Protection through One Microsoft Cyber Security Platform from Client to Server
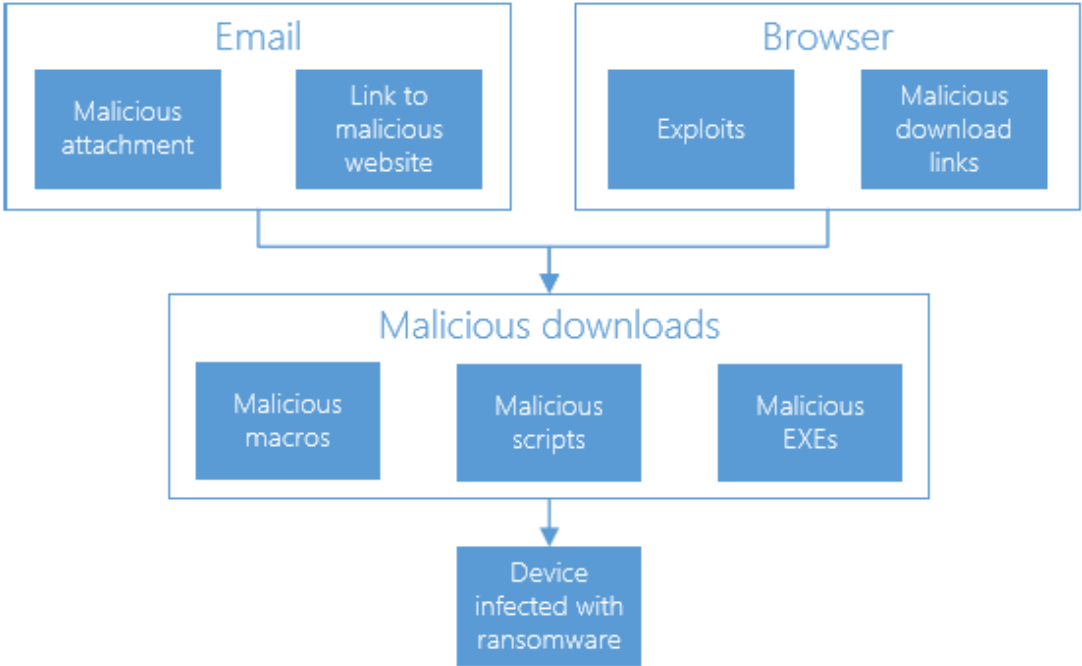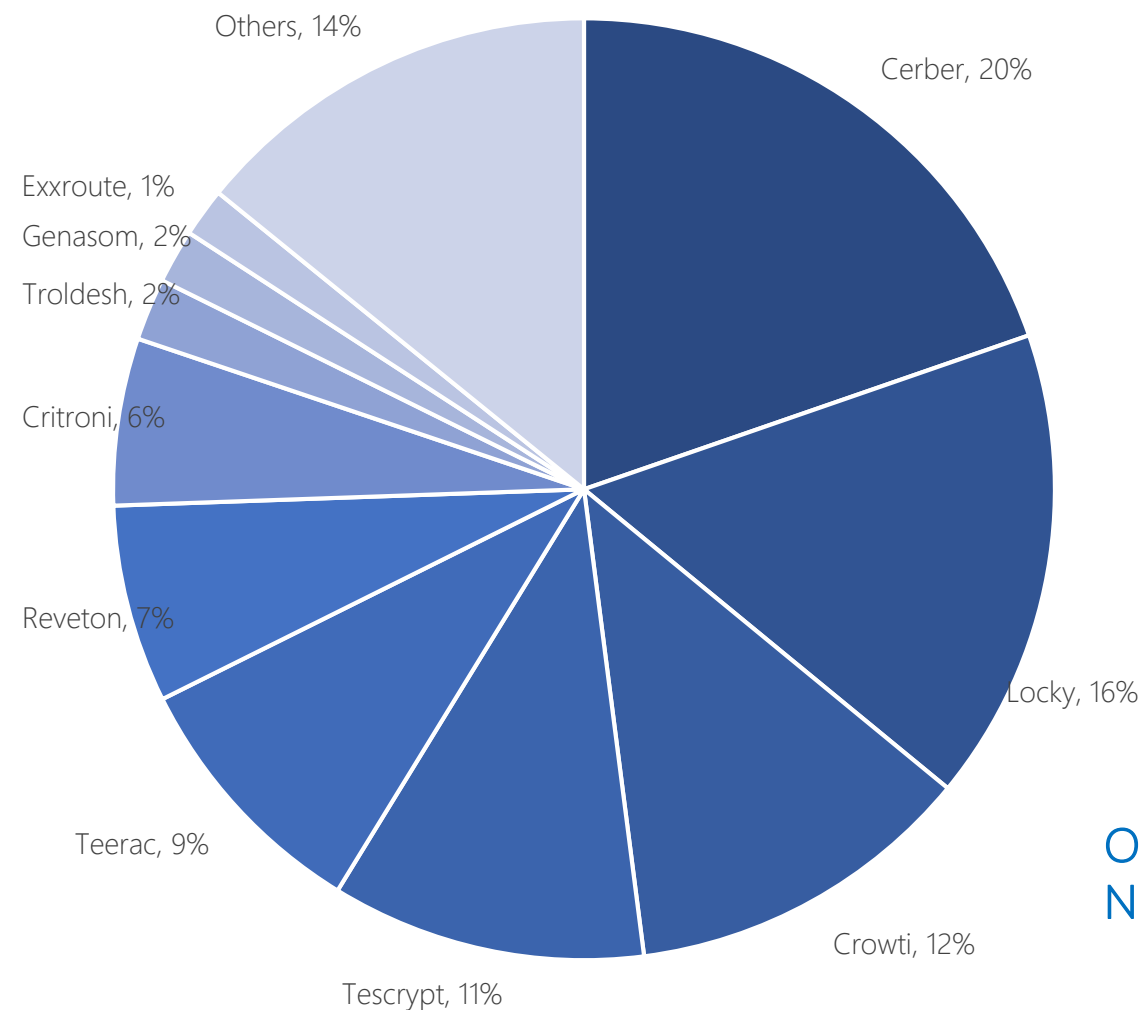
Andy Fung
Technology Strategist
Microsoft Hong Kong

■ Windows

# Ransomware – Top Families and Attack Vectors

Ransomware encounters by family in 2016

- Cerber, 20%
- Locky, 16%
- Crowti, 12%
- Tescrypt, 11%
- Teerac, 9%
- Reveton, 7%
- Critroni, 6%
- Troldesh, 2%
- Genasom, 2%
- Exxroute, 1%
- Others, 14%

