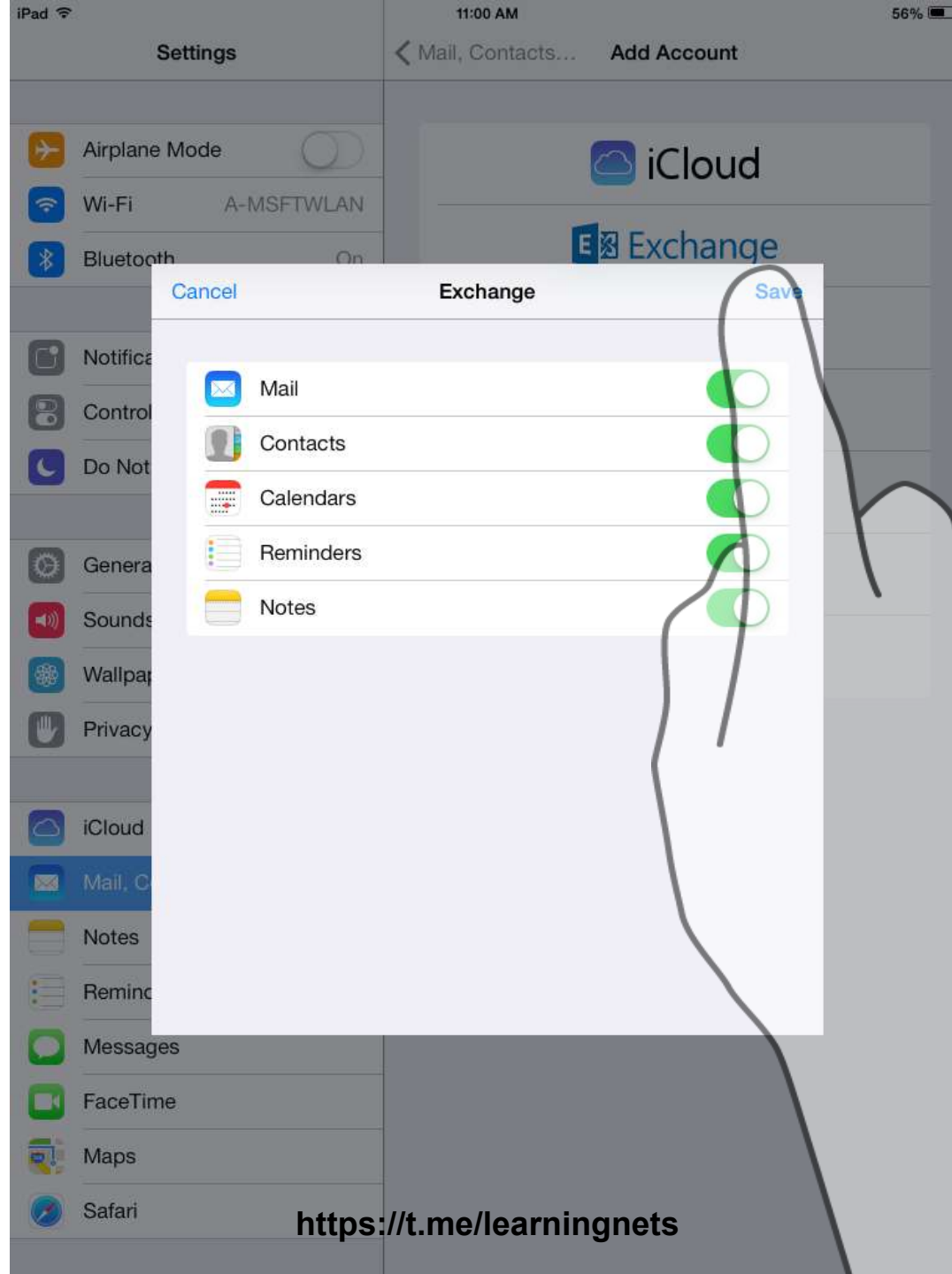
<https://t.me/learningnets>

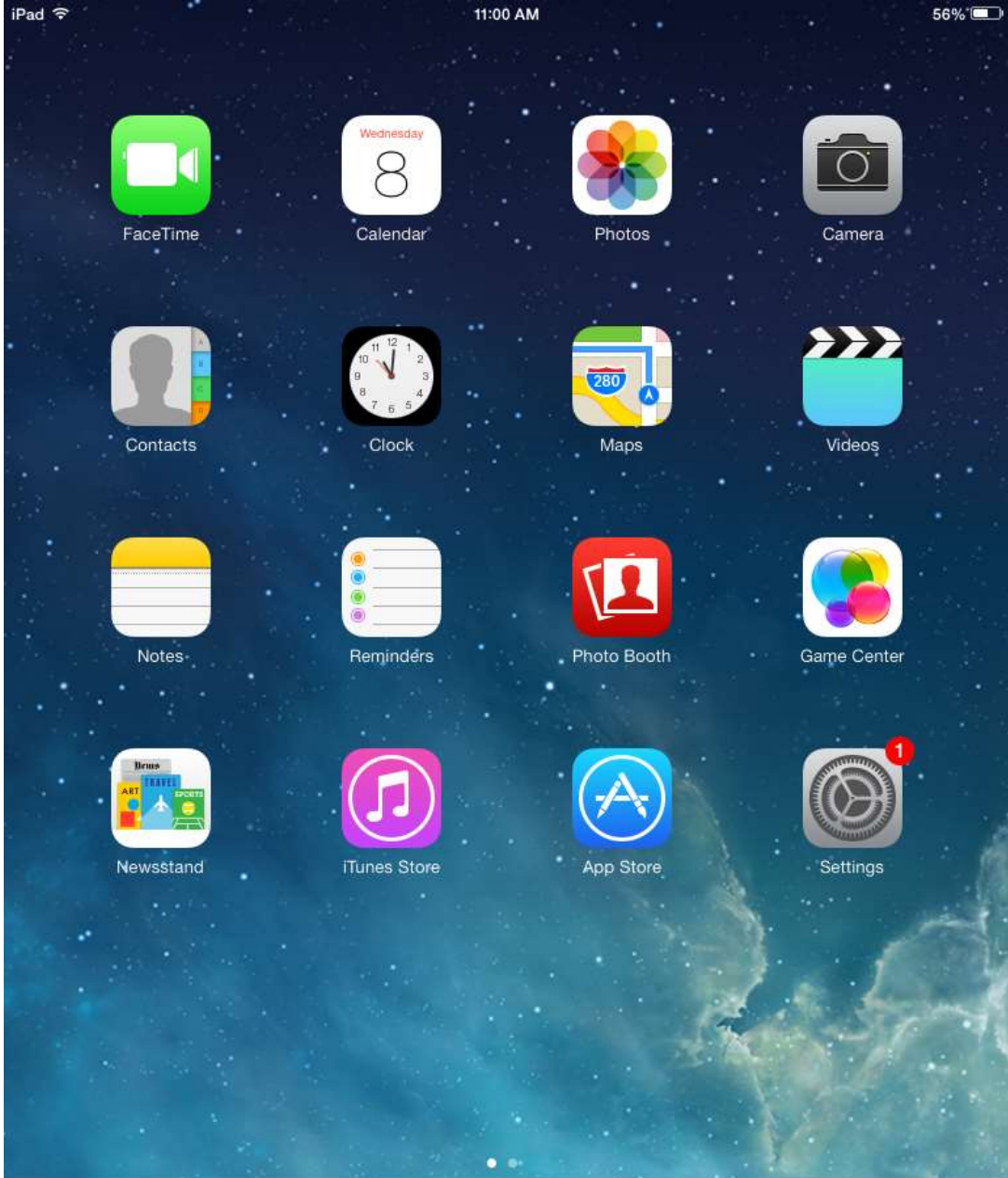


<https://t.me/learningnets>





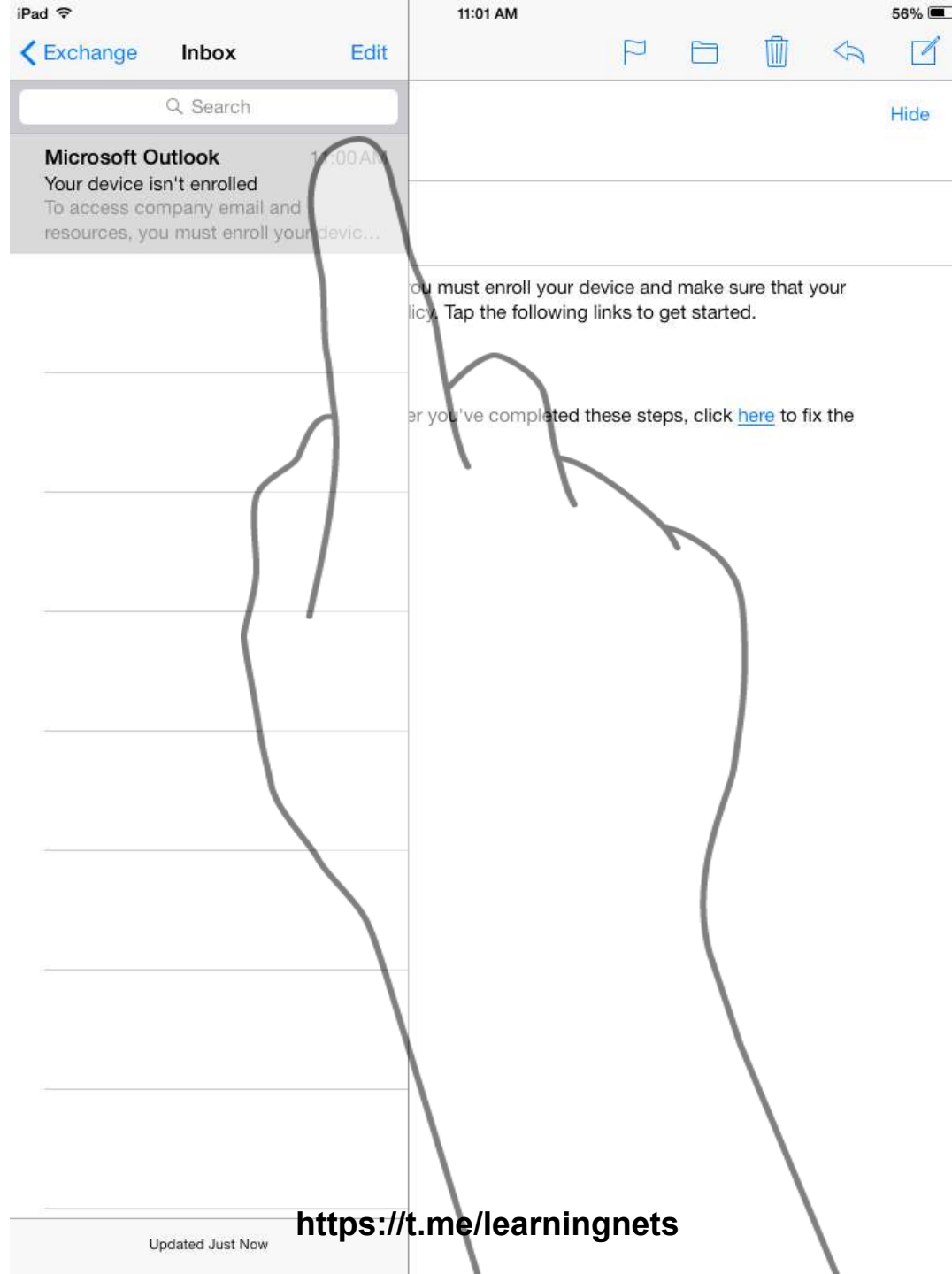




EAS



<https://t.me/learningnets>



From: [Microsoft Outlook](#) >

Hide

To: [IW User 3](#) >

Your device isn't enrolled

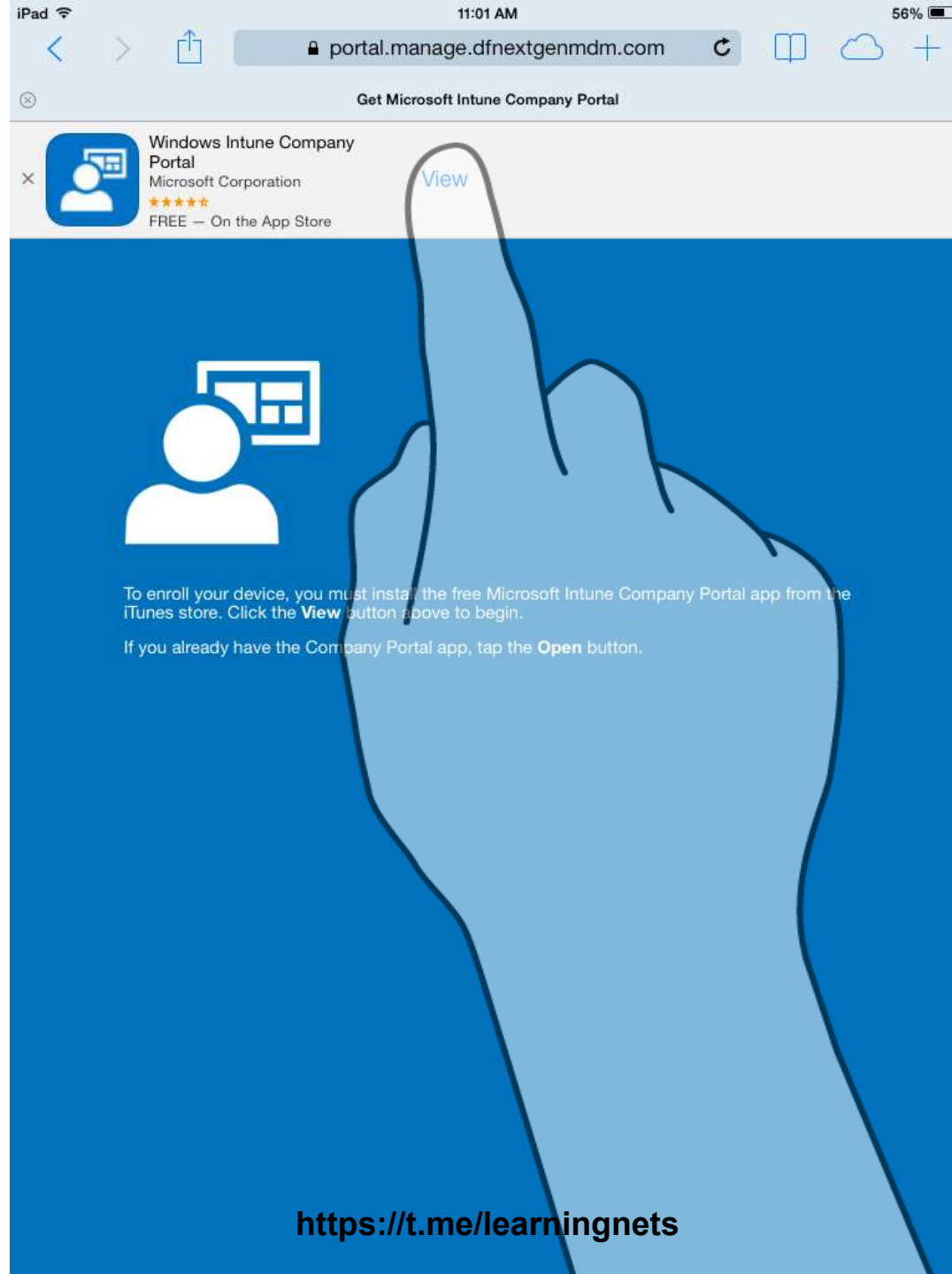
October 8, 2014 at 11:00 AM

To access company email and resources, you must enroll your device and make sure that your device complies with company security policy. Tap the following links to get started.

1. [Enroll device](#)
2. [Check device compliance status](#)

If you can't access email a few minutes after you've completed these steps, click [here](#) to fix the problem.








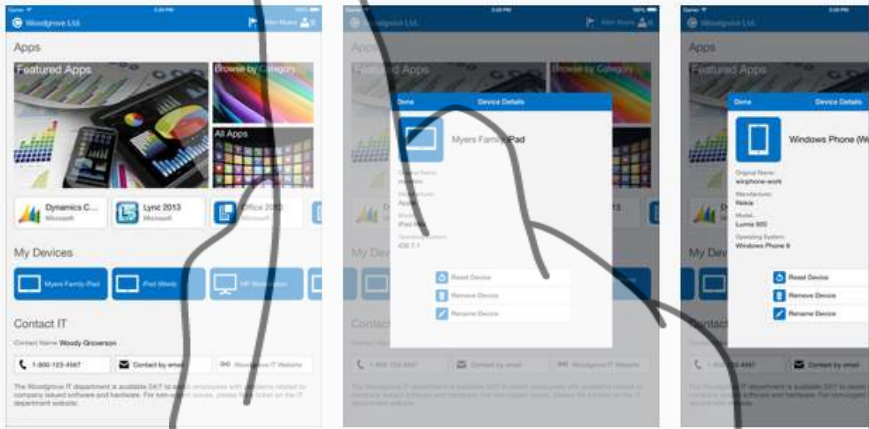
EAS

Windows Intune Company Portal
Microsoft Corporation >
★★★★☆



[OPEN](#)

[Details](#) [Reviews](#) [Related](#)



Description
The Company Portal app helps you search, browse and install apps made available to you by your organization through the Windows Intune online service. Apps can be installed without requiring a connection to your

