Enterprise Mobility + Security
Automation + Security for the Digital Workplace

Daniel Dickinson
Digital Workplace Cyber Security Specialist
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

Windows Defender
- 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

Exchange Online
- 35 billion messages/month

World's largest threat telemetry
Microsoft’s Security Approach

INTELLIGENT SECURITY GRAPH

- Cyber Defense Operations Center
  - Malware Protection Center
  - Cyber Hunting Teams
  - Security Response Center
  - Digital Crimes Unit

Industry Partners
Antivirus Network
CERTs

Conditional Access
Cloud App Security
Event Management
Rights Management
Key Vault
Security Center
Office 365 Advanced Threat Protection

Active Protection Service
Windows Update
SmartScreen

Advanced Threat Analytics
Azure Active Directory
Active Directory

Identity
Apps and Data
Infrastructure
Device

Office 365
PaaS
IaaS
SaaS

Microsoft’s Security Approach

Applications and Data
SaaS
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**

**Inside the Intelligent security graph**

**INTERFLOW API & THREAT ATTRIBUTION SERVICE**
(Interface into Threat Intel big data platform and attribution reports)

**ANALYTICS**
(Machine Learning, detonation service, behavioral tracking/heuristics)

**DATA COLLECTION & NORMALIZATION**
(Data feeds from products)

[Privacy/Compliance boundary]
# 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.

<table>
<thead>
<tr>
<th>Regulation/Standard Name and Description</th>
<th>Last Tested</th>
<th>Controls Tested</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001:2013</td>
<td>28/10/2015</td>
<td>231</td>
<td>No findings</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 27018:2014</td>
<td>28/10/2015</td>
<td>51</td>
<td>No findings</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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 CCCPF  Singapore MTCS Level 3  Australian Signals Directorate  New Zealand GCIO  Japan Financial Services  ENISA IAF
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
Empowering enterprise mobility

People-centric approach

User

Enable your users

Devices

Apps

Data

IT

Unify your environment

Protect your data
A HOLISTIC SOLUTION

Enterprise Mobility + Security

Extend enterprise-grade security to your cloud and SaaS apps

Microsoft Cloud App Security

Protect your users, devices, and apps

Microsoft Intune

Protect your data, everywhere

Azure Information Protection

Detect threats early with visibility and threat analytics

Microsoft Advanced Threat Analytics

Manage identity with hybrid integration to protect application access from identity attacks

Azure Active Directory Premium

A HOLISTIC SOLUTION
Enterprise Mobility + Security

Identity and access management

**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

**Microsoft Cloud App Security**
- Enterprise-grade visibility, control, and protection for your cloud applications

Managed Mobile Productivity

**Microsoft Intune**
- Mobile device and app management to protect corporate apps and data on any device.

Information Protection

**Azure Information Protection Premium P1**
- Encryption for all files and storage locations. Cloud based file tracking

Identity Driven Security

**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)

EMS E5

EMS E3

EMS E3

EMS E5

Sensitivity: Microsoft General
Integrated Identity as the control plane

One common identity

Simple connection

Self-service

Single sign on

Username

Microsoft Azure Active Directory

On-premises

Other Directories

Windows Server Active Directory

MIM

Cloud

Public cloud

Azure

SaaS

Office 365
Mini Exercise
Identity

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

Identity Devices Authentication
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

INTEGRATED APPLICATIONS
- Application usage
- Account provisioning activity
- Password rollover status
- Account provisioning errors

ACTIVITY LOGS
- Audit report
- Password reset activity
- Password reset registration activity
- Self service groups activity

RIGHTS MANAGEMENT
- RMS usage
- Most active RMS users
- RMS device usage
- RMS enabled application usage

EXTERNAL ACCESS
- Invitation summary
<table>
<thead>
<tr>
<th>DETECTION TYPE</th>
<th>RISK EVENT TYPE</th>
<th>RISK EVENTS CLOSED</th>
<th>DATE RANGE (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time</td>
<td>Sign-ins from unfamiliar location(s)</td>
<td>2 of 2</td>
<td>3/9/2016 - 3/10/2016</td>
</tr>
</tbody>
</table>

![Graph showing sign-ins from anonymous IP addresses](image)
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

Cloud services
- Azure
- Amazon.com
- FCS
- HyperV
- Private cloud or On-premises
- force.com
- Salesforce.com
MDM beyond email
Supported Platforms

- iOS
- macOS
- Android
- Windows
# Mobile Device Management for Office 365

## User-centric approach

<table>
<thead>
<tr>
<th>Conditional Access</th>
<th>Device Management</th>
<th>Selective Wipe</th>
<th>Application Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Envelope" /> <img src="image" alt="Lock" /> <img src="image" alt="Green Cube" /></td>
<td><img src="image" alt="Apple" /> <img src="image" alt="Android" /> <img src="image" alt="Windows" /></td>
<td><img src="image" alt="Pie Chart" /> <img src="image" alt="Bar Chart" /></td>
<td><img src="image" alt="Software Icons" /></td>
</tr>
</tbody>
</table>

**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

New Device Security Policy

What requirements do you want to have on devices?