Email
- Malicious attachment
- Link to malicious website

Browser
- Exploits
- Malicious download links

Malicious downloads
- Malicious macros
- Malicious scripts
- Malicious EXEs

Device infected with ransomware

Office 365 analyze 200B emails per month for spam and malware
NSS labs study shows Edge most secure browser against SEM
Edge blocks SEM 16x faster than Chrome or Firefox

WINDOWS DEFENDER SMARTSCREEN
BLOCKS MALICIOUS URL'S AND APPS

→ Blocks phishing and exploit sites

→ Blocks downloading of malicious apps

→ Supported in Microsoft Edge, Internet Explorer and Universal Windows Apps

→ Constantly updated by the Intelligent Security Graph
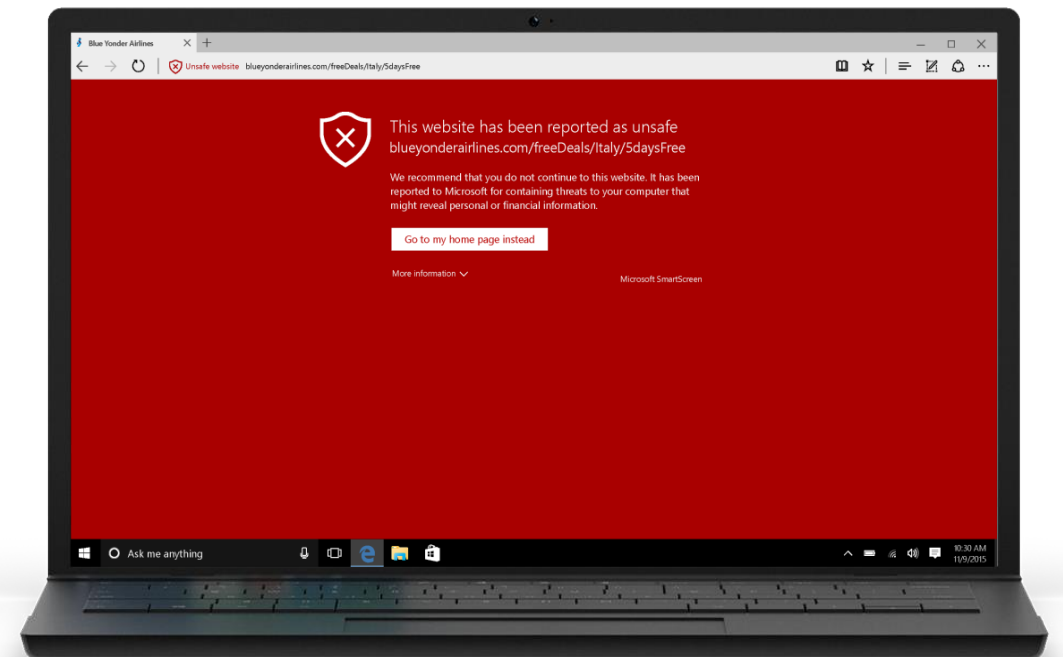
WINDOWS DEFENDER ANTIVIRUS
MALWARE PROTECTION

Protection that competes to win
Scored 100% detection in Real World Testing against top competitors (AVTest Dec 2016) and Scored 100% for Prevalent Malware (AV Comparatives Jan 2017).

Behavior and cloud-powered malware detection
Can detect fast changing malware varietals using behavior monitoring and cloud-powered protection that expedites signature delivery
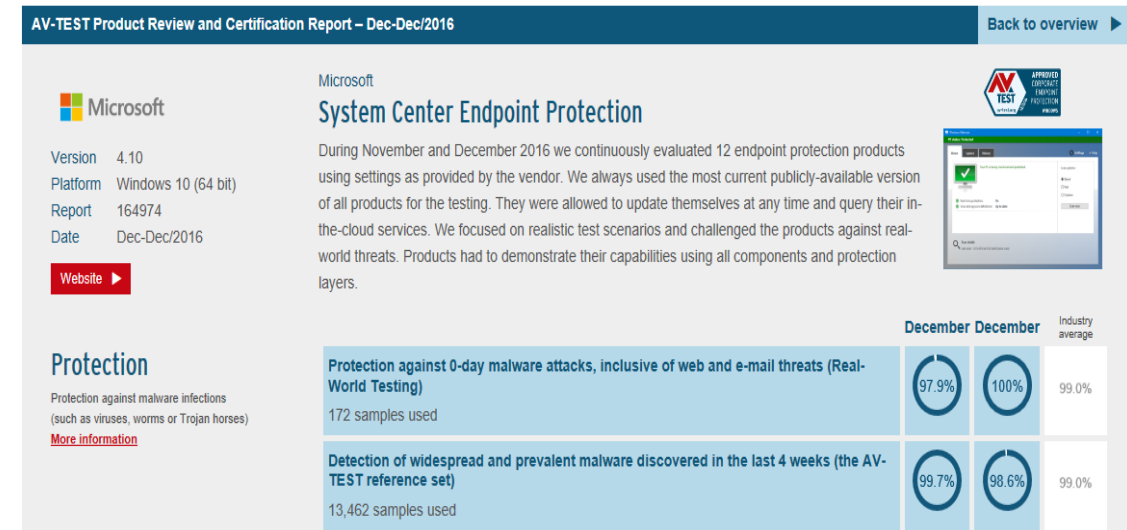
Tamper Resistant
Windows Trusted Boot and platform isolation and protect Windows Defender from attacks and enable it to self-repair

Built into Windows and Always Up-To-Date
No additional deployment & Infrastructure. Continuously up-to-date, lower costs

The best antivirus software for Windows Client Business User

AV-TEST Product Review and Certification Report – Dec-Dec/2016

Back to overview ▶

Microsoft

Microsoft
System Center Endpoint Protection

Version	4.10
Platform	Windows 10 (64 bit)
Report	164974
Date	Dec-Dec/2016

Website ▶

During November and December 2016 we continuously evaluated 12 endpoint protection products using settings as provided by the vendor. We always used the most current publicly-available version of all products for the testing. They were allowed to update themselves at any time and query their in-the-cloud services. We focused on realistic test scenarios and challenged the products against real-world threats. Products had to demonstrate their capabilities using all components and protection layers.