<https://t.me/learningnets>



Apps

New Apps | Browse by Category

Cancel **Device Enrollment** Enroll

Enrolling this device will give you access to email and other company resources and gives your organization the ability to manage this device.

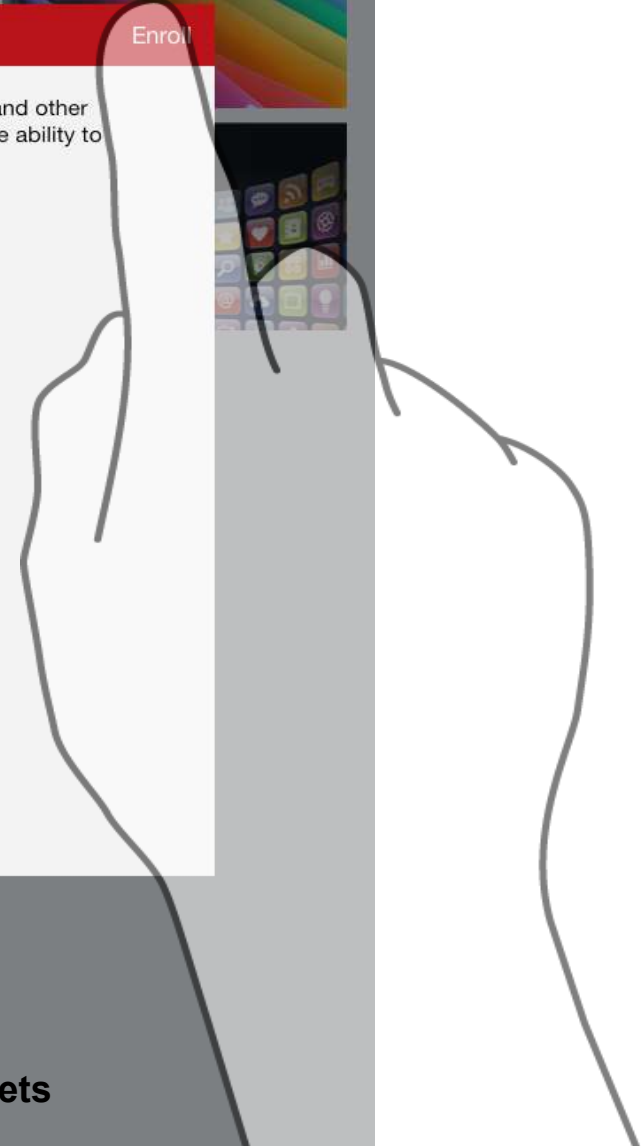
[More information about enrolling you device](#)

My Dev



Contact

Contact Nam



Apps

Featured Apps



Reader
Adobe

My Devices



Brandon's iPad Air

Enroll your device



For added security, we need to verify your account. We have sent a text message with the verification code.



Brian Shiers
(xxx) xxx-xx12

Please enter the code to continue

[Other security verification options](#)

[Sign in with another account](#)

Sign in

Cancel



Apps

Featured Apps



Reader
Adobe

My Devices



Brandon's iPad Air

Enroll your device



Contoso
Corporation

For added security, we need to verify your account. We have sent a text message with the verification code.



Brian Shiers
(xxx) xxx-xx12

Please enter the code to continue

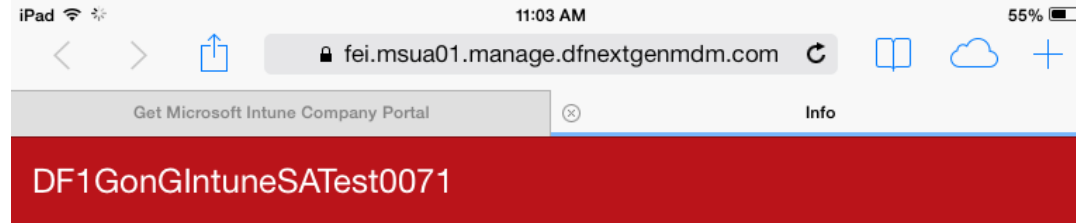
[Other security verification options](#)

[Sign in with another account](#)

