Protection through One Microsoft Cyber Security Platform from Client to Server
Ransomware – Top Families and Attack Vectors

Ransomware encounters by family in 2016

- Cerber, 20%
- Locky, 16%
- Crowti, 12%
- Tescrypt, 11%
- Teerac, 9%
- Teerac, 9%
- Citroni, 6%
- Reveton, 6%
- Exrout, 1%
- Genasom, 2%
- Trolsdh, 2%
- Others, 14%

Office 365 analyzes 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.
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.
Windows Defender Instant Cloud Protection
Closing the Traditional Protection Gap

Malware’s lifecycle is faster than signature based protection can react.

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’

Today’s Protection is Too Reactive
Most malware achieves economic goal within a few hours.

- 10% of the devices are infected in the first hour
- 70% of the devices are infected in the first 24 hours

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)
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
Computer 1

The proposal we discussed

Frederic Chopin
Jun 1 (12 days ago)

Randy,

We need to find the proposal we discussed via RSA here:

Business Proposal

Looking forward to working with you on this!

Regards,

Frederic

Computer 2

Business proposal

Frederic Chopin
Jun 6 (7 days ago)

Bertrand.

Please read the attached Business Proposal.

Mathieu

Bertrand.

Business Proposal

Looking forward to working with you on this!

Regards,

Frederic
VIRTUALIZATION BASED SECURITY

Windows Defender Application Guard uses VBS to hardware isolate Microsoft Edge.
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 10

YOUR LAST LINE OF DEFENSE WHEN EVERYTHING ELSE FAILS

BACKUP, BACKUP, BACKUP
Introducing **Files Restore**

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

Recover from accidental deletes, corruption, or ransomware events.
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 your OneDrive up to.

Date presets

Today

Change ↓  File name

- Today 9/24/2017 (30)
- Uploaded by Kat Larson 11:19:03 AM  Next Generation V1 > Next Gen V1 hacked
- Uploaded by Kat Larson 10:29:03 AM  Next Generation V1
- Uploaded by Kat Larson 10:20:09 AM  Pipeline Gasworks Diagram
- Uploaded by Kat Larson 10:19:03 AM  Worcestershire Initiative
- Edited by Ranvir Javan 9:51:03 PM  Buffer API Docs
- Renamed by Leon Hristov 6:01:03 PM  Buffer APIs > Buffer API Docs
- Edited by Netalya Schreder 4:37:19 PM  Important paper
- Edited by Tahl Haasnov 3:34:03 PM  Brainstorms
- Edited by Kat Larson 1:08:03 PM  Brainstorms
- Deleted by Anshagoki Azev 3:34:03 PM  Native Juices Project
- Renamed by Franz Schmitt 11:11:21 AM  Next Gen > Next Generation V1
- Uploaded by Franz Schmitt 9:40:06 AM  Sycomore Proposal
- Created by Eta Angelinas 7:11:23 AM  Triggan Business Designs
- Returned by Kat Larson 3:34:03 AM  2017 Budget
- Returned by Kat Larson 3:34:03 AM  CY17 Sales Figures North America
- Returned by Kat Larson 3:34:03 AM  Contoso Insulin Parts schematics
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 your 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 1 0

Days ago

Change ↓         File name

6 days ago 9/18/2017 (40020)

Renamed by Kat Larson 3:34:03 AM    WM23456WRTY1112R

Deleted by Kat Larson 3:40:04 AM    Next Generation V1

Deleted by Kat Larson 3:40:05 AM    Pipeline Gasworks Diagram

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

Edited by Razzaro Javer 9:51:00 PM    Buffer API Docs

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

Edited by Neelolaya Schneder 4:37:19 PM    Important paper

Edited by Tafel Hasenow 3:34:03 PM    Brainstorms

Edited by Kat Larson 1:08:03 PM    Brainstorms

Deleted by Arshagholu Aalif jade 11:34:06 AM    Native Juices Project

Renamed by Franz Schmilt 1:11:21 AM    Next Gen > Next Generation V1

Uploaded by Franz Schmilt 9:40:08 AM    Sysmore Proposal

Created by Elsa Angelica 7:11:23 AM    Strigon Business Designs

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

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

Edited by Kat Larson 3:34:03 AM    Contoso Insulin Pumps schematics
Are you sure you want to restore your OneDrive?

Restoring your OneDrive to 8/12/2017 3:49:02 PM will revert 2300 changes.
CLOUD BACKUP
Backup your files with Azure Backup - Recovery Services vault

Microsoft Azure Backup has a limit of 54400 GB per volume of data that can be backed up in one Backup operation.
CLOUD OPERATION
Monitor your IT environment with Operation Management Dashboard
One Microsoft Cloud Solutions

- 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

SharePoint

Office365 Education

Free

Paid Services

Azure

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

- Files sharing
- 5TB per user

- Files sharing
- 5TB per user
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 Five Weeks

1st Week
Handshaking & Understanding

2nd Week
Proof of Concept

3rd Week
Final Decision & Partner Engagement

4th Week
Deployment & Migration

5th Week
Thank You. Contact Us.

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