Protection

Protection against malware infections (such as viruses, worms or Trojan horses)

More information

	December	December	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 172 samples used	97.9%	100%	99.0%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 13,462 samples used	99.7%	98.6%	99.0%

WINDOWS DEFENDER INSTANT CLOUD PROTECTION
CLOSING THE TRADITIONAL PROTECTION GAP

Malware's lifecycle is faster than signature based protection can react

Today's Protection is Too Reactive
Most malware achieves economic goal within a few hours
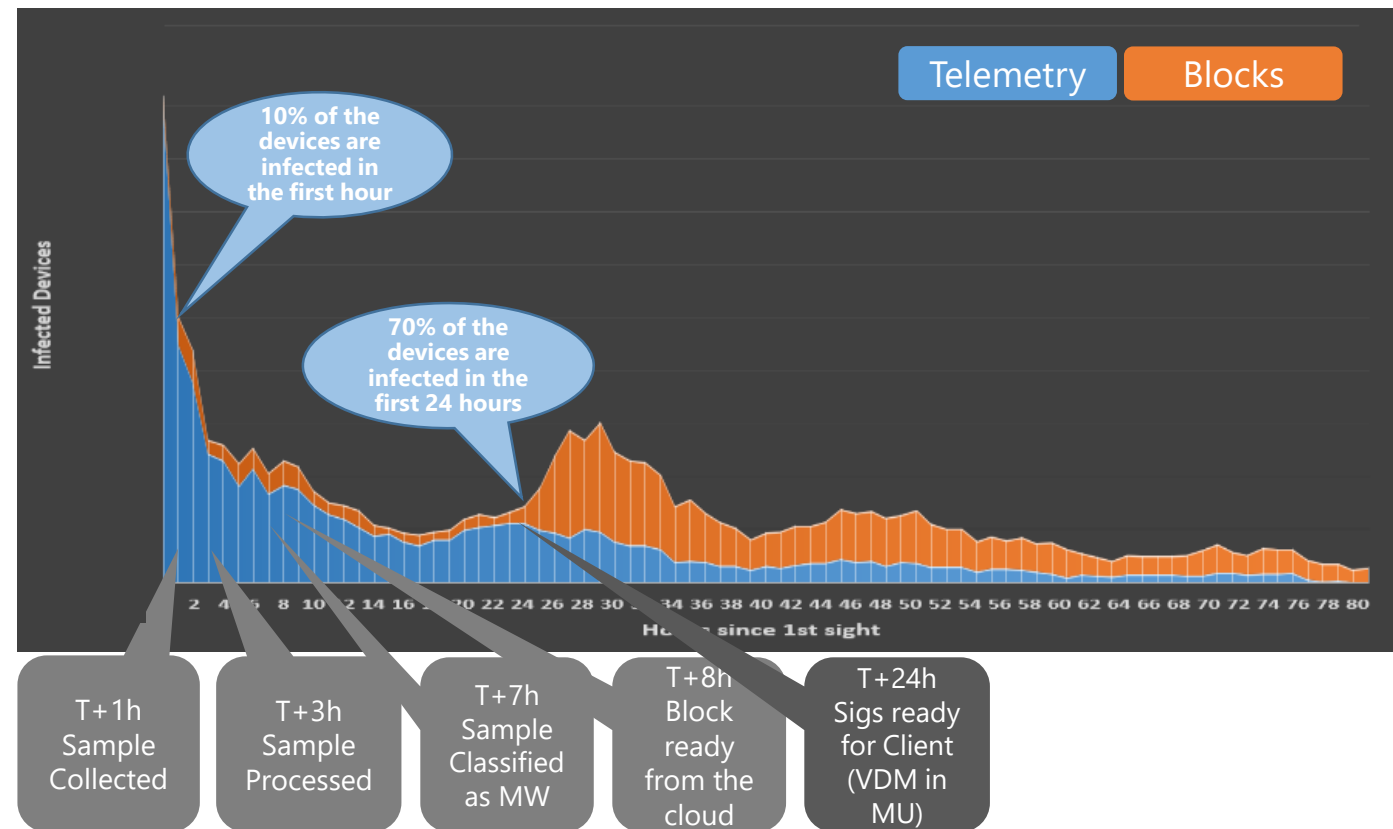
Modern Malware is Polymorphic

90%
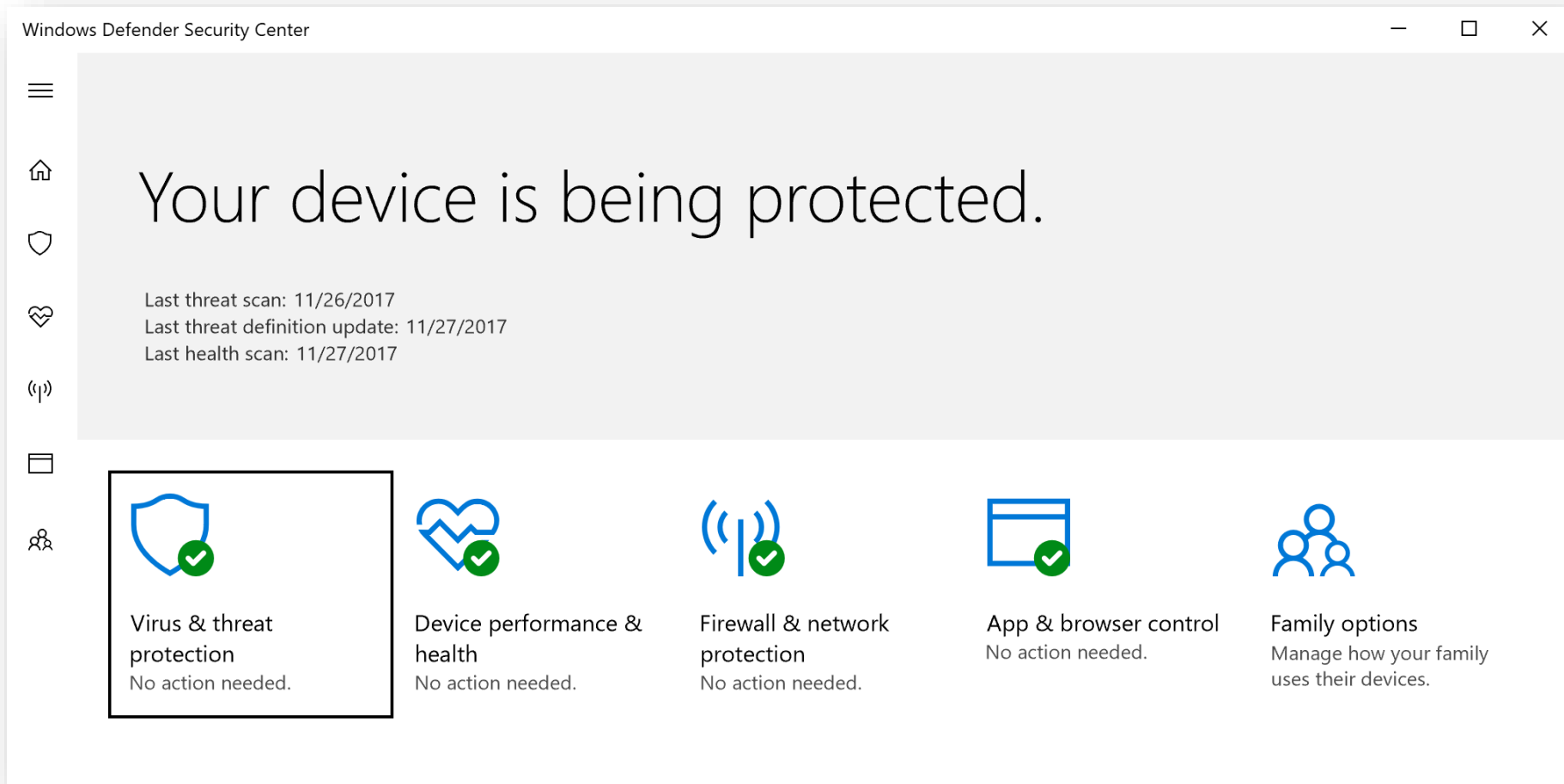**Of the files collected are uniquely handcrafted to each instance**