Sign in

Cancel

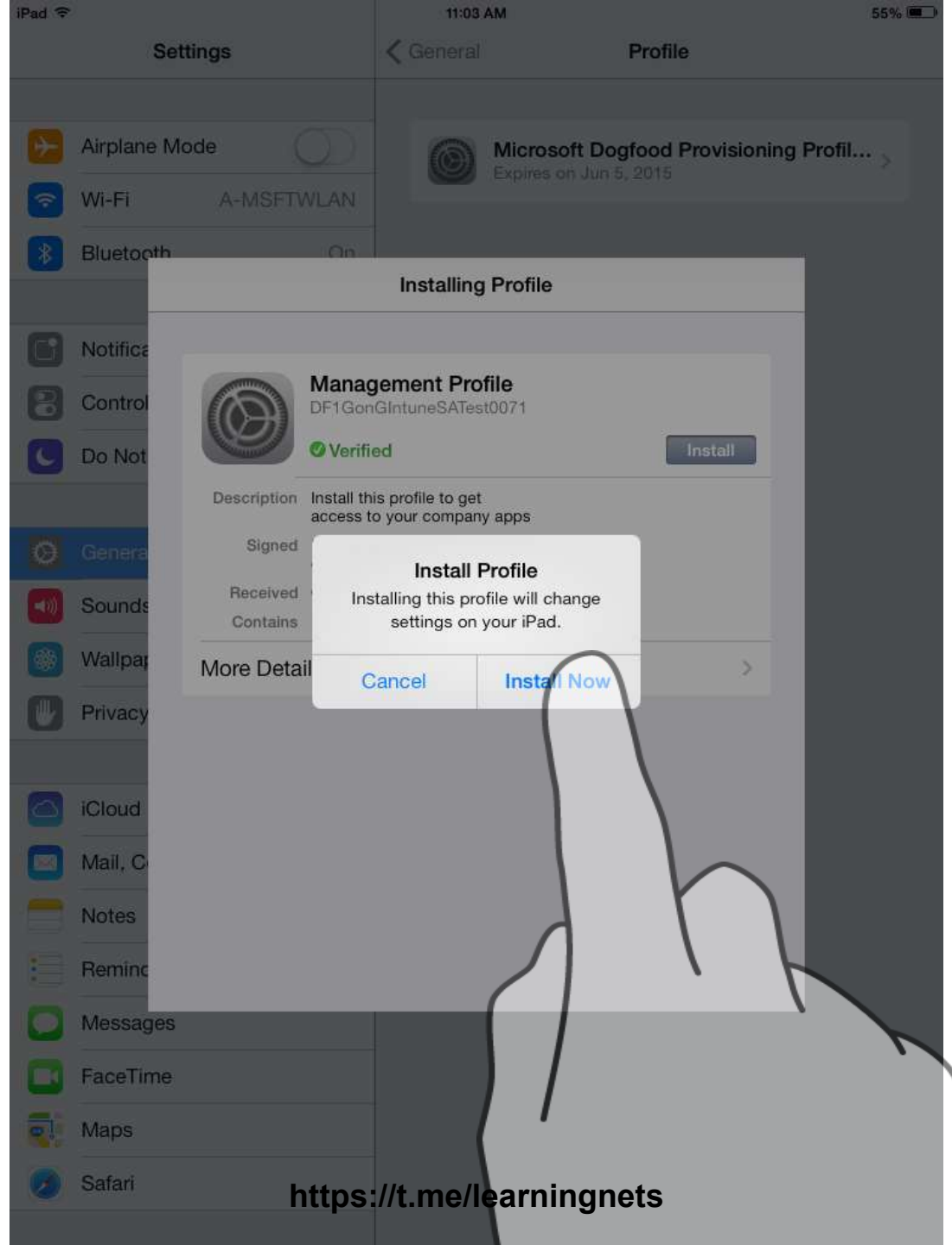


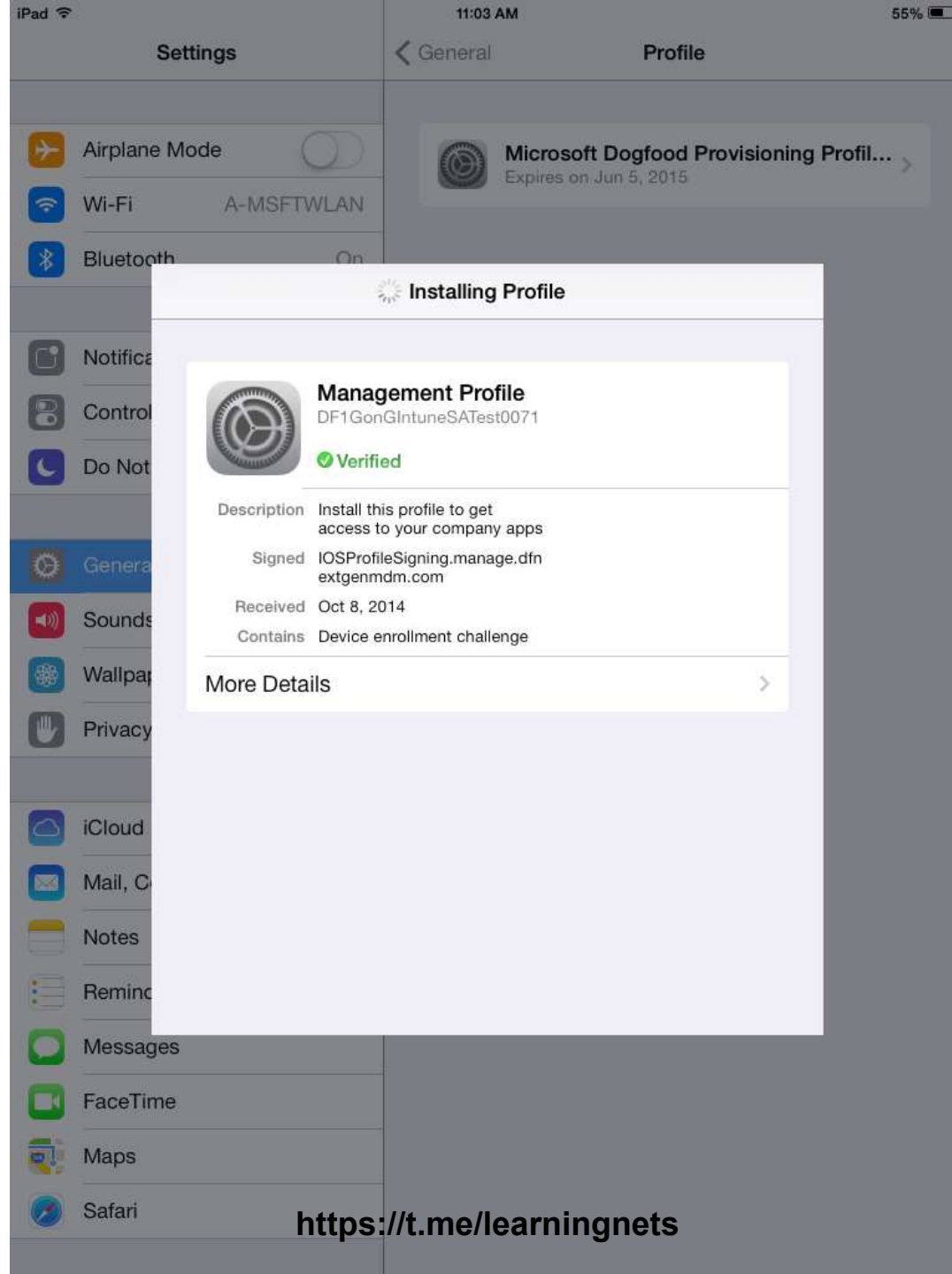


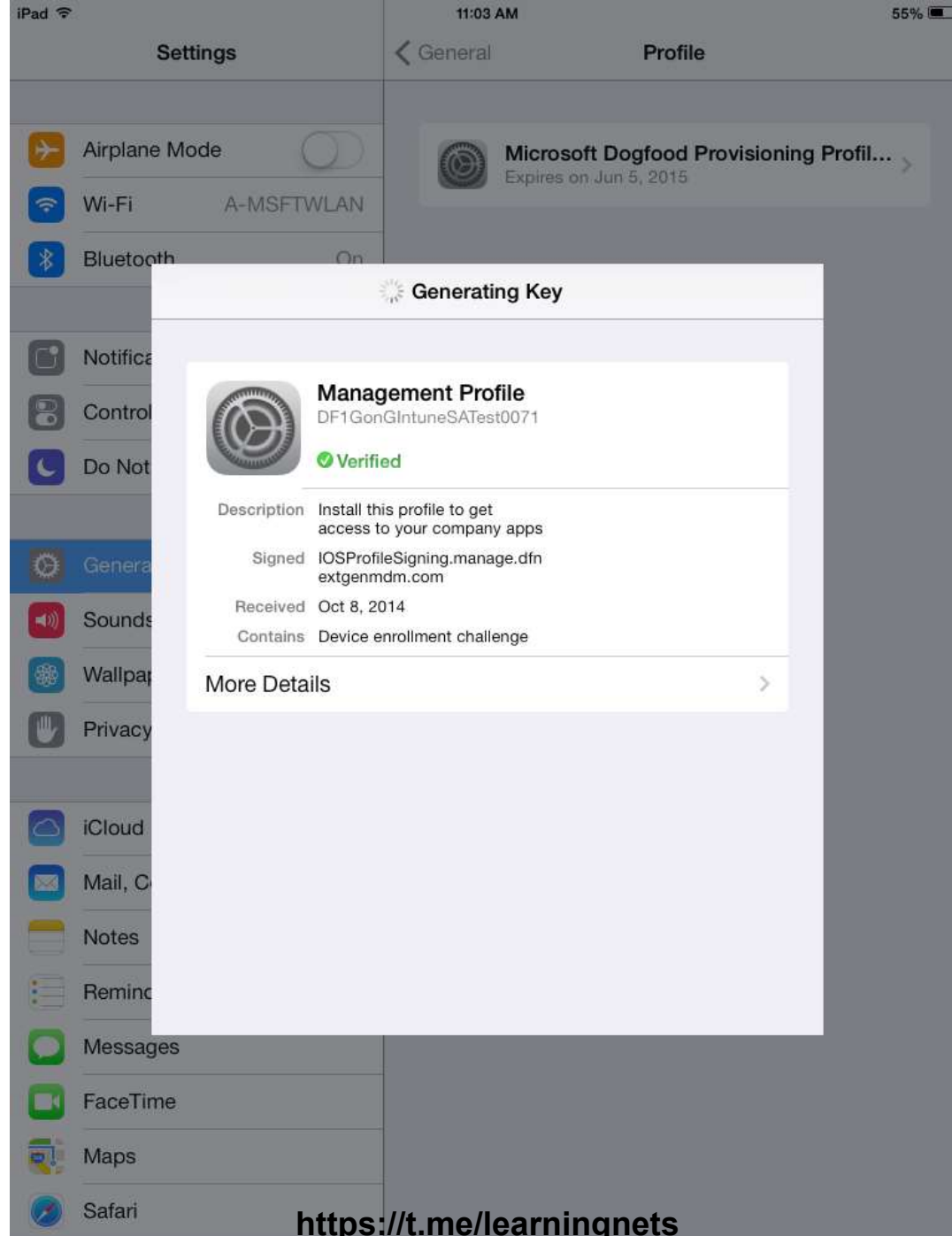
Adding Device...