- [x] Require a password
- [ ] Prevent simple password
- [ ] Require an alphanumeric password:
  - Password must include at least [ ] character sets
- [x] 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
- [x] Require data encryption on devices
- [ ] Device cannot be jail broken or rooted
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
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
Managed by your company

Enter your PIN

Forgot your PIN?
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

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

-Daniel
Managed by your company

Enter your PIN

Forgot your PIN?
### Downloads by Country (Top 10)

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

Numbers are for illustration purposes only.
<table>
<thead>
<tr>
<th>Country</th>
<th>Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.A.</td>
<td>12,551,290</td>
</tr>
<tr>
<td>U.K.</td>
<td>3,296,331</td>
</tr>
<tr>
<td>China</td>
<td>3,060,986</td>
</tr>
<tr>
<td>Mexico</td>
<td>1,427,828</td>
</tr>
<tr>
<td>Germany</td>
<td>1,242,704</td>
</tr>
<tr>
<td>Russia</td>
<td>1,181,069</td>
</tr>
<tr>
<td>Canada</td>
<td>1,122,512</td>
</tr>
<tr>
<td>Brazil</td>
<td>1,121,363</td>
</tr>
<tr>
<td>Australia</td>
<td>1,114,262</td>
</tr>
<tr>
<td>France</td>
<td>936,482</td>
</tr>
</tbody>
</table>

Numbers are for illustration purposes only.
<table>
<thead>
<tr>
<th>Country</th>
<th>Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.A.</td>
<td>12,551,290</td>
</tr>
<tr>
<td>U.K.</td>
<td>3,296,331</td>
</tr>
<tr>
<td>China</td>
<td>3,060,986</td>
</tr>
<tr>
<td>Mexico</td>
<td>1,427,828</td>
</tr>
<tr>
<td>Germany</td>
<td>1,242,704</td>
</tr>
<tr>
<td>Russia</td>
<td>1,181,069</td>
</tr>
<tr>
<td>Canada</td>
<td>1,122,512</td>
</tr>
<tr>
<td>Brazil</td>
<td>1,112,363</td>
</tr>
<tr>
<td>Australia</td>
<td>1,114,262</td>
</tr>
<tr>
<td>France</td>
<td>936,482</td>
</tr>
</tbody>
</table>

Numbers are for illustration purposes only.
Managed by your company
App Data Report:

Additional references:
http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1
App Data Report:

Additional references:
http://windows.microsoft.com/is-IS/windows-
<table>
<thead>
<tr>
<th>Country</th>
<th>Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.K.</td>
<td>3,296,331</td>
</tr>
<tr>
<td>China</td>
<td>3,060,986</td>
</tr>
<tr>
<td>Mexico</td>
<td>1,427,828</td>
</tr>
<tr>
<td>Germany</td>
<td>1,242,704</td>
</tr>
<tr>
<td>Russia</td>
<td>1,181,069</td>
</tr>
<tr>
<td>Canada</td>
<td>1,122,512</td>
</tr>
<tr>
<td>Brazil</td>
<td>1,121,363</td>
</tr>
<tr>
<td>Australia</td>
<td>1,114,262</td>
</tr>
<tr>
<td>France</td>
<td>936,482</td>
</tr>
</tbody>
</table>
Additional references:
http://windows.microsoft.com/is-IS/windows-8/apps#Cat=t1
Additional resources:

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

Enter your PIN

Forgot your PIN?
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 Genesis classic.

writr
An interactive journal and calendar for personal growth.
Alert
Access to this website has been blocked.
Contact your IT administrator if you feel you should have access to this resource.
End User Enrollment Walkthrough
Enrolling in Office 365 MDM

Connect through Office Apps

Connect to email via Built-In Email Client
Enrolling in Office 365 MDM

- Download & sign into Office applications
- Connect to email via Built-In Email Client
Office apps

- Mail++ for Outlook
  - iKonics LLC
  - $5.99
  - Offers In-App Purchases

- Inbox Pro, Outlook Edition
  - Code Below Dreams, Inc.
  - $6.99
  - (121)

- OWA for iPad
  - Microsoft Corporation
  - FREE

- myMail - Free Hotmail, Gmail, Yahoo, Outlook, Live, AOL M...
  - My.com
  - (17)

- Yahoo Mail – Free Email App
  - Yahoo
  - FREE

- Eye Color Changer - Magic Photo Editor for Blue, Brown, ...
brian@contoso.com

Sign in with your organizational account

Keep me signed in

Sign in

Can't access your account?
You need to enroll your device

Your organization requires that you enroll your device before you can access workplace resources.
To enroll your device, you must install the free Microsoft Intune Company Portal app from the iTunes store. Click the View button above to begin.