Block at 1st Sight

Gartner: innovative technology challenging traditional EPPs: 'contain/ hold until found not guilty'

Telemetry | Blocks

10% of the devices are infected in the first hour

70% of the devices are infected in the first 24 hours

Infected Devices

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64 66 68 70 72 74 76 78 80

Hours since 1st sight

T+1h Sample Collected

T+3h Sample Processed

T+7h Sample Classified as MW

T+8h Block ready from the cloud

T+24h Sigs ready for Client (VDM in MU)

WINDOWS DEFENDER ANTIVIRUS
CLOUD-BASED MALWARE PROTECTION

Windows Defender Security Center

Your device is being protected.

Last threat scan: 11/26/2017
Last threat definition update: 11/27/2017
Last health scan: 11/27/2017

Virus & threat protection
No action needed.

Device performance & health
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Family options
Manage how your family uses their devices.

Demo
Windows Defender Antivirus
Block at First Sight
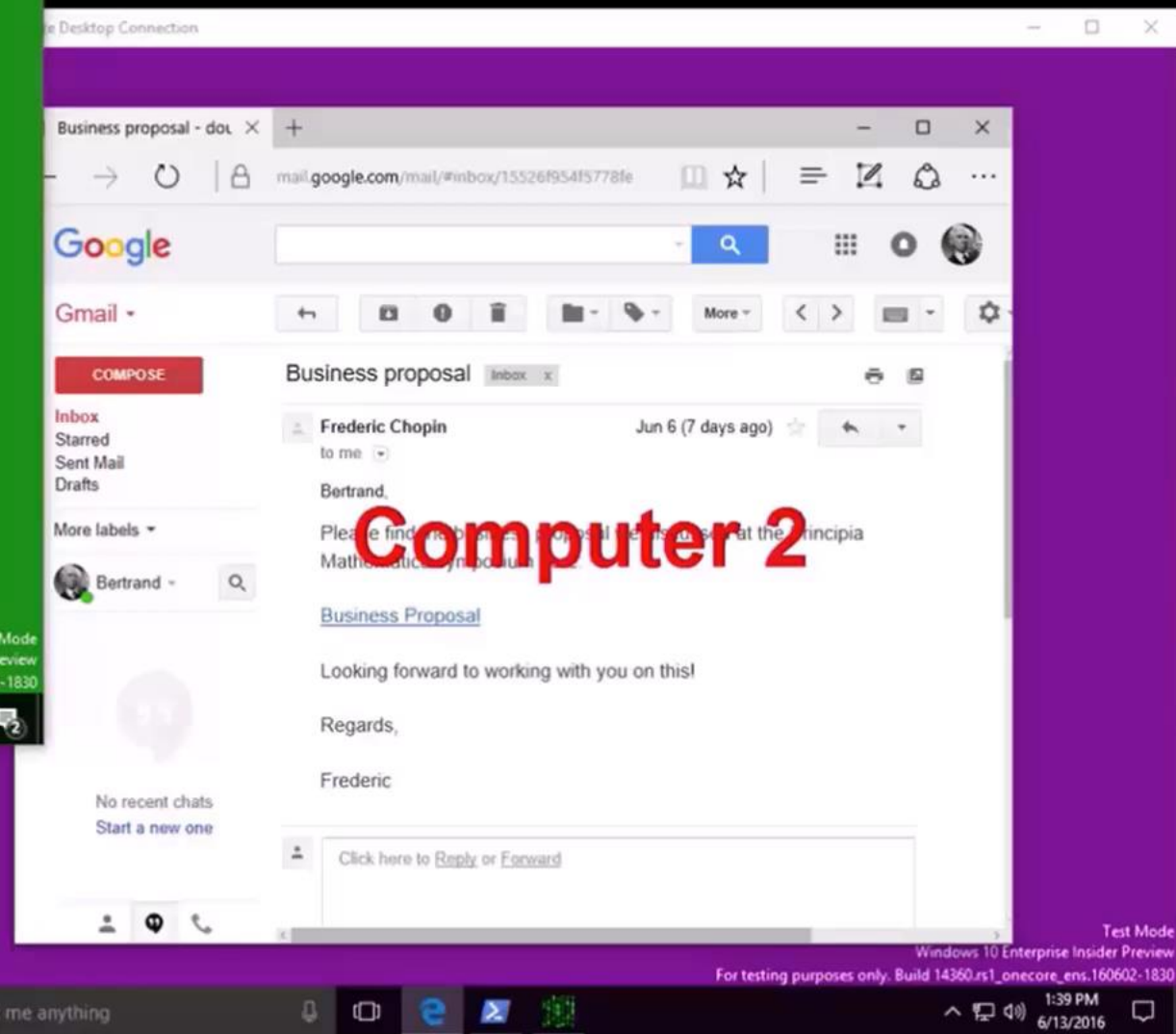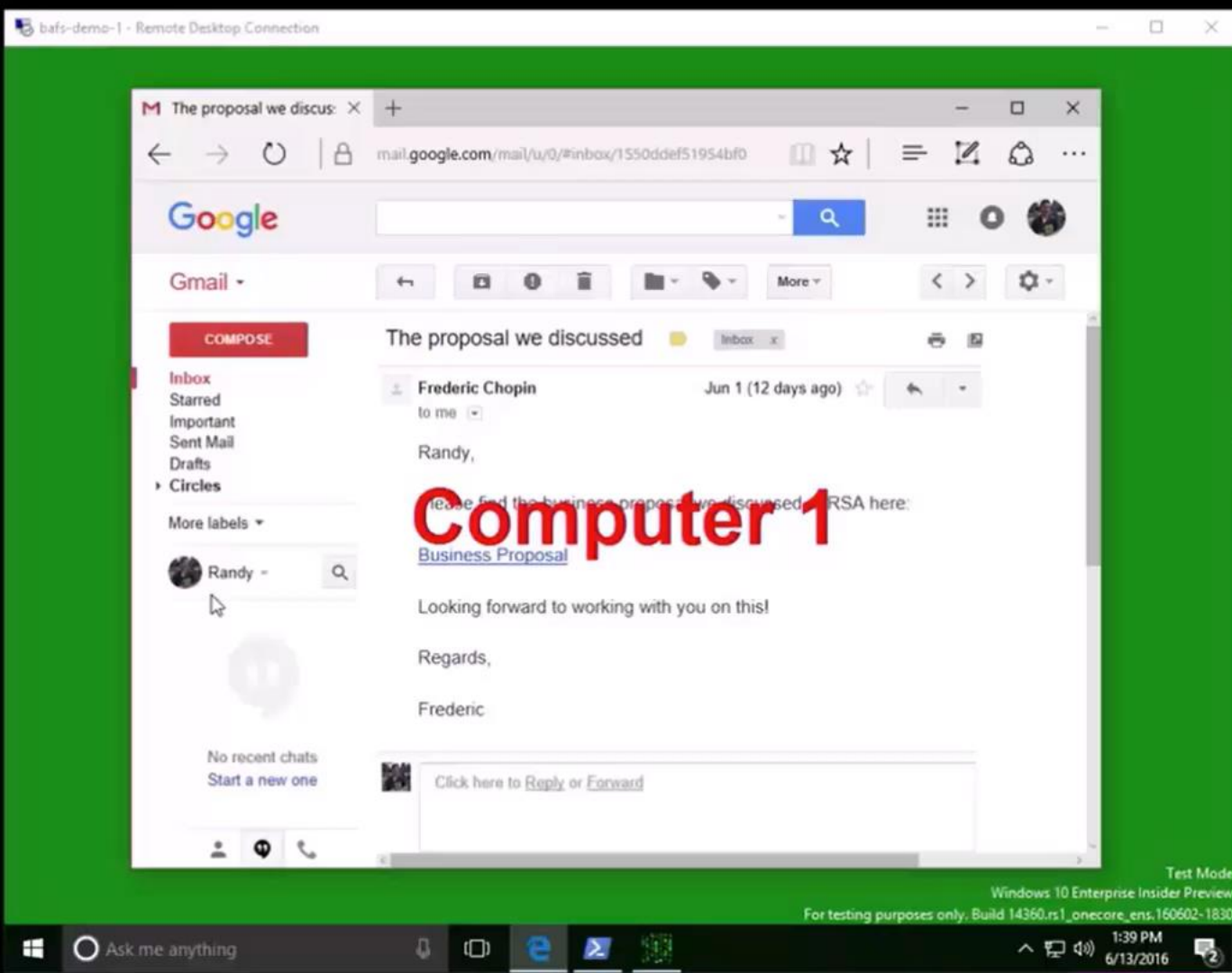
Normal looking website
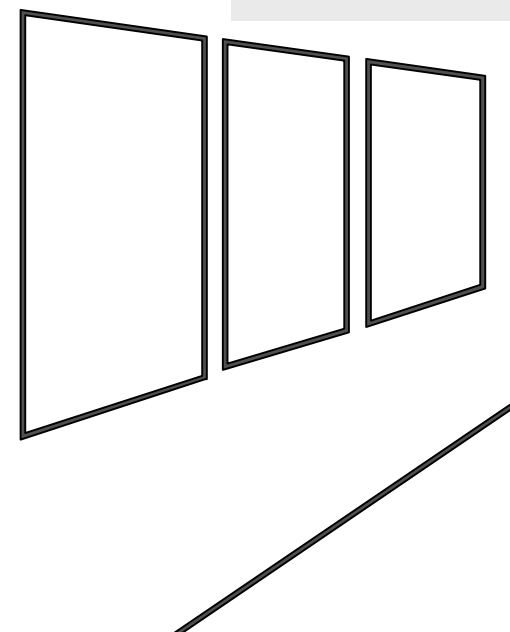
VIRTUALIZATION BASED SECURITY