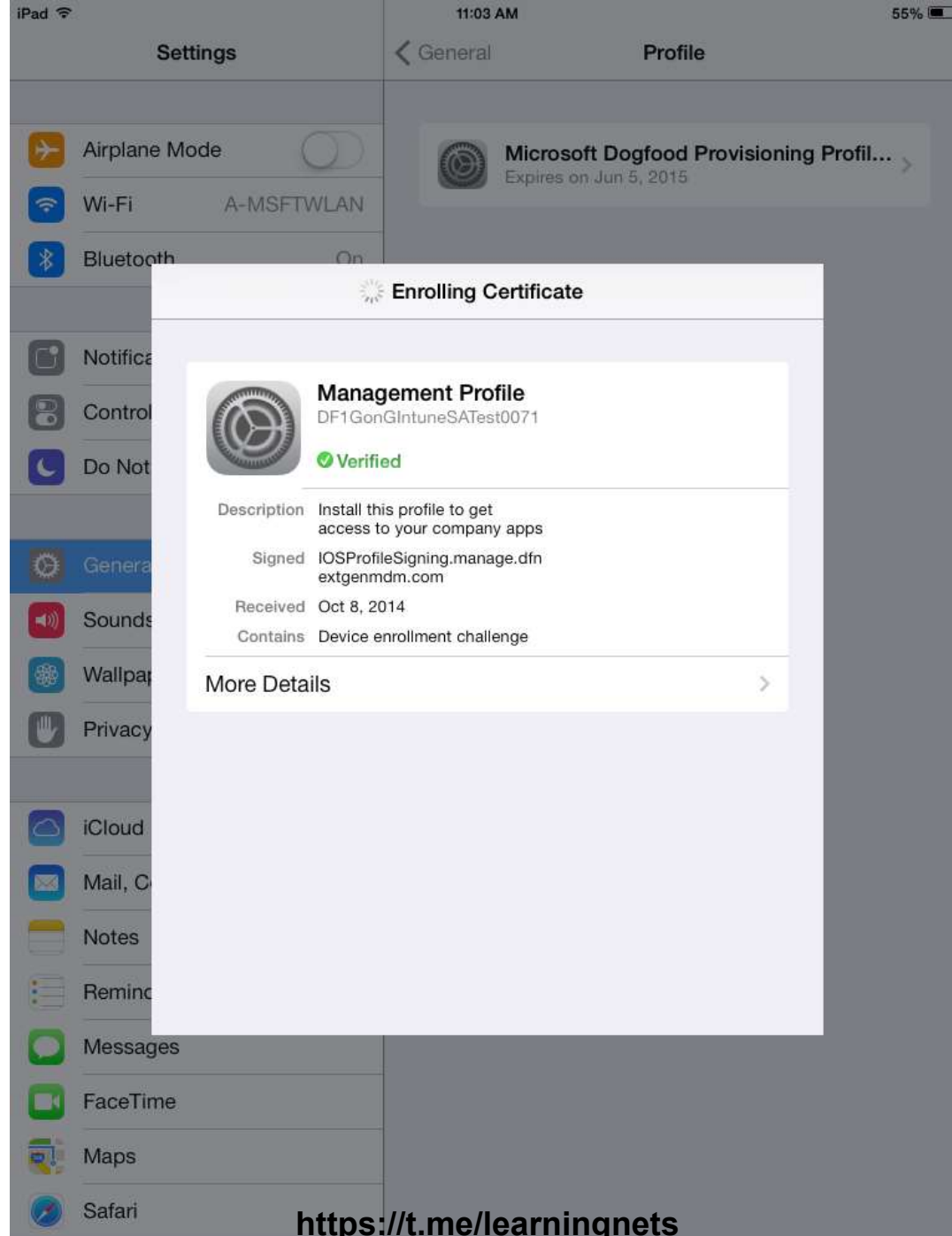
<https://timelearningnets>

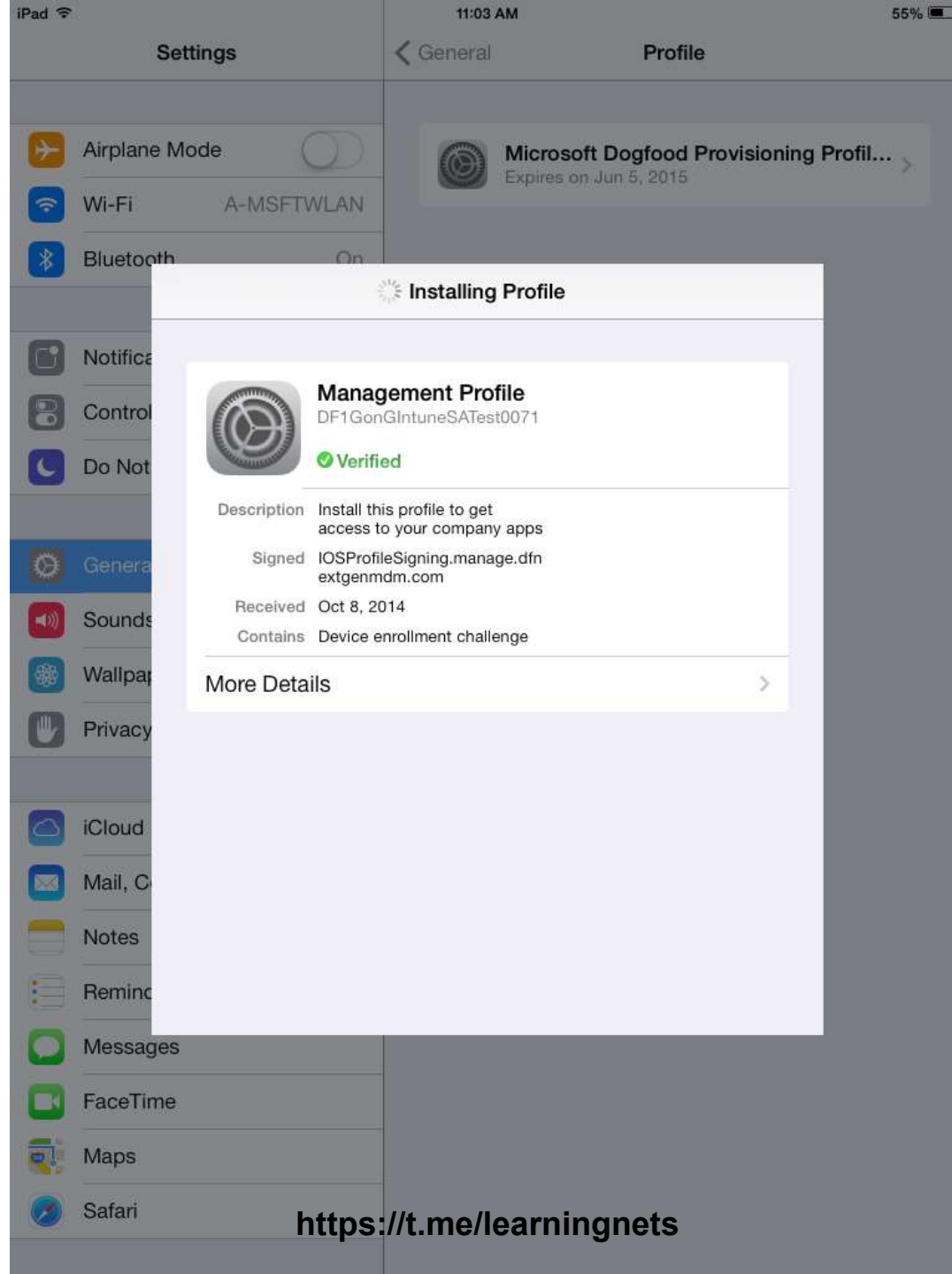


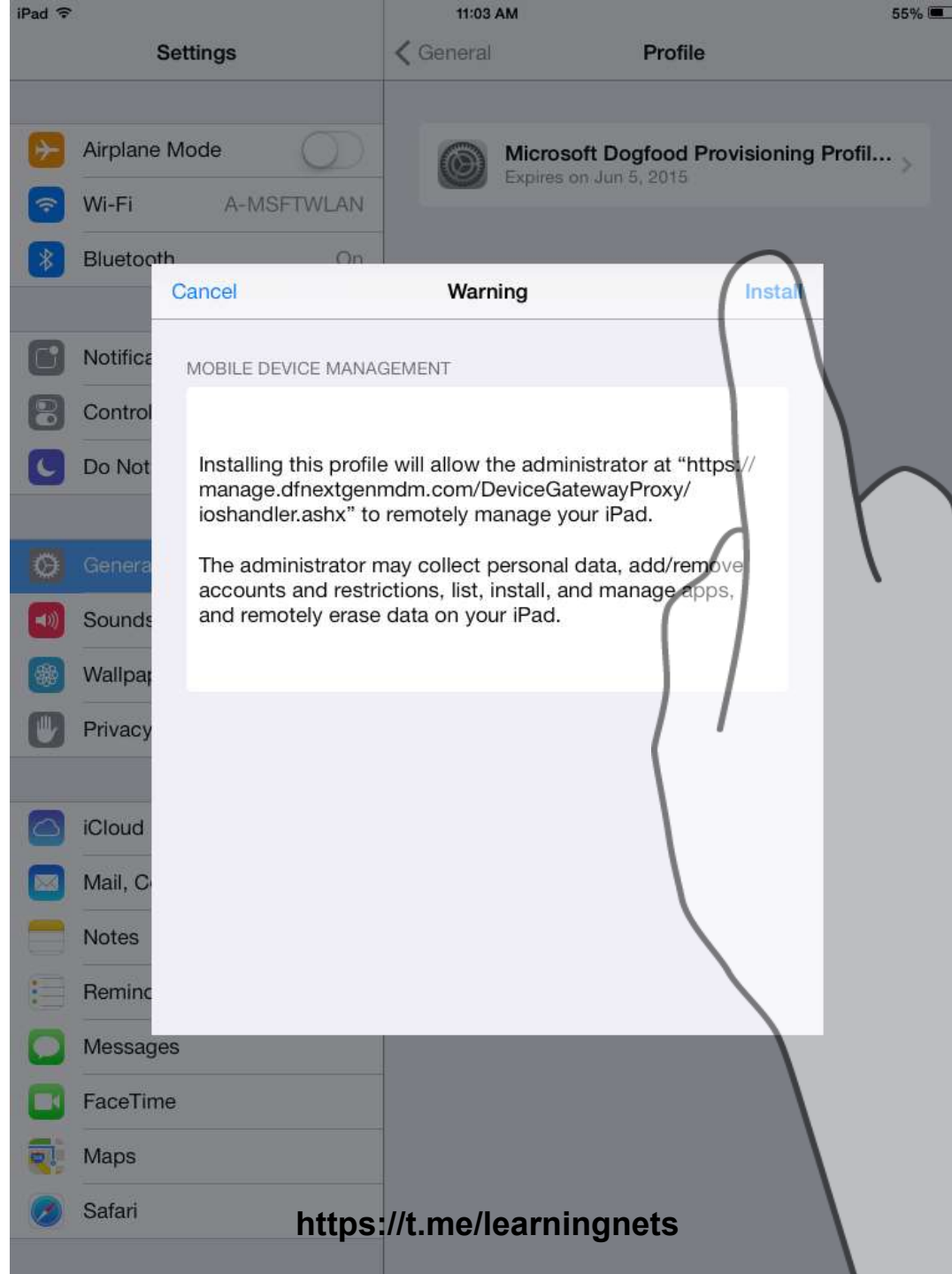


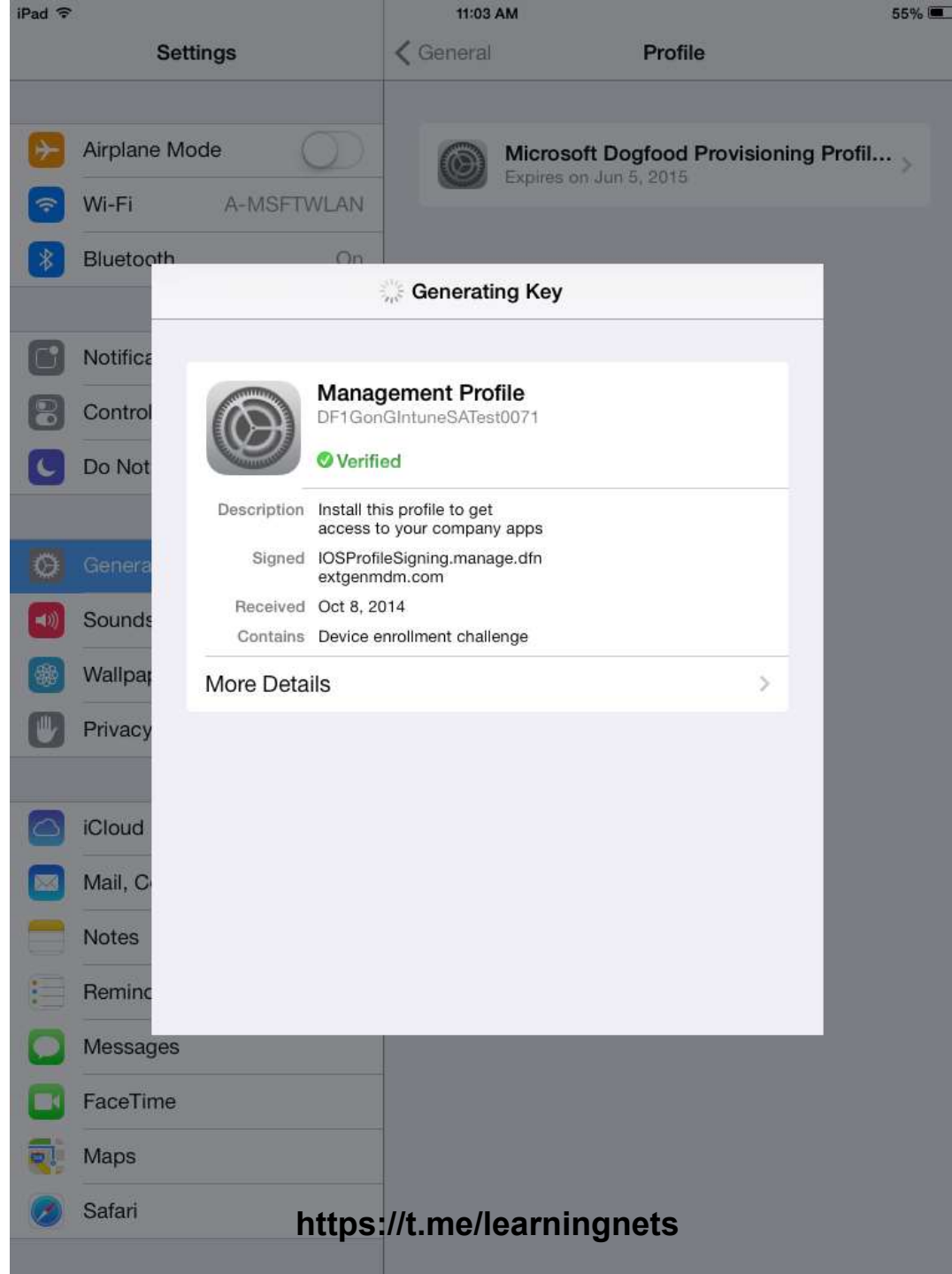


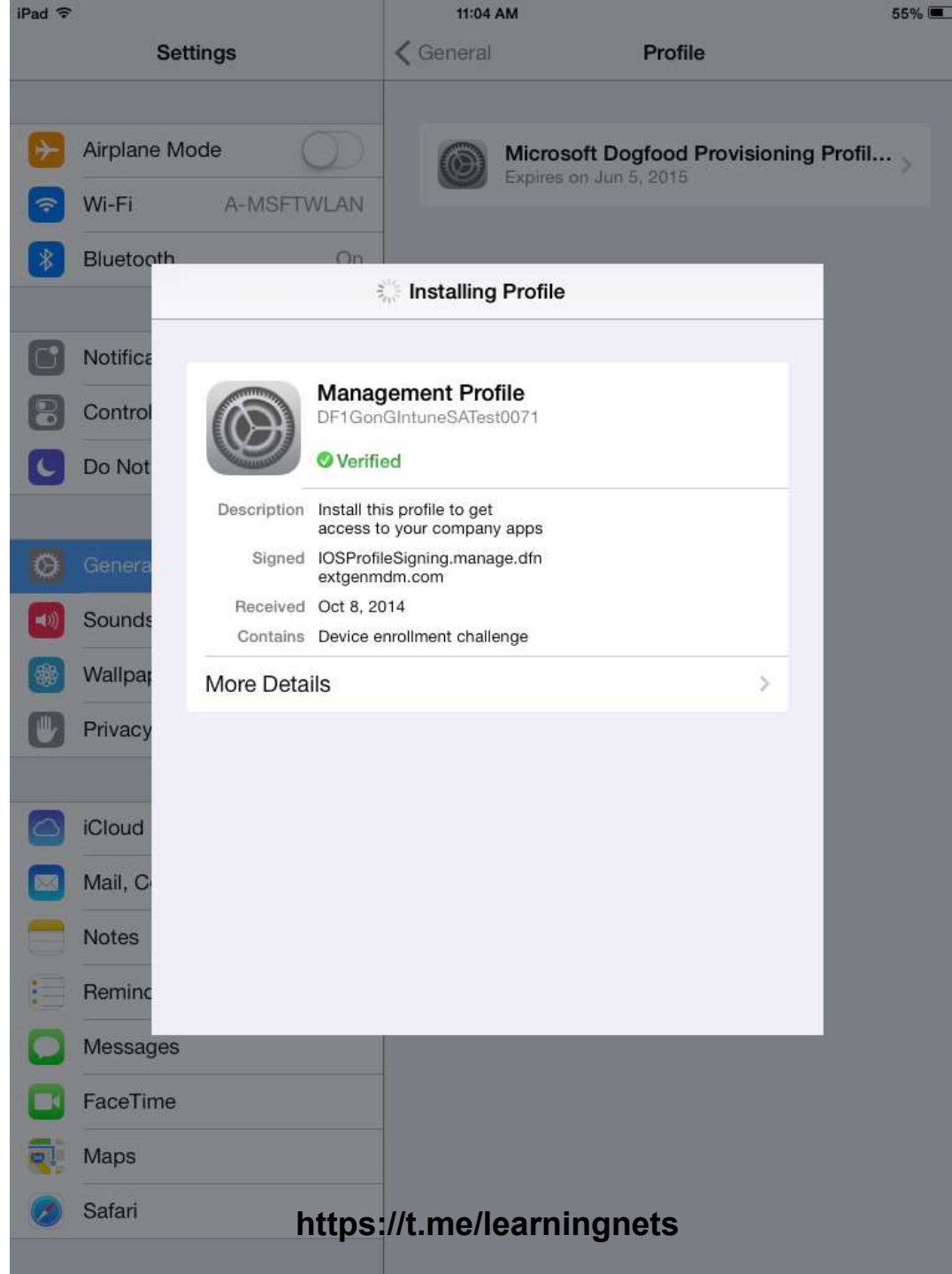


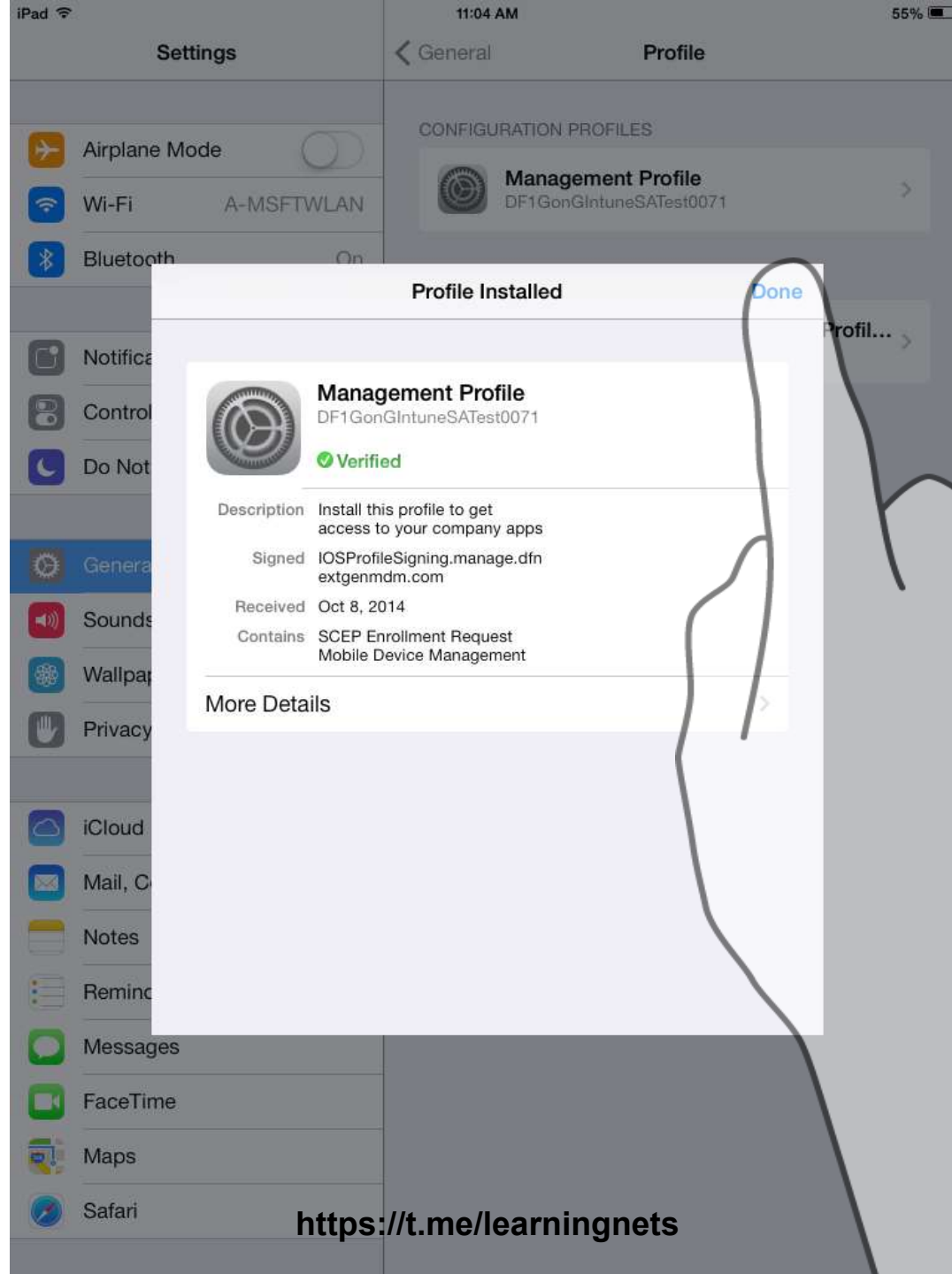


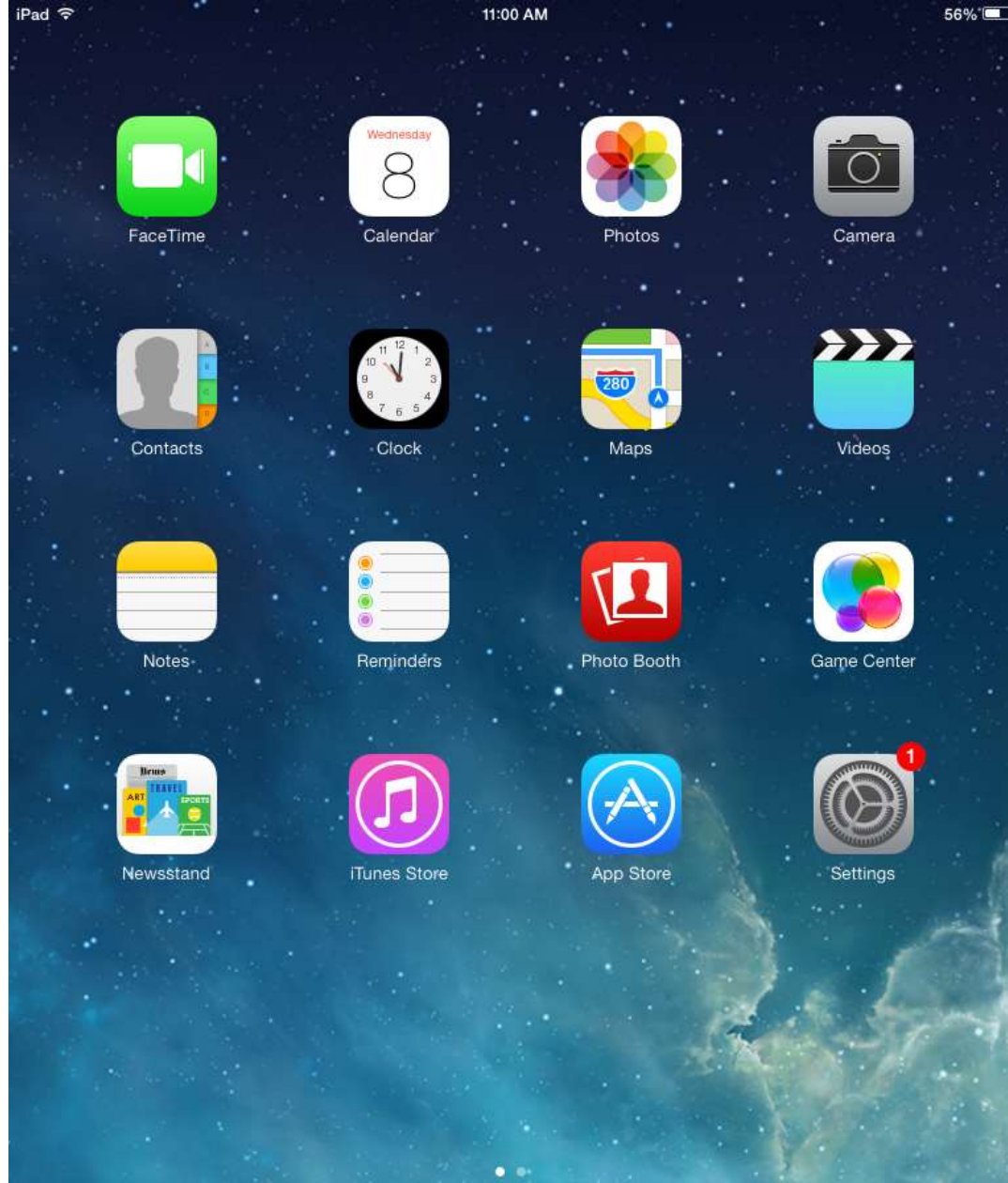




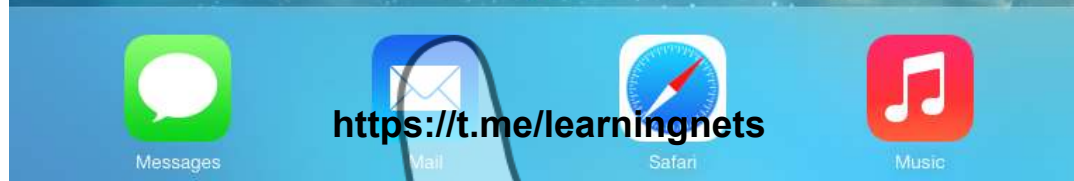








EAS



From: [Microsoft Outlook](#) >

Hide

To: [IW User 3](#) >