If you already have the Company Portal app, tap the Open button.
Office apps

Windows Intune Company Portal

Microsoft Corporation

Description

The Company Portal app helps you search, browse and install apps made available to you by your organization. With the Windows Intune Company Portal, apps can be installed without elevation or connection to a user.
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 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
Device Successfully Enrolled

Return to email

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

Brian Shiers
(333) xxx-xx12

Please enter the code to continue

XYZZY

Other security verification options
Sign in with another account

Sign in  Cancel
Office apps

Installing Profile

Management Profile

Install this profile to get access to your company apps

Verified

Description
Install this profile to get access to your company apps

Signed

Received

Contains

More Details

Install Profile

Installing this profile will change settings on your iPad.

Cancel  Install Now
Office apps

Management Profile

Description: Install this profile to get access to your company apps
Signed: IOSProfileSigning.manage.dfn iosgen-mdm.com
Received: Oct 8, 2014
Contains: Device enrollment challenge

More Details

Installing Profile
Generating Key

Management Profile
DPI 89C13299SATm39071
Verified

Description: Install this profile to get access to your company apps
Signed: IOSProfileSigning.manage.dfn
VeriSignMDM.com
Received: Oct 8, 2014
Contains: Device enrollment challenge

More Details
Office apps

Installing Profile

Management Profile

- Description: Install this profile to get access to your company apps
- Signed: iOSProfileSigning.manage.dfn
- Received: Oct 8, 2014
- Contains: Device enrollment challenge

More Details
MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://manage.cefnextgenmdm.com/DeviceGatewayProxy/ioshandler.ashx” to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.
Management Profile

Description: Install this profile to get access to your company apps.
Signed: iOSProfileSigning.manage.dfn
Verified: True
Received: Oct 8, 2014
Contains: Device enrollment challenge

More Details

Verified

Microsoft Dogfood Provisioning Profile...
Office apps

Management Profile

Description: Install this profile to get access to your company apps
Signed: IOSProfileSigning_manage.dm
Received: Oct 8, 2014
Contains: Device enrollment challenges

More Details
Katie Jordan
Adobe vision video
Agreed, things are moving quickly.

Katie Jordan
Trip Expenses!
10/30/2014
What is the ROI code we should use for...

Draft Katie Jordan
Expense Summary
10/30/2014
2014 Expenses, consider, shared via OneDrive...

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

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

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

Katie Jordan
Tracking info
10/24/2014
Tracking information: Ship Carrier; FedEx...

Alex Darrow
Support org changes
10/24/2014
Hi Sara. I’d love to chat with you some...

Garth Fort
Review meeting
10/23/2014
Can you set up a review meeting with 8...

Garth Fort
Lunch today?
10/21/2014
How does your schedule look? Would l...

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

t 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=FLR9ANGsDo
Enrolling in Office 365 MDM

Download & sign into Office applications

Connect to email via Built-In Email App
<table>
<thead>
<tr>
<th>Settings</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane Mode</td>
<td>About</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Software Update</td>
</tr>
<tr>
<td>Bluetooth</td>
<td></td>
</tr>
<tr>
<td>Notification Center</td>
<td>Siri</td>
</tr>
<tr>
<td>Control Center</td>
<td>Spotlight Search</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Text Size</td>
</tr>
<tr>
<td>General</td>
<td>Accessibility</td>
</tr>
<tr>
<td>Sounds</td>
<td></td>
</tr>
<tr>
<td>Wallpapers &amp; Brightness</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
</tr>
<tr>
<td>iCloud</td>
<td>Multitasking Gestures</td>
</tr>
<tr>
<td>Mail, Contacts, Calendars</td>
<td>Use four or five fingers to:</td>
</tr>
<tr>
<td>Notes</td>
<td>• Pinch to the Home Screen</td>
</tr>
<tr>
<td>Reminders</td>
<td>• Swipe up to multitasking</td>
</tr>
<tr>
<td>Messages</td>
<td>• Swipe left or right between apps</td>
</tr>
<tr>
<td>FaceTime</td>
<td></td>
</tr>
<tr>
<td>Maps</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td></td>
</tr>
</tbody>
</table>

**USE SIDE SWITCH TO:**

- Lock Rotation
- Mute

Rotation Lock is available in Control Center.