Windows Defender Application Guard uses VBS to hardware isolate Microsoft Edge

Microsoft Edge

Windows Platform Services

Kernel

Windows Defender Application Guard

Apps

Windows Platform Services

Kernel

Operating System

Critical System Processes

Kernel

System Container

Device Hardware

Hypervisor

Demo
Windows Defender
Application Guard

Windows Defender Application Guard protects by hard isolating all internet activity away from the device when using Microsoft Edge.

CONTROLLED FOLDER ACCESS

Stops ransomware by preventing unauthorized access to your important files

Windows Defender Security Center

Controlled folder access

Protect your files and folders from unauthorized changed by unfriendly applications.

[On]

Protected folders
Allow an app through Controlled folder access

Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

Add or remove exclusions

Windows Defender Security Center

Protected folders

Windows system folders are protected by default. You can also add additional protected folders.

[+] Add a protected folder

MyImportantDocuments
D:\MyImportantDocuments

Documents
C:\Users\█████\Documents

Documents
C:\Users\Public\Documents

Pictures
C:\Users\█████\Pictures

Pictures
C:\Users\Public\Pictures

Videos
C:\Users\Public\Videos

Videos
C:\Users\█████\Videos

Music
C:\Users\█████\Music

Music
C:\Users\Public\Music

Desktop
C:\Users\█████\Desktop

Desktop
C:\Users\Public\Desktop

Favorites
C:\Users\█████\Favorites

🛡 **Virus & threat protection**

Unauthorized changes blocked
Controlled Folder Access blocked C:\Users\av\...\cerber.exe from making changes to the folder █████████\Desktop