Your device isn't enrolled

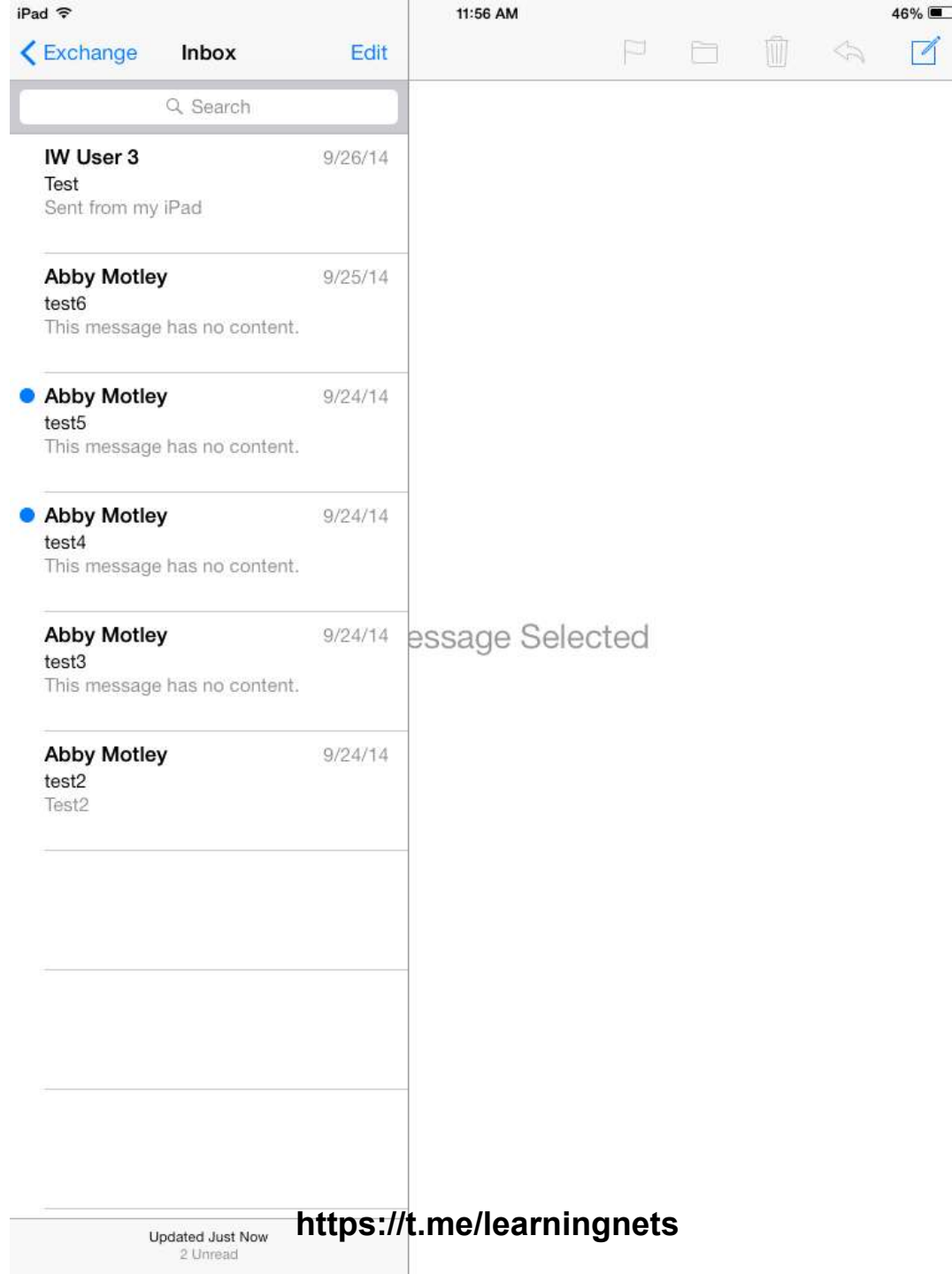
October 8, 2014 at 11:00 AM

To access company email and resources, you must enroll your device and make sure that your device complies with company security policy. Tap the following links to get started.

1. [Enroll device](#)
2. [Check device compliance status](#)

If you can't access email a few minutes after you've completed these steps, click [here](#) to fix the problem.