- Usage
- Background App Refresh

- Auto-Lock: Never
- Passcode Lock: Off
- Restrictions: Off
Settings

- Airplane Mode
- Wi-Fi
- Bluetooth
- Notification Center
- Control Center
- Do Not Disturb

General

Sounds

Wallpapers & Brightness

Privacy

iCloud

Mail, Contacts, Calendars

- Notes
- Reminders
- Messages
- FaceTime
- Maps
- Safari

Other:
brian@contoso.com

Email brian@contoso.com
Password ********
Description Exchange
Email: brian@contoso.com
Password: ********
Description: Exchange
From: Microsoft Outlook
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.
To enroll your device, you must install the free Microsoft Intune Company Portal app from the iTunes store. Click the View button above to begin.

If you already have the Company Portal app, tap the Open button.
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 your device
For added security, we need to verify your account. We have sent a text message with the verification code.

Brian Shiers
(***-***-**12)

Please enter the code to continue

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

Please enter the code to continue

XYZZY

Other security verification options
Sign in with another account

Sign in  Cancel
Install Profile

Management Profile

DPI-GoCImageFATwin0071

Description: Install this profile to get access to your company apps
Signed: iOSProfile/Signing_manage.dfn
Organization: iisagentmdm.com
Received: Oct 8, 2014
Contains: Device enrollment challenge

More Details
Management Profile
DPI SecAhead@AT&amp;Tm0071

Description: Install this profile to get access to your company apps
Signed: IOSProfileSigning.manage.dfn xotgenmdm.com
Received: Oct 8, 2014
Contains: Device enrollment challenges

More Details
Management Profile

DPI: 0x0161 and 0x0167

Description: Install this profile to get access to your company apps

Signed: iOSProfileSigning.manage.dtm

VeriSign MDM

Received: Oct 8, 2014

Contains: Device enrollment challenge

More Details
Installing this profile will allow the administrator at "https://manage.citrixcloud.com/DeviceGatewayProxy/ioshandler.cshx" to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.
From: Microsoft Outlook
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 in a few minutes after you’ve completed these steps, click here to fix the problem.
<table>
<thead>
<tr>
<th>Sender</th>
<th>Date</th>
<th>Message Content</th>
</tr>
</thead>
</table>
| IW User 3  | 9/26/14 | Test
| Abby Motley| 9/25/14 | test16
| Abby Motley| 9/24/14 | test15
| Abby Motley| 9/24/14 | test14
| Abby Motley| 9/24/14 | test13
| Abby Motley| 9/24/14 | test12
| Abby Motley| 9/24/14 | test12

This message has no content.
Detects 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.
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
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

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

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

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

Skeleton key malware
Golden ticket
Remote execution
Malicious replication requests

Reconnaissance
Compromised credential
Lateral movement
Privilege escalation
Domain dominance
Classify, Label, Protect
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
Hi Holly,

Here's the expense report data you asked for:

Visa: 4539 0962 7832 4402
Expires: 2/2018

MC: 5167 3095 0226 1332
Expires: 3/2017
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
Classify, Label, Protect

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

Applications:
- Office 365 SharePoint Online
  - Category: Content Management
  - Status: Managed
  - Users: 1
  - Web RBAC: 508
  - Data Storage: 170.8 MB
  - Files: 0
  - Last Access: 04/21/16

- Office 365 Exchange Online
  - Category: Mail
  - Status: Managed
  - Users: 2
  - Web RBAC: 688
  - Data Storage: 17.3 MB
  - Files: 0
  - Last Access: 06/21/16

- Windows Azure
  - Category: Developer Services
  - Status: Managed
  - Users: 1
  - Web RBAC: 482
  - Data Storage: 11.3 MB
  - Files: 0
  - Last Access: 04/20/16

- Active Directory Access Panel
  - Category: Data Services
  - Status: Managed
  - Users: 1
  - Web RBAC: 9
  - Data Storage: 1.4 MB
  - Files: 0
  - Last Access: 04/20/16

- Yammer
  - Category: Social
  - Status: Unmanaged
  - Users: 1
  - Web RBAC: 25
  - Data Storage: 11 MB
  - Files: 0
  - Last Access: 04/20/16

- Okta
  - Category: Collaboration
  - Status: Unmanaged
  - Users: 1
  - Web RBAC: 8
  - Data Storage: 89.2 KB
  - Files: 0
  - Last Access: 04/20/16