Windows 10

YOUR LAST LINE OF DEFENSE WHEN EVERYTHING ELSE FAILS

BACKUP, BACKUP, BACKUP

CLOUD DRIVE
Protect your files with OneDrive for Business

Introducing **Files Restore**
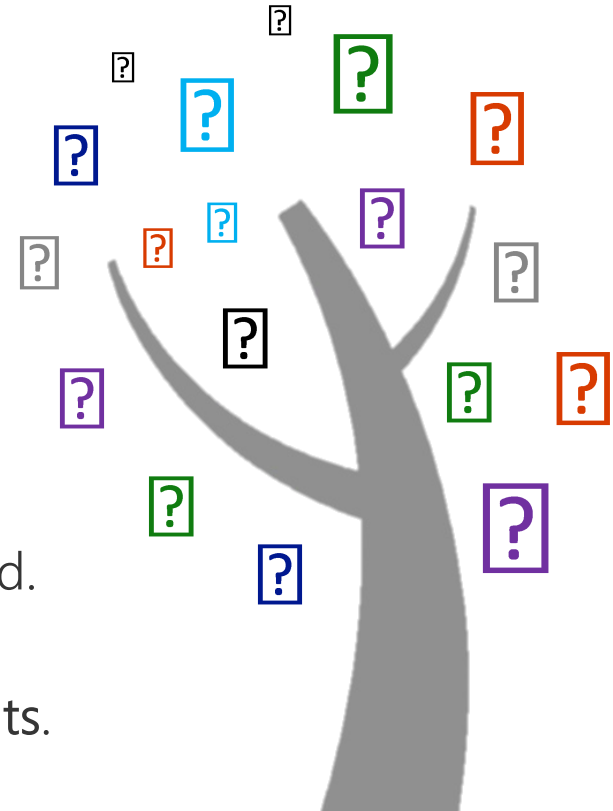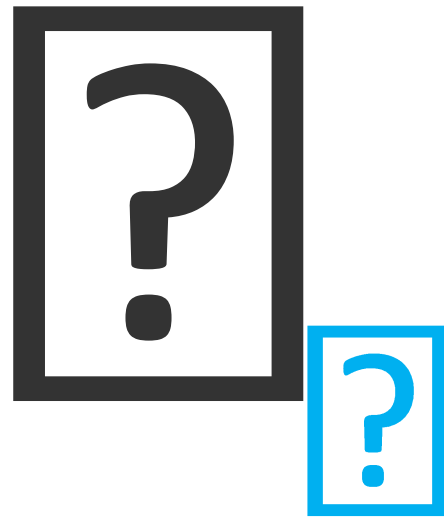
Allowing **self service recovery** for the **last 30 days** up to the second.

Recover from **accidental deletes**, **corruption**, or **ransomware events**.

Randy Wong

Restore my OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Choose a preset or select custom date and time and Restore. To restore your entire OneDrive to a custom time, use the slider to find a date with unusual activity in the chart. Then select a file change that you want to restore you OneDrive up to.

Date presets

| Today ▼ | Restore |

| 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 0 |

Days ago
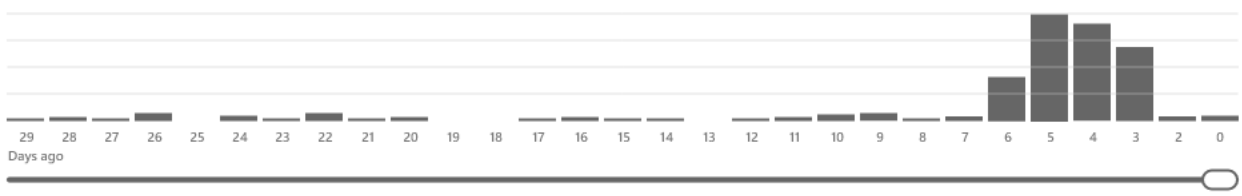
	Change ↓	File name
○ ∧	Today 9/24/2017 (30)	
○ ↑	Uploaded by Kat Larson 11:19:03 AM	Next Generation V1 > Next Gen V1hacked
○ ↑	Uploaded by Kat Larson 10:29:03 AM	Next Generation V1
○ ↑	Uploaded by Kat Larson 10:20:03 AM	Pipeline Gasworks Diagram
○ ↑	Uploaded by Kat Larson 10:19:03 AM	Worchestershire Initiative
○ ✎	Edited by Razeena Javan 9:51:03 PM	Buffer API Docs
○ ⊟	Renamed by Leon Hristova 6:01:03 PM	Buffer APIs > Buffer API Docs
○ ✎	Edited by Nedelya Schroder 4:37:19 PM	Important paper
○ ✎	Edited by Tahel Hasanov 3:34:03 PM	Brainstorms
○ ✎	Edited by Kat Larson 1:08:03 PM	Brainstorms
○ 🗑	Deleted by Arshagouhi Asef zade 11:34:03 AM	Native Juices Project
○ ⊟	Renamed by Franz Schmitt 11:11:23 AM	Next Gen > Next Generation V1
○ ↑	Uploaded by Franz Schmitt 9:40:08 AM	Sycamore Proposal
○ +	Created by Elsa Angelovaa 7:11:23 AM	Trigon Business Designs
○ ⊟	Renamed by Kat Larson 3:34:03 AM	2017 Budget
○ ⊟	Renamed by Kat Larson 3:34:03 AM	CY17 Sales Figures-North America
○ ⊟	Renamed by Kat Larson 3:34:03 AM	Contoso Insulin Pants schematics

Search

Randy Wong

Files

Recent

Shared with me

Discover

Recycle bin

Contoso +

Groups bring teams together. Join one or create your own.

Restore my OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Choose a preset or select custom date and time and Restore. To restore your entire OneDrive to a custom time, use the slider to find a date with unusual activity in the chart. Then select a file change that you want to restore you OneDrive up to.

Date presets

| Custom date and time ⌄ | Restore |

29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 0
Days ago

	Change ↓	File name
○ ⌃	6 days ago 9/18/2017 (40020)	
☑	Renamed by Kat Larson 3:34:03 AM	WE23435EWRTRT.WNCRY
☑	Deleted by Kat Larson 3:34:04 AM	Next Generation V1
☑	Deleted by Kat Larson 3:34:05 AM	Pipeline Gasworks Diagram
○	Uploaded by Kat Larson 10:19:03 AM	Worchestershire Initiative
○	Edited by Razeena Javan 9:51:03 PM	Buffer API Docs
○	Renamed by Leon Hristova 6:01:03 PM	Buffer APIs > Buffer API Docs
○	Edited by Nedelya Schroder 4:37:19 PM	Important paper
○	Edited by Tahel Hasanov 3:34:03 PM	Brainstorms
○	Edited by Kat Larson 1:08:03 PM	Brainstorms
○	Deleted by Arshagouhi Asef zade 11:34:03 AM	Native Juices Project
○	Renamed by Franz Schmitt 11:11:23 AM	Next Gen > Next Generation V1
○	Uploaded by Franz Schmitt 9:40:08 AM	Sycamore Proposal
○	Created by Elsa Angelovaa 7:11:23 AM	Trigon Business Designs
○	Renamed by Kat Larson 3:34:03 AM	2017 Budget
○	Renamed by Kat Larson 3:34:03 AM	CY17 Sales Figures-North America
○	Renamed by Kat Larson 3:34:03 AM	Contoso Insulin Pants schematics

OneDrive admin

Get the OneDrive apps

Return to classic OneDrive

Randy Wong

Search

Randy Wong

Files

Recent

Shared with me

Discover

Recycle bin

Contoso

Groups bring teams together.
Join one or create your own.

