

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Los secuestradores van a la oficina

Windows vs Ransomware



- Fernando Rubio Román
- Microsoft
- fernando.rubio@microsoft.com

Índice

1. Introducción al Ransomware empresarial
2. Mitigaciones para organizaciones
 - Bloquear los ataques en la primera línea
 - Defensas para contener a los atacantes
 - Copias de seguridad para emergencias

Introducción al Ransomware





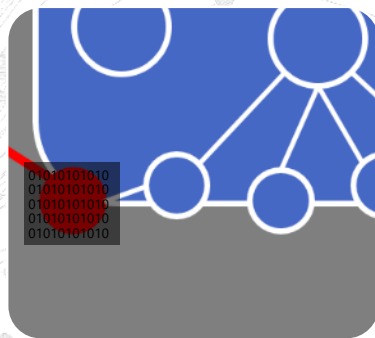
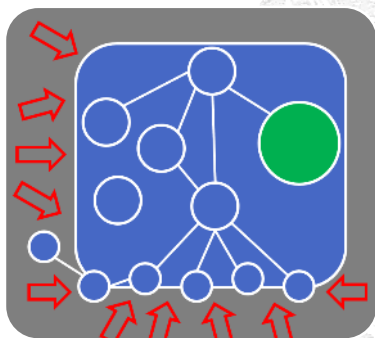
Nuestro análisis nos hace esperar mayor actividad de ransomware a lo largo de 2018 (nuevos atacantes, menor coste por la automatización...)

Modus operandi

- Tomar activos digitales personales y empresariales como rehenes usando cifrado fuerte.
- Pedir un pago a las victimas a cambio de la clave de descifrado
- Usa técnicas de presión para que las victimas paguen
 - **Datos irrecuperables pasado un tiempo**
 - **Amenaza con publicar la información públicamente**
 - **Amenazas con eliminar todos los datos**
 - **Incrementa la cantidad a pagar según pasa el tiempo**

Ataques de ransomware de una sola fase

Único equipo/Usuario impactado



Planear

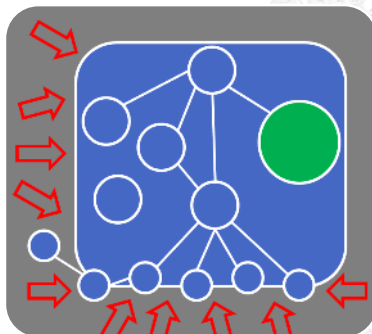
Entrar

Características claves

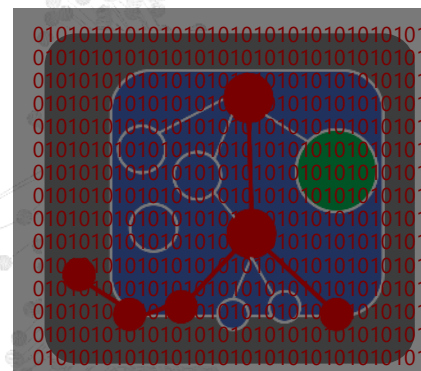
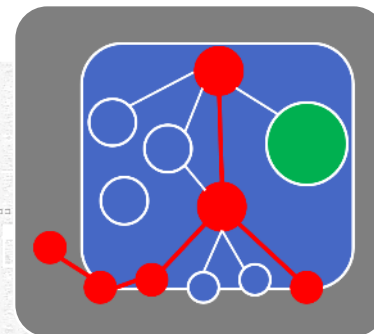
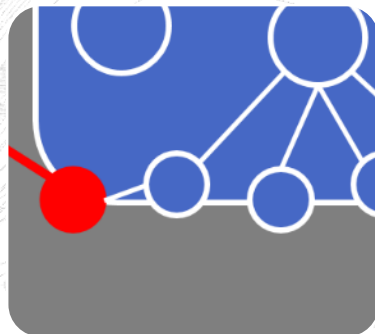
- El correo es el vector primario
 - Adjuntos o enlaces
 - Descargas involuntarias
- Los atacantes usan cifrado fuerte
 - Poca probabilidad de saltarlo
- Encriptación rápida automatizada
 - Los permisos sobre shares pueden convertirlos en una amenaza empresarial

Ataques de ransomware a toda una organización

Impacto a un único usuario/equipo



Impacto a toda la organización



Planear

Entrar

Extender

Cifrar

C&C

Características de los ransomware empresariales

Entrar

Extenderse

Cifrar

- Dos puntos de entrada

- Ataques a estaciones de trabajo
- Servidores en la DMZ vulnerables