message Selected

<https://t.me/learningnets>

Microsoft Advanced Threat Analytics

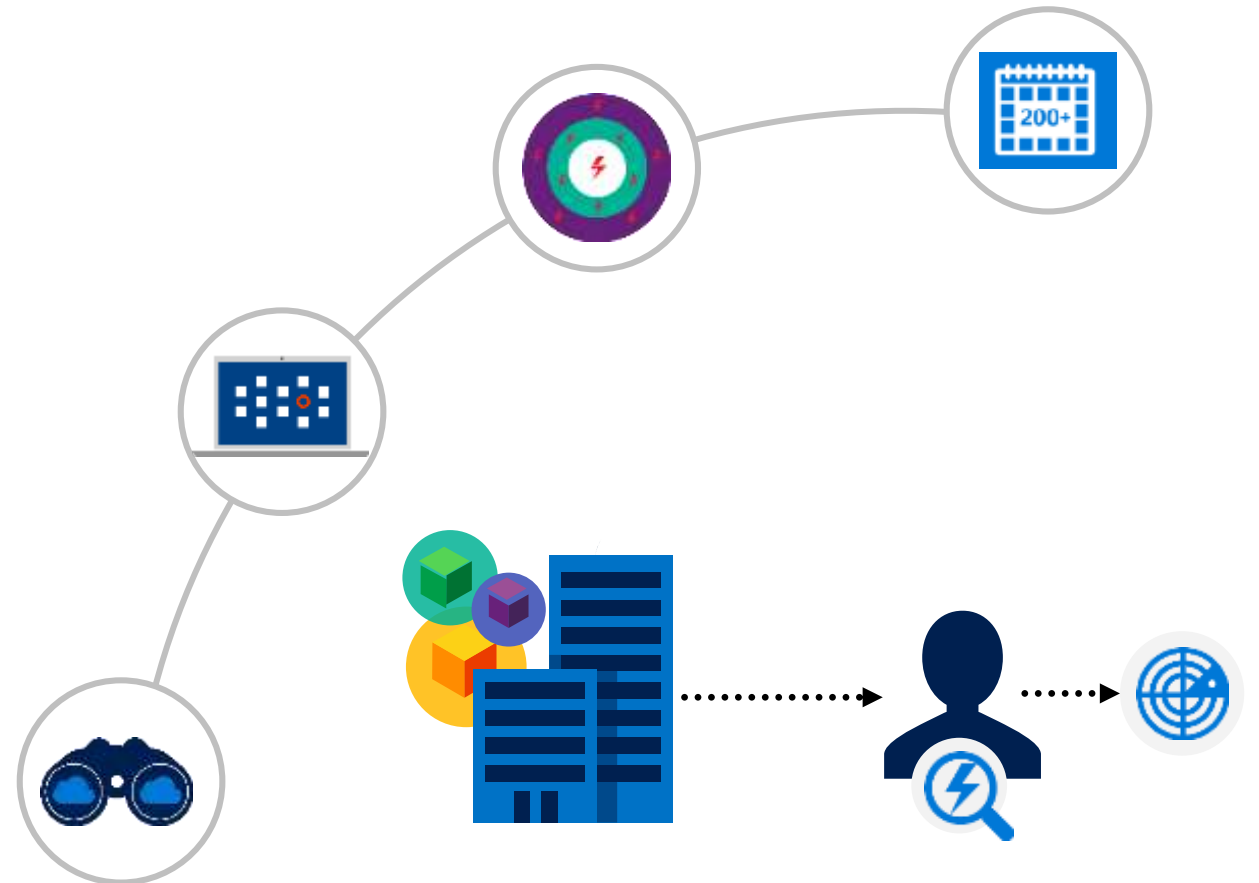


<https://t.me/learningnets>

DETECT ATTACKS BEFORE THEY CAUSE DAMAGE

Microsoft Advanced Threat Analytics

- ➔ Identifies advanced persistent threats (APTs) on-premises using User and Entity Behavioral Analytics
- ➔ Detects suspicious user and entity behavior with machine learning
- ➔ Detects malicious attacks (i.e. Pass the Hash, Pass the Ticket)
- ➔ Provides a simple attack timeline with clear and relevant attack information



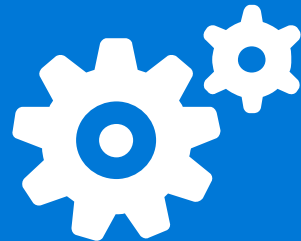
Focus on what is important fast

Detect threats fast
with Behavioral
Analytics



No need to create rules or policies, deploy agents, or monitor a flood of security reports. The intelligence needed is ready to analyze and continuously learning.

Adapt as fast as
your enemies



ATA continuously learns from the organizational entity behavior (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly evolving enterprise.

Focus on what is
important fast
using the simple
attack timeline



The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving you the power of perspective on the "who-what-when-and-how" of your enterprise. It also provides recommendations for next steps

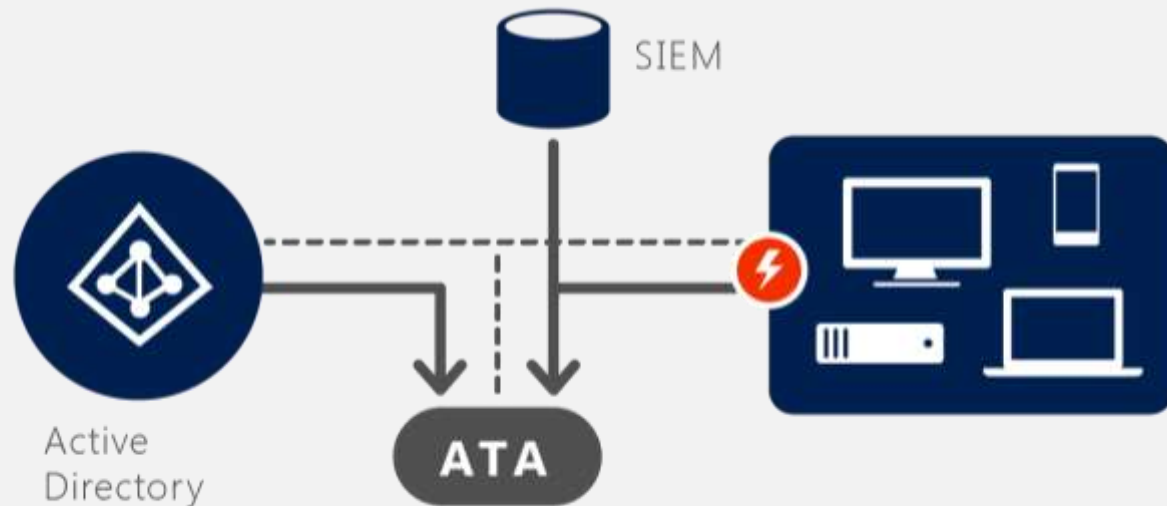
Reduce the fatigue
of false positives



Alerts only happen once suspicious activities are contextually aggregated, not only comparing the entity's behavior to its own behavior, but also to the profiles of other entities in its interaction path.

How Microsoft Advanced Threat Analytics works

1 Analyze

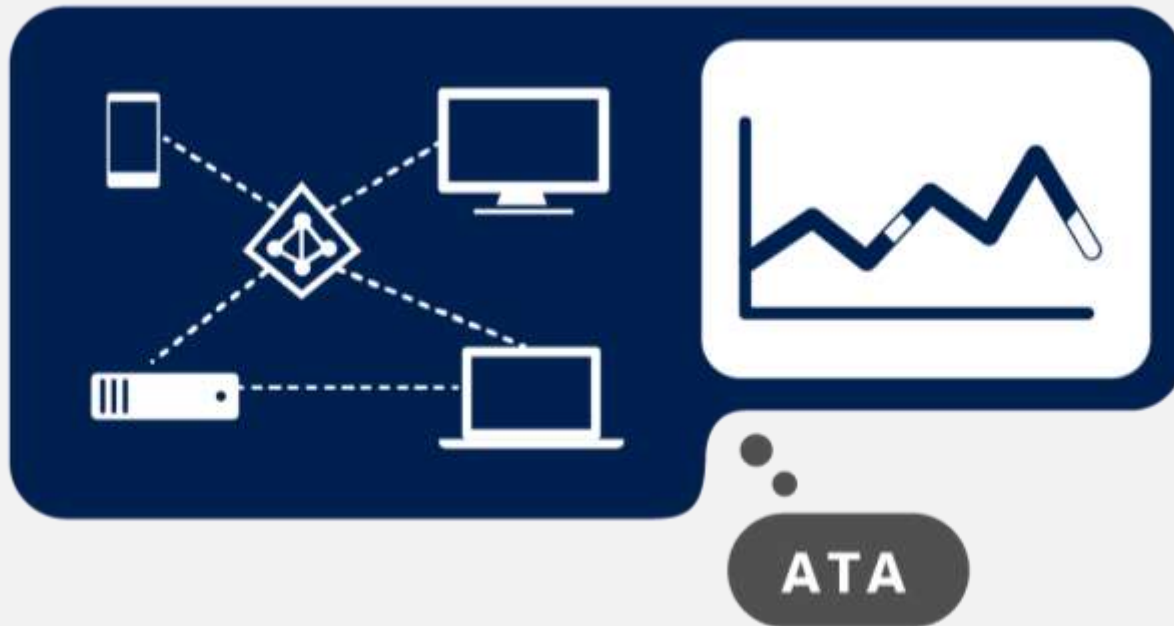


After installation:

- Simple non-intrusive port mirroring, or deployed directly onto domain controllers
- Remains invisible to the attackers
- Analyzes all Active Directory network traffic
- Collects relevant events from SIEM and information from Active Directory (titles, groups membership, and more)

How Microsoft Advanced Threat Analytics works

2 Learn



ATA:

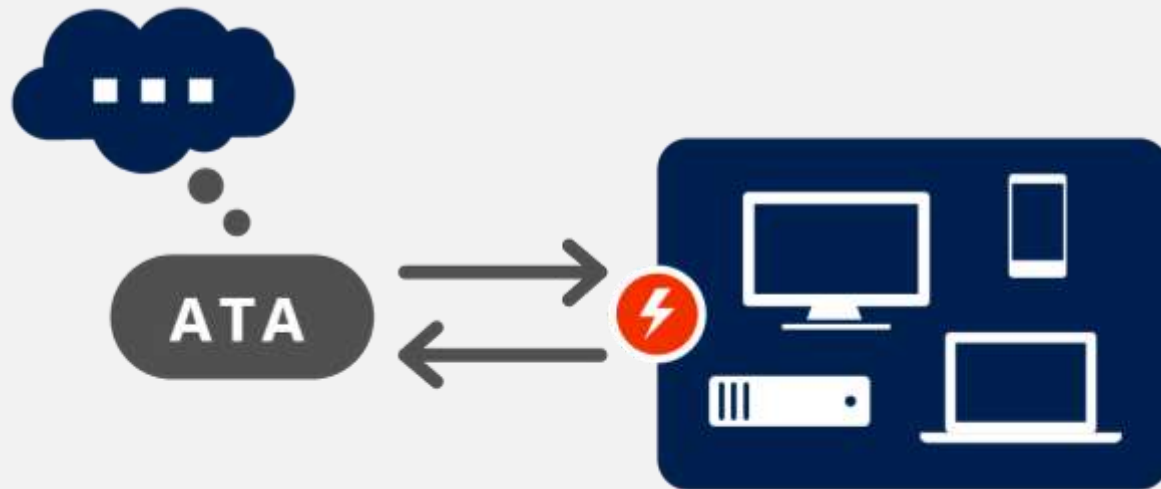
- Automatically starts learning and profiling entity behavior
- Identifies normal behavior for entities
- Learns continuously to update the activities of the users, devices, and resources

What is entity?

Entity represents users, devices, or resources

How Microsoft Advanced Threat Analytics works

3 Detect



Microsoft Advanced Threat Analytics:

- Looks for abnormal behavior and identifies suspicious activities
- Only raises red flags if abnormal activities are contextually aggregated
- Leverages world-class security research to detect security risks and attacks in near real-time based on attackers Tactics, Techniques, and Procedures (TTPs)

ATA not only compares the entity's behavior to its own, but also to the behavior of entities in its interaction path.

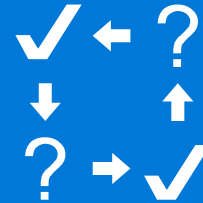
How Microsoft Advanced Threat Analytics works

4 Alert

ATA reports all suspicious activities on a simple, functional, actionable attack timeline



ATA identifies
Who?
What?
When?
How?



For each suspicious activity, ATA provides recommendations for the investigation and remediation



ATA detects a wide range of suspicious activities

Abnormal resource access
Account enumeration
Net Session enumeration
DNS enumeration



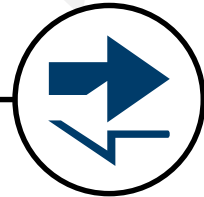
Reconnaissance

Compromised credential



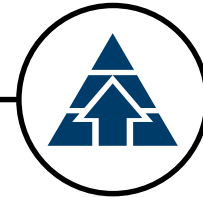
Abnormal working hours
Brute force using NTLM, Kerberos or LDAP
Sensitive accounts exposed in plain text authentication
Service accounts exposed in plain text authentication
Honey Token account suspicious activities
Unusual protocol implementation
Malicious Data Protection Private Information (DPAPI) Request

Abnormal authentication requests
Abnormal resource access
Pass-the-Ticket
Pass-the-Hash
Overpass-the-Hash



Lateral movement

Privilege escalation



MS14-068 exploit (Forged PAC)
MS11-013 exploit (Silver PAC)

Skeleton key malware
Golden ticket
Remote execution
Malicious replication requests



Domain dominance

Q1 Quarterly Report.xlsx

↑ All documents



Summary List Timeline Map Settings

Q1 Quarterly Report.xlsx



Shared
April 23, 2015

Expires
June 21, 2016

40
views
13 users

Michael Adams
Mark Adams
Katrina Redding
Joy Lawman
Bill Isvan
Mike Keller
Klaas Pluck
Paul Jensen
Yi Xu
...