OneDrive admin

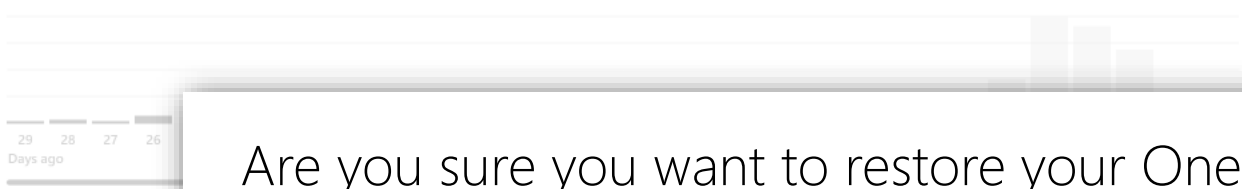Get the OneDrive apps

Return to classic OneDrive

Restore my OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find
a date with unusual activity in the chart. Then select the changes that you want to undo.

Date presets

Custom date and time ⌄   Restore

29   28   27   26
Days ago

Change

6 days

Renamed

Deleted by

Deleted by

Are you sure you want to restore your OneDrive?

Restoring your OneDrive to 8/12/2017 3:49:02 PM will revert 2300 changes.

Restore   Cancel

Uploaded by Kat Larson 10:19:03 AM   Worchestershire Initiative

Edited by Razeena Javan 9:51:03 PM   Buffer API Docs

Renamed by Leon Hristova 6:01:03 PM   Buffer APIs > Buffer API Docs

Edited by Nedelya Schroder 4:37:19 PM   Important paper

Edited by Tahel Hasanov 3:34:03 PM   Brainstorms

Edited by Kat Larson 1:08:03 PM   Brainstorms

Deleted by Arshagouhi Asef zade 11:34:03 AM Native Juices Project

Renamed by Franz Schmitt 11:11:23 AM   Next Gen > Next Generation V1

Uploaded by Franz Schmitt 9:40:08 AM   Sycamore Proposal

Created by Elsa Angelovaa 7:11:23 AM   Trigon Business Designs

Renamed by Kat Larson 3:34:03 AM   2017 Budget

Renamed by Kat Larson 3:34:03 AM   CY17 Sales Figures-North America

Renamed by Kat Larson 3:34:03 AM   Contoso Insulin Pants schematics

CLOUD BACKUP
Backup your files with Azure Backup - Recovery Services vault

Confirmation

Getting started
Select Items to Backup
Specify Backup Schedule
Select Retention Policy
Choose Initial Backup Type
Confirmation
Modify Backup Progress

You are about to save the following backup schedule:

Backup items:	Selected files (C:\)
File(s) Excluded:	None
Backup Time:	10:30 AM
Backup Days:	Everyday
Initial Backup Creation	Network

ⓘ Microsoft Azure Backup has a limit of 54400 GB per volume of data that can be backed up in one Backup operation.

Recover Data Wizard ✕

Select Volume and Date

Getting Started
Select Recovery Mode
Select Volume and Date
Browse And Recover Files

Select the volume: C:\

Available backups
Oldest available backup: 11/26/2017 9:40 PM
Newest available backup: 11/26/2017 9:40 PM

Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

Backup date: 11/26/2017

◄   November 2017   ►

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Time: 9:40 PM

ⓘ Clicking 'Mount' will mount the selected recovery point as a volume. This might take a few minutes.

< Previous   Next >   Mount   Cancel

Favorites

File   Home   Share   View

This PC > CB-{3335A207-9BB5-4F8D- (D:) > Users > andyfung > Favorites

Name	Date modified
Favorites Bar	11/14/2017 10:30 AM
Bing	11/13/2017 5:52 PM
ITWeb (Microsoft IT)	11/13/2017 5:52 PM
MSW (Microsoft Web)	11/13/2017 5:52 PM
My Microsoft IT	11/13/2017 5:52 PM
Opportunities My Accounts Opportunities - ...	10/12/2017 5:21 PM