- Disqus
  - Category: Productivity
  - Status: Unmanaged
  - Users: 1
  - Web RBAC: 6
  - Data Storage: 67.2 KB
  - Files: 0
  - Last Access: 04/20/16

- GlobalSign
  - Category: Security
  - Status: Unmanaged
  - Users: 1
  - Web RBAC: 2
  - Data Storage: 6.8 KB
  - Files: 0
  - Last Access: 04/21/16

- LinkedIn
  - Category: Social
  - Status: Unmanaged
  - Users: 1
  - Web RBAC: 0
  - Data Storage: 14.4 KB
  - Files: 0
  - Last Access: 04/20/16
<table>
<thead>
<tr>
<th>User</th>
<th>Upload</th>
<th>Traffic</th>
<th>Transactions</th>
<th>Last seen (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:Lenn@contoso.com">Lenn@contoso.com</a></td>
<td>2.1 MB</td>
<td>197.3 MB</td>
<td>5K</td>
<td>Mar 29, 2016</td>
</tr>
<tr>
<td><a href="mailto:Vanessa@contoso.com">Vanessa@contoso.com</a></td>
<td>24.0 MB</td>
<td>70.9 MB</td>
<td>5K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td><a href="mailto:Rodrique@contoso.com">Rodrique@contoso.com</a></td>
<td>776.5 KB</td>
<td>20.3 MB</td>
<td>5K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td><a href="mailto:Audrina@contoso.com">Audrina@contoso.com</a></td>
<td>17.9 MB</td>
<td>72.9 MB</td>
<td>5K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td><a href="mailto:Sofia@contoso.com">Sofia@contoso.com</a></td>
<td>21.9 MB</td>
<td>65.0 MB</td>
<td>5K</td>
<td>Mar 21, 2016</td>
</tr>
<tr>
<td><a href="mailto:Lilianna@contoso.com">Lilianna@contoso.com</a></td>
<td>24.7 MB</td>
<td>78.7 MB</td>
<td>4K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td><a href="mailto:Diane@contoso.com">Diane@contoso.com</a></td>
<td>25.0 MB</td>
<td>177.5 MB</td>
<td>4K</td>
<td>Mar 15, 2016</td>
</tr>
<tr>
<td><a href="mailto:Janiyah@contoso.com">Janiyah@contoso.com</a></td>
<td>21.1 MB</td>
<td>199.5 MB</td>
<td>4K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td><a href="mailto:Mckney@contoso.com">Mckney@contoso.com</a></td>
<td>25.3 MB</td>
<td>96.0 MB</td>
<td>4K</td>
<td>Mar 21, 2016</td>
</tr>
<tr>
<td><a href="mailto:Alisha@contoso.com">Alisha@contoso.com</a></td>
<td>8.2 MB</td>
<td>167.7 MB</td>
<td>4K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td><a href="mailto:Esperanza@contoso.com">Esperanza@contoso.com</a></td>
<td>16.8 MB</td>
<td>37.2 MB</td>
<td>4K</td>
<td>Mar 10, 2016</td>
</tr>
<tr>
<td>File name</td>
<td>Owner</td>
<td>App</td>
<td>Collaborators</td>
<td>Last modified</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Shared with Everyone</td>
<td><a href="mailto:leanna@acme.com">leanna@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td>1 collaborator</td>
<td>Oct 22, 2015</td>
</tr>
<tr>
<td>Payment schedule and details.xlsx</td>
<td><a href="mailto:jared@acme.com">jared@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td>1 collaborator</td>
<td>Oct 22, 2015</td>
</tr>
<tr>
<td>Test_file_for_DLP_test.docx</td>
<td><a href="mailto:leanna@acme.com">leanna@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td>1 collaborator</td>
<td>Oct 22, 2015</td>
</tr>
<tr>
<td>ACMEL CORP</td>
<td><a href="mailto:kamilia@acme.com">kamilia@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td></td>
<td>Aug 4, 2015</td>
</tr>
<tr>
<td>Test Files</td>
<td><a href="mailto:kamilia@acme.com">kamilia@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td></td>
<td>Aug 4, 2015</td>
</tr>
<tr>
<td>Customers</td>
<td><a href="mailto:adams@acme.com">adams@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td>7 collaborators</td>
<td></td>
</tr>
<tr>
<td>DLP Project</td>
<td><a href="mailto:adams@acme.com">adams@acme.com</a></td>
<td>Microsoft OneDrive</td>
<td>7 collaborators</td>
<td></td>
</tr>
</tbody>
</table>