9
denied
one user

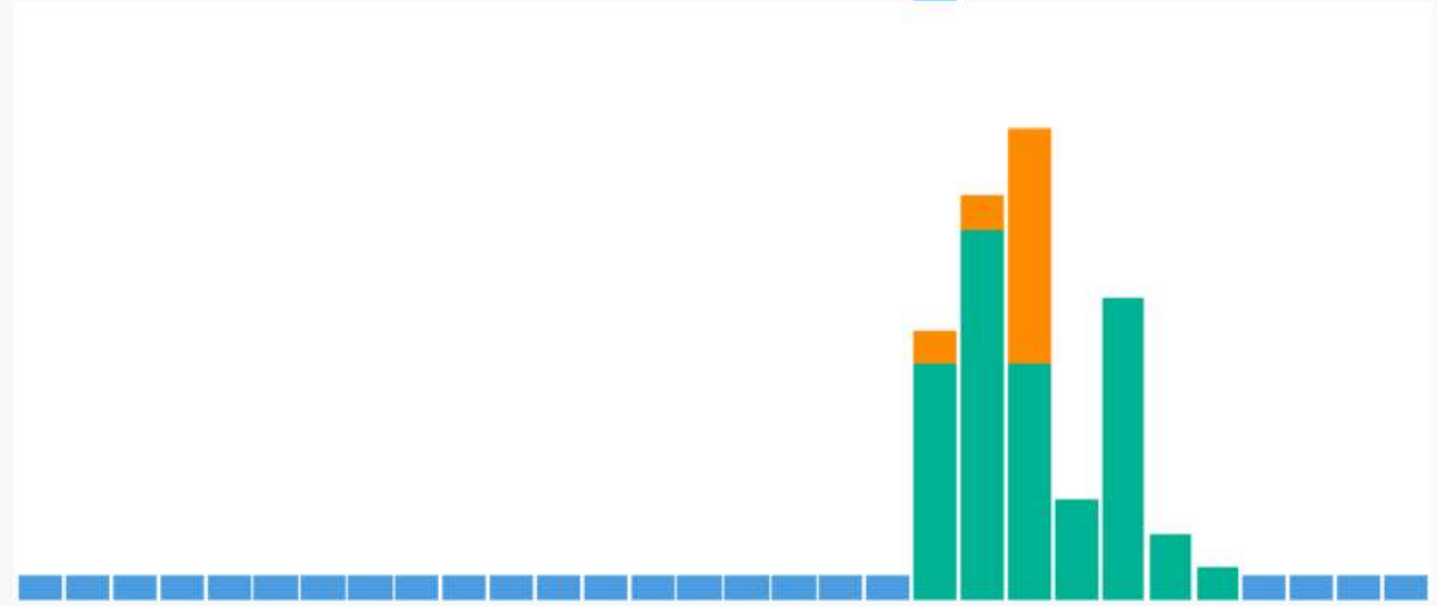
Bryan Swan

4
days
since last activity

Apr 29, 2015 10:51 AM
Apr 28, 2015 10:41 AM
Apr 28, 2015 10:26 AM
Apr 27, 2015 10:59 AM
...

<https://t.me/learningnets>

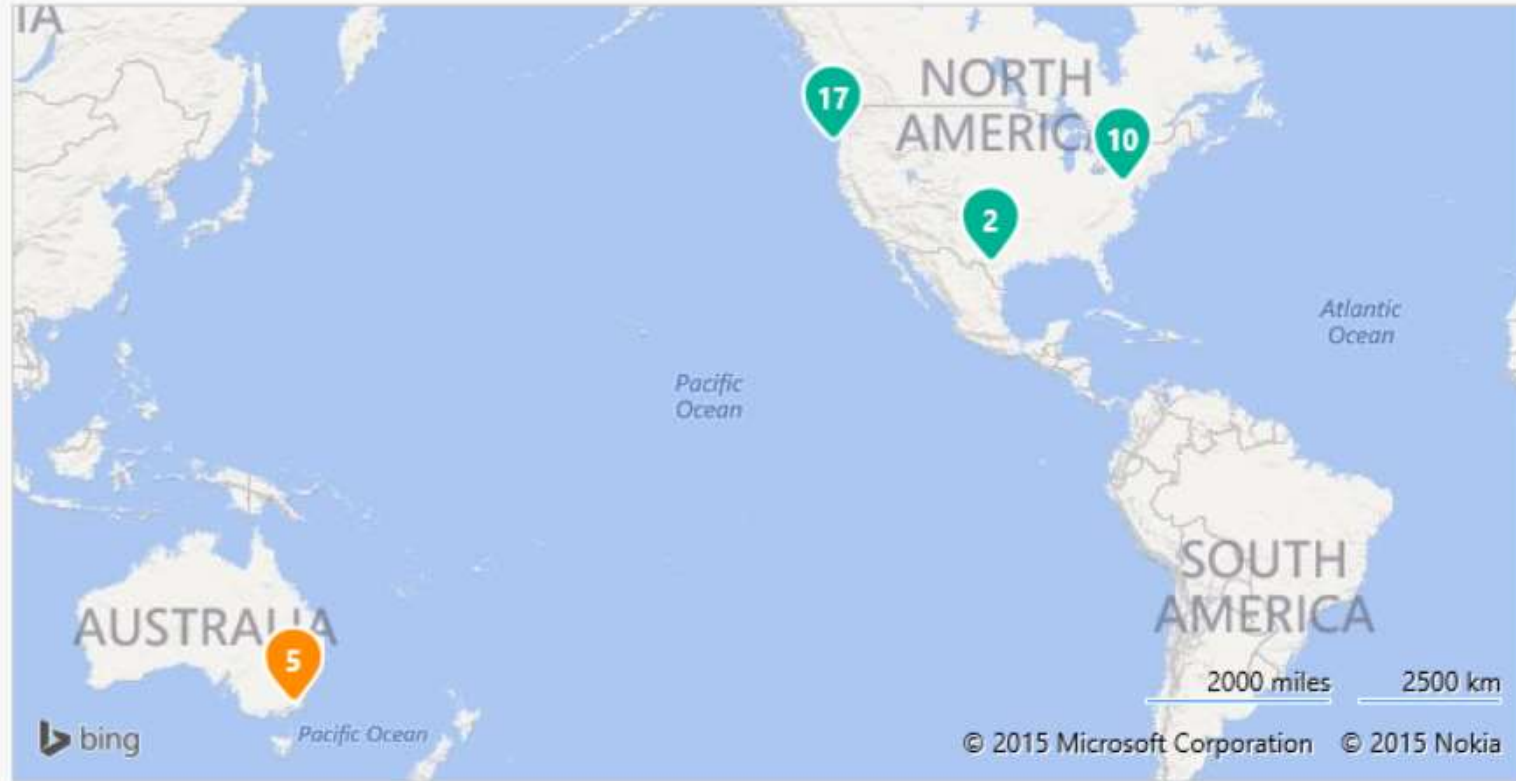
April 4 - May 3, 2015 - 40 viewed, 9 denied



Name	Status	Date ^
Mark Adams	Viewed	Apr 23, 2015 12:14 PM
Klaas Pluck	Viewed	Apr 23, 2015 12:20 PM
Bryan Swan	Denied	Apr 23, 2015 12:21 PM
Bill Isvan	Viewed	Apr 23, 2015 12:24 PM

<https://t.me/learningnets>

Worldwide - 40 viewed, 9 denied



viewed denied - at least one denied

United States

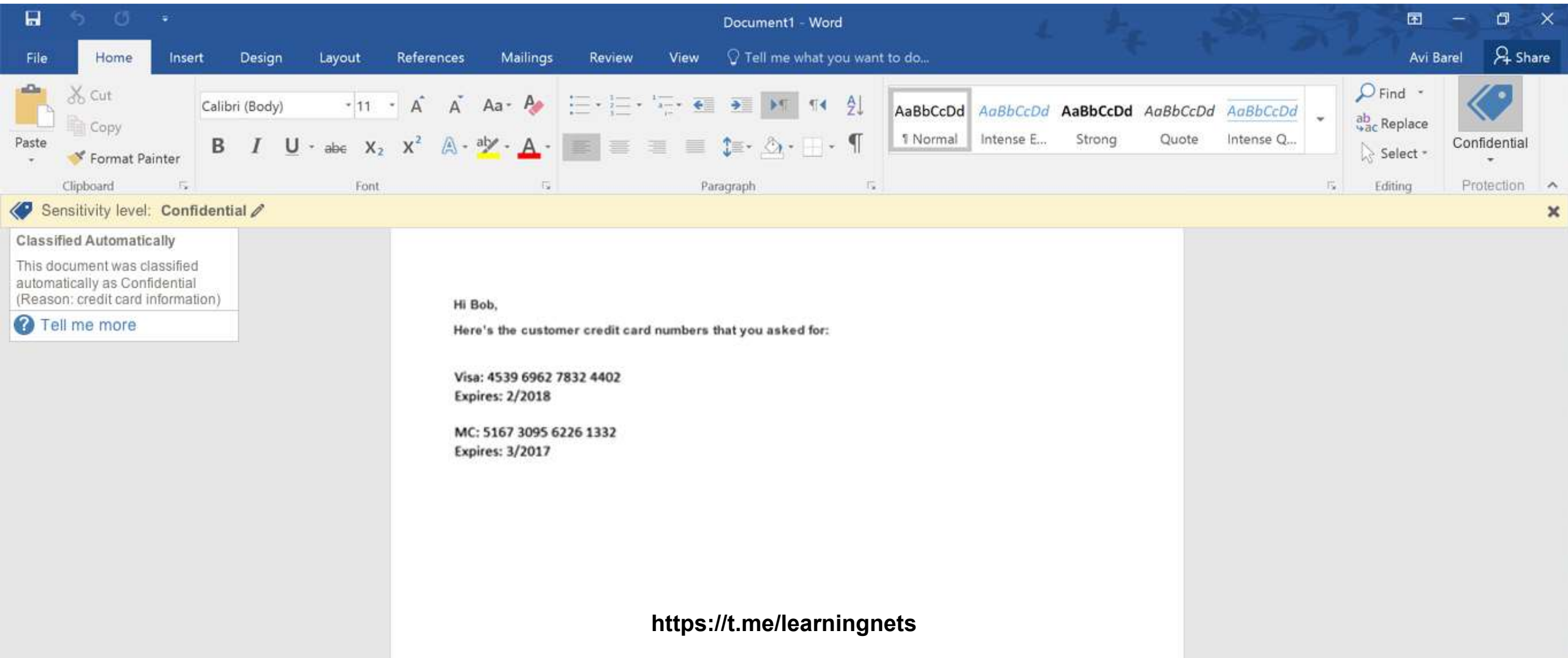
Name	Status	Date
Mark Adams	Viewed	Apr 23, 2015 12:14 PM
Klaas Pluck	Viewed	Apr 23, 2015 12:20 PM

<https://t.me/learningnets>

Classify, Label, Protect

Classify, Label, Protect

Automated classification



The screenshot shows the Microsoft Word interface with the document titled "Document1 - Word". The ribbon is set to "Home", and the "Confidential" sensitivity level is displayed in the top right corner. A yellow banner at the top of the document area indicates the sensitivity level is "Confidential".

Sensitivity level: Confidential

Classified Automatically
This document was classified automatically as Confidential (Reason: credit card information)
[Tell me more](#)

Hi Bob,
Here's the customer credit card numbers that you asked for:

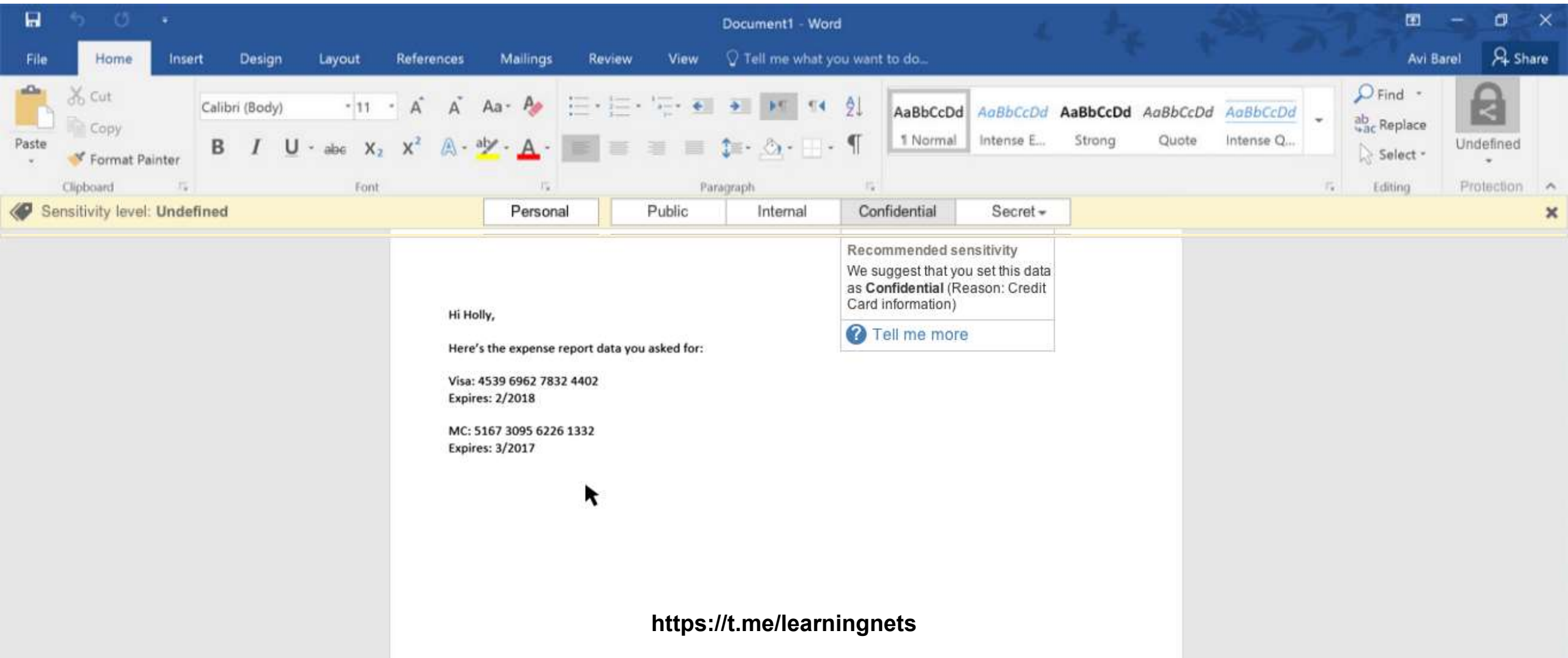
Visa: 4539 6962 7832 4402
Expires: 2/2018

MC: 5167 3095 6226 1332
Expires: 3/2017

<https://t.me/learningnets>

Classify, Label, Protect

Recommended classification



The screenshot shows the Microsoft Word interface with the following elements:

- File Name:** Document1 - Word
- Navigation Pane:** File, Home, Insert, Design, Layout, References, Mailings, Review, View
- Home Tab Ribbon:**
 - Clipboard:** Paste, Cut, Copy, Format Painter
 - Font:** Calibri (Body), 11, Bold (B), Italic (I), Underline (U), Text Color (abc), Background Color (X₂), Font Color (A), Text Highlighting (A)
 - Paragraph:** Bulleted List, Numbered List, Decrease Indent, Increase Indent, Paragraph Spacing, Paragraph Style, Paragraph Orientation, Paragraph Alignment, Paragraph Spacing (Before/After), Paragraph Spacing (Line and Paragraph Spacing), Paragraph Spacing (Line and Paragraph Spacing)
 - Styles:** 1 Normal, Intense E..., Strong, Quote, Intense Q...
 - Editing:** Find, Replace, Select
 - Protection:** Undefined
- Sensitivity Level:** Undefined (with a dropdown menu showing Personal, Public, Internal, Confidential, Secret)
- Document Content:**

Hi Holly,

Here's the expense report data you asked for:

Visa: 4539 6962 7832 4402
Expires: 2/2018

MC: 5167 3095 6226 1332
Expires: 3/2017
- Recommended Sensitivity Pop-up:**

Recommended sensitivity
We suggest that you set this data as **Confidential** (Reason: Credit Card information)
[Tell me more](#)

Classify, Label, Protect

Manual classification

Document1 - Word

File Home Insert Design Layout References Mailings Review View Tell me what you want to do... Avi Barel Share

Clipboard: Paste, Cut, Copy, Format Painter

Font: Calibri (Body), 11, Bold, Italic, Underline, Text Color, Background Color, Paragraph styles: Normal, Intense E..., Strong, Quote, Intense Q...

Editing: Find, Replace, Select

Protection: Confidential

Sensitivity level: Confidential

Personal Public Internal Confidential Secret

- All finance
- All employees

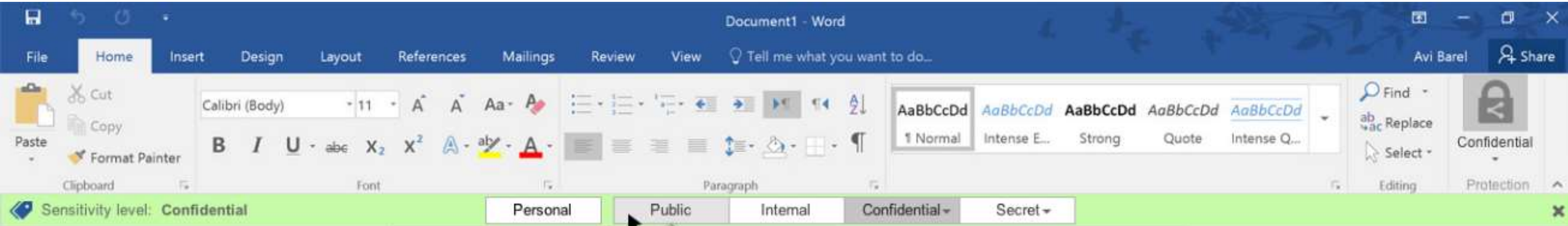
Hi Bob,
Here's the customer credit card numbers that you asked for:

Visa: 4539 6962 7832 4402
Expires: 2/2018

MC: 5167 3095 6226 1332
Expires: 3/2017

Classify, Label, Protect

Business justification required to re-classify



Hi Bob,
Here's the customer credit
card information:
Visa: 4539 6962 7832 4402
Expires: 2/2018
MC: 5167 3095 6226 1332
Expires: 3/2017

Lowering Sensitivity level [X]

Please tell why you are lowering from "Confidential" to "Internal":

The data was something that it is not

I need to change it to perform a certain task

Please explain why:

[Text area]

Cancel OK

Classify, Label, Protect

Prevent edit, copy, print and save with Azure Rights Management integration

The screenshot shows the Microsoft Word interface with a document titled "Document1 - Word". The ribbon is set to "Home". A yellow banner at the top of the document area indicates: "Sensitivity level: Confidential" and "This document is protected and will be expired in 4 days. You can't Reclassify, Export, Edit or Print it." A "Details" link is visible in the banner. A dialog box titled "Details" is open, showing the user's identity and permissions.

Details

You are viewing this document as:
bob.rotter@microsoft.com

You have the following permissions:

View:	Yes
Edit:	No
Copy:	No
Print:	No
Save:	No
Export:	No
Full control:	No
Access the document programmatically:	No

Expiration date: 01-25-2016

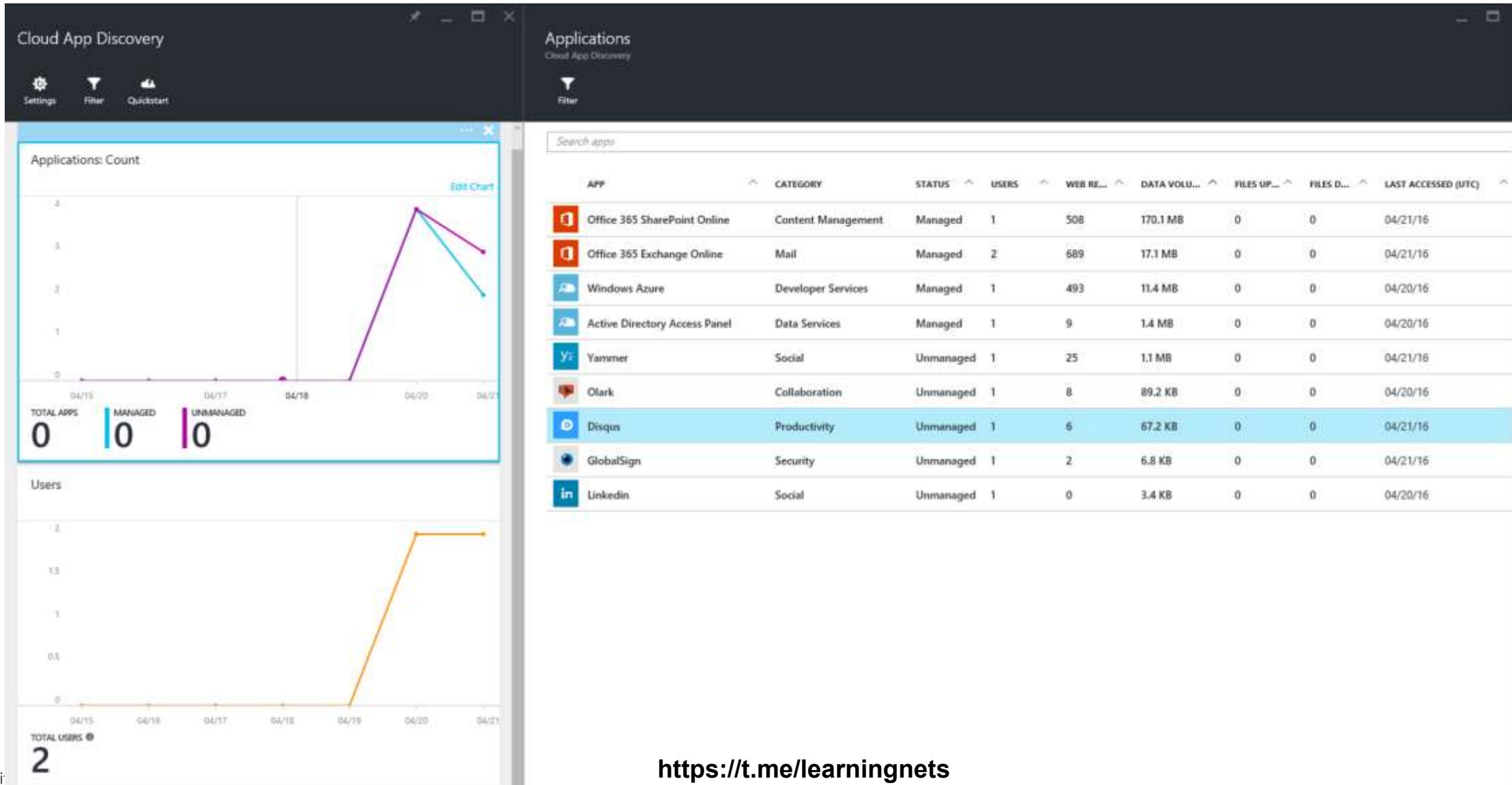
[? Tell me more](#) OK

SHADOW IT

SOFTPEDIA™
www.softpedia.com

<https://t.me/learningnets>

Cloud App Discovery



<https://t.me/learningnets>

Cloud App Security

Cloud App Security | Discover | Investigate | Control | Alerts 11 | Microsoft

Cloud Discovery

Global view | Last updated: Apr 21, 2018 | Last 90 days | Actions | Settings

All Cloud Discovery logs you manually uploaded are processed.

Dashboard | Discovered apps | IP addresses | Users

512 Discovered apps

12 Risky apps

2K Cloud users

3K IP addresses

App scores

- Low (score 1-3)
- Medium (score 4-6)
- High (score 7-10)
- Not scored

Sanctioned apps

- Sanctioned
- Discovered

Top apps

Traffic

Microsoft OneDrive	226.1 GB
Office 365	9.5 GB
Microsoft Exchange Online	9.2 GB
Microsoft Dynamics	6.2 GB
Microsoft Azure	4.2 GB

[View all apps](#)

Top risky apps

Traffic

MEGA	12.3 MB
IcalledU	97.5 KB
Marketwired	90.8 KB
Vortex	78.4 KB
MLB	64.8 KB

[View all risky apps](#)

Top users

Traffic

No users

[View all users](#)

Top IP addresses

Traffic

No IP addresses

[View all IP addresses](#)

<https://t.me/learningnets>

Cloud Discovery > Microsoft OneDrive Cloud storage

Global view
Last updated: Apr 21, 2016
Last 90 days

- Use
- Info
- Top IP addresses
- Top users
- Alerts

Overview

1K Total active users	3K Total IP addresses	88.7 GB Upload traffic	137.4 GB Download traffic	355K Total transactions
--------------------------	--------------------------	---------------------------	------------------------------	----------------------------

Users



Total traffic



Active source IP addresses



<https://t.me/learningnets>



Cloud Discovery > Microsoft OneDrive cloud storage

Global view

Last updated: Apr 21, 2016 ▾

Last 90 days ▾

[Use](#) [Info](#) [Top IP addresses](#) [Top users](#) [Alerts](#)

Go to a specific user

Top 100 users (by use)

User	Upload	Traffic	Transactions	+	Last seen (UTC)	↻ -
Lexi@contoso.com	2.1 MB	197.3 MB	5K		Mar 29, 2016	
Vanessa@contoso.com	24.0 MB	70.9 MB	5K		Mar 10, 2016	
Rodrique@contoso.com	776.5 KB	20.3 MB	5K		Mar 10, 2016	
Audriana@contoso.com	17.3 MB	72.9 MB	5K		Mar 10, 2016	
Sofia@contoso.com	21.9 MB	65.0 MB	5K		Mar 31, 2016	
Lillianna@contoso.com	24.7 MB	78.7 MB	4K		Mar 10, 2016	
Dane@contoso.com	25.0 MB	177.6 MB	4K		Mar 15, 2016	
Janiyah@contoso.com	21.1 MB	199.6 MB	4K		Mar 10, 2016	
Mckinley@contoso.com	25.3 MB	96.0 MB	4K		Mar 21, 2016	
Alisha@contoso.com	8.3 MB	167.7 MB	4K		Mar 10, 2016	
Esperanza@contoso.com	10.8 MB	37.2 MB	4K		Mar 10, 2016	



Files

New policy from search

New user notification

APP:
OWNER:
ACCESS LEVEL:
FILE TYPE:
VIOLATED POLICY:
Advanced ▾

1 - 7 of 7 files ⌵ ⌵ ⌵

File name	Owner	App	Collaborators	Last modified ▾
Shared with Everyone	leanna@acme.com	Microsoft OneDrive	1 collaborator	Oct 22, 2015 🔍 ⋮
Payment schedule and details.xlsx	jaeden@acme.com	Microsoft OneDrive	1 collaborator	Oct 22, 2015 ⋮
Test_file_for_DLP_test.docx	leanna@acme.com	Microsoft OneDrive	1 collaborator	Oct 22, 2015 ⋮
ACMEL CORP	kamila@acme.com	Microsoft OneDrive		Aug 4, 2015 🔍 ⋮
Test Files	kamila@acme.com	Microsoft OneDrive		Aug 4, 2015 🔍 ⋮
Customers	adams@acme.com	Microsoft OneDrive	7 collaborators	— 🔍 ⋮
DLP Project	adams@acme.com	Microsoft OneDrive	7 collaborators	— 🔍 ⋮