Quick access
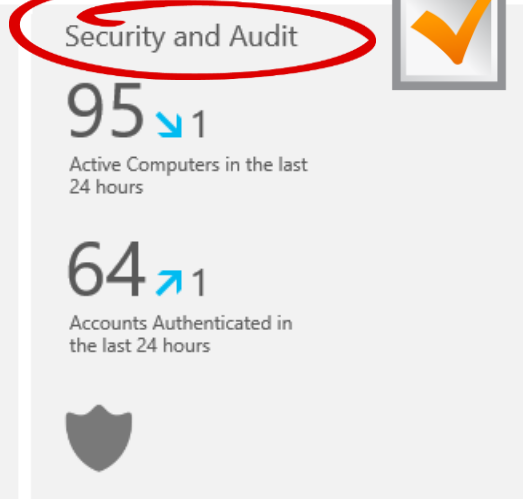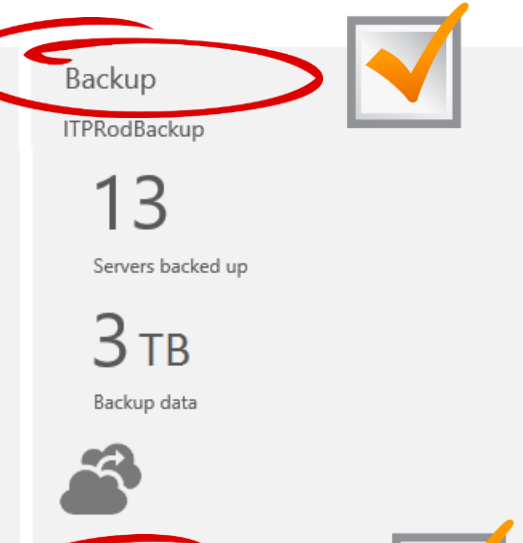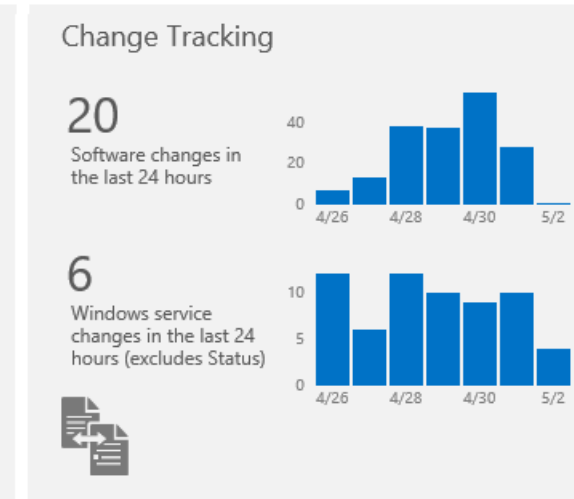 Desktop
  Downloads
  Documents
  Pictures
CB-{3335A207-9BB5-4F8D- (D:)
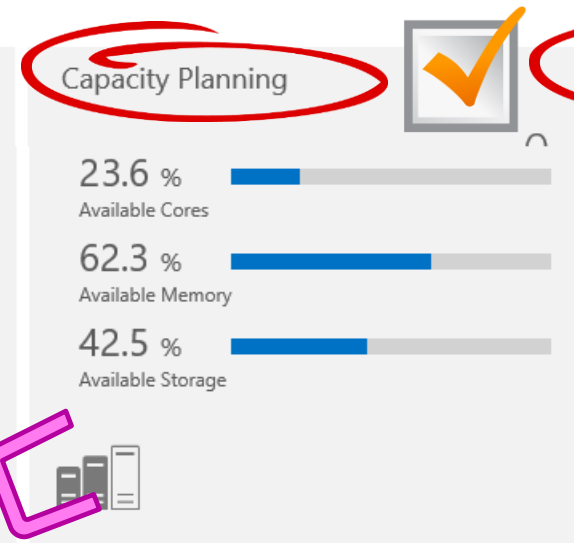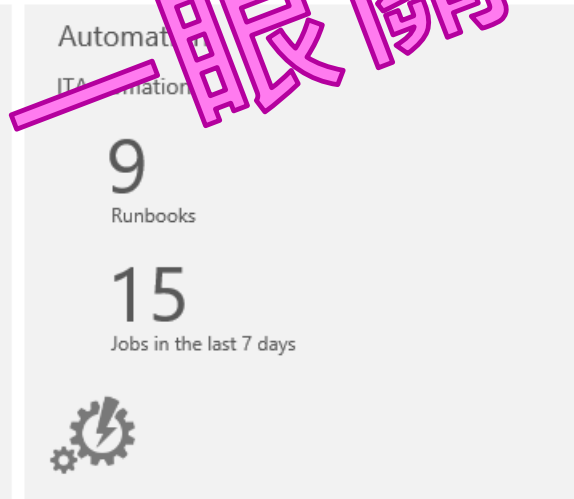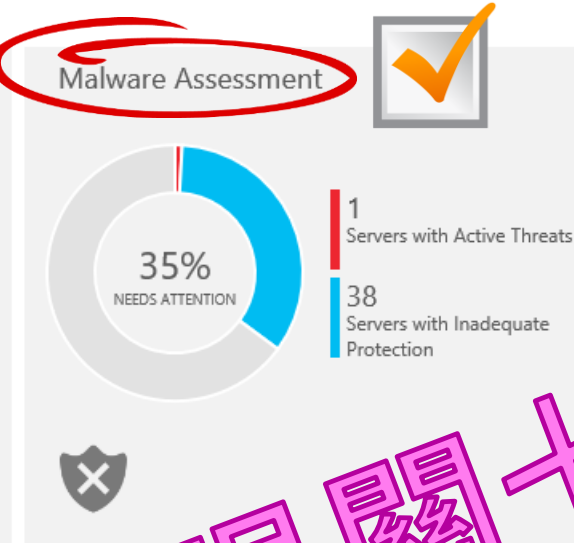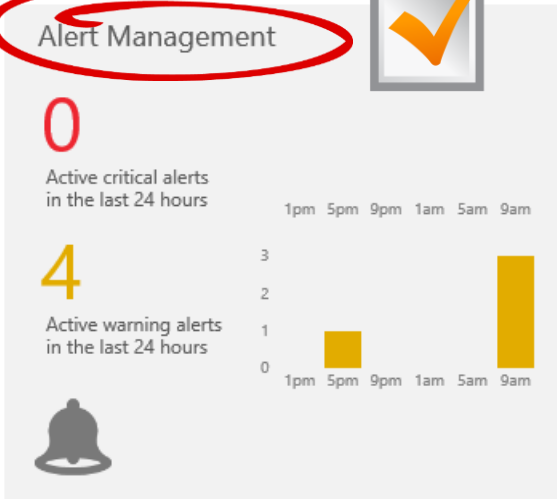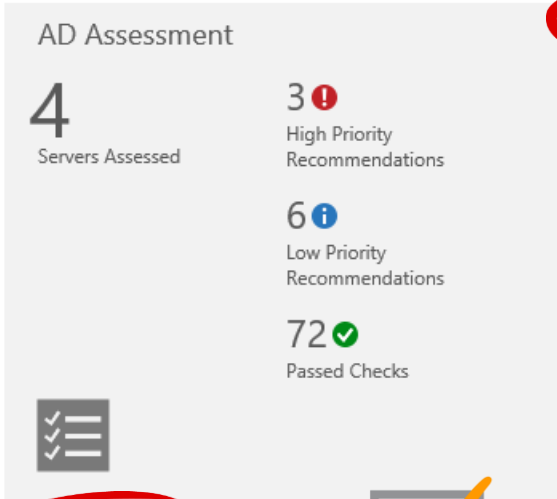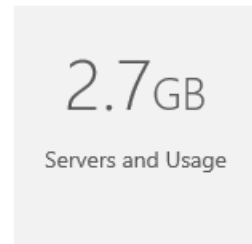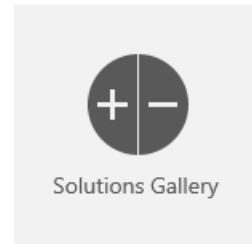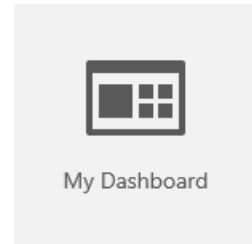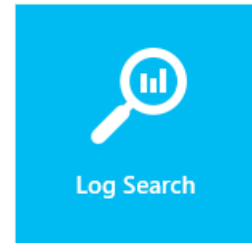
One Microsoft Cloud Solutions

免費服務
出沒注意

- Multi-user access
- Subject/Project Site
- 1TB + 0.5GB x # subscribed users

- Single access
- Files sharing
- 5TB per user

- In-campus Video Streaming Service
- 500GB + 0.5GB x # subscribed users

Trusted Cloud Services from Storage, Management to Data-driven Insights

SharePoint

OneDrive

Stream

Azure

Office365 Education

Free

Paid Services

Case Study – Full Cloud Adoption

Sample School 1 | Scope : **Full Cloud Adoption**

Phase 1

| File Server | Domain Server | Site-to-Site VPN |
| Cloud Backup for Servers | OMS | O365 |

Phase 2

| Single Sign On | Student Analytics |

Case Study – Partial System

Sample School 2 Scope : **Partial System**

Phase 1

Web Server

Cloud Backup for Servers

Cloud Backup for Critical Machine

Phase 2

Student Analytics

OUR JOURNEY TO SAFER PLACE – CLOUD

→ Fast Delivery in <u>Five</u> Weeks

5th Week

4th Week
Deployment
&
Migration

2nd Week
Proof of Concept

3rd Week
Final Decision
&
Partner
Engagement

1st Week
Handshaking
&
Understanding

Thank You. Contact Us.

Crystal Lai / a-crlai@microsoft.com / +852 6401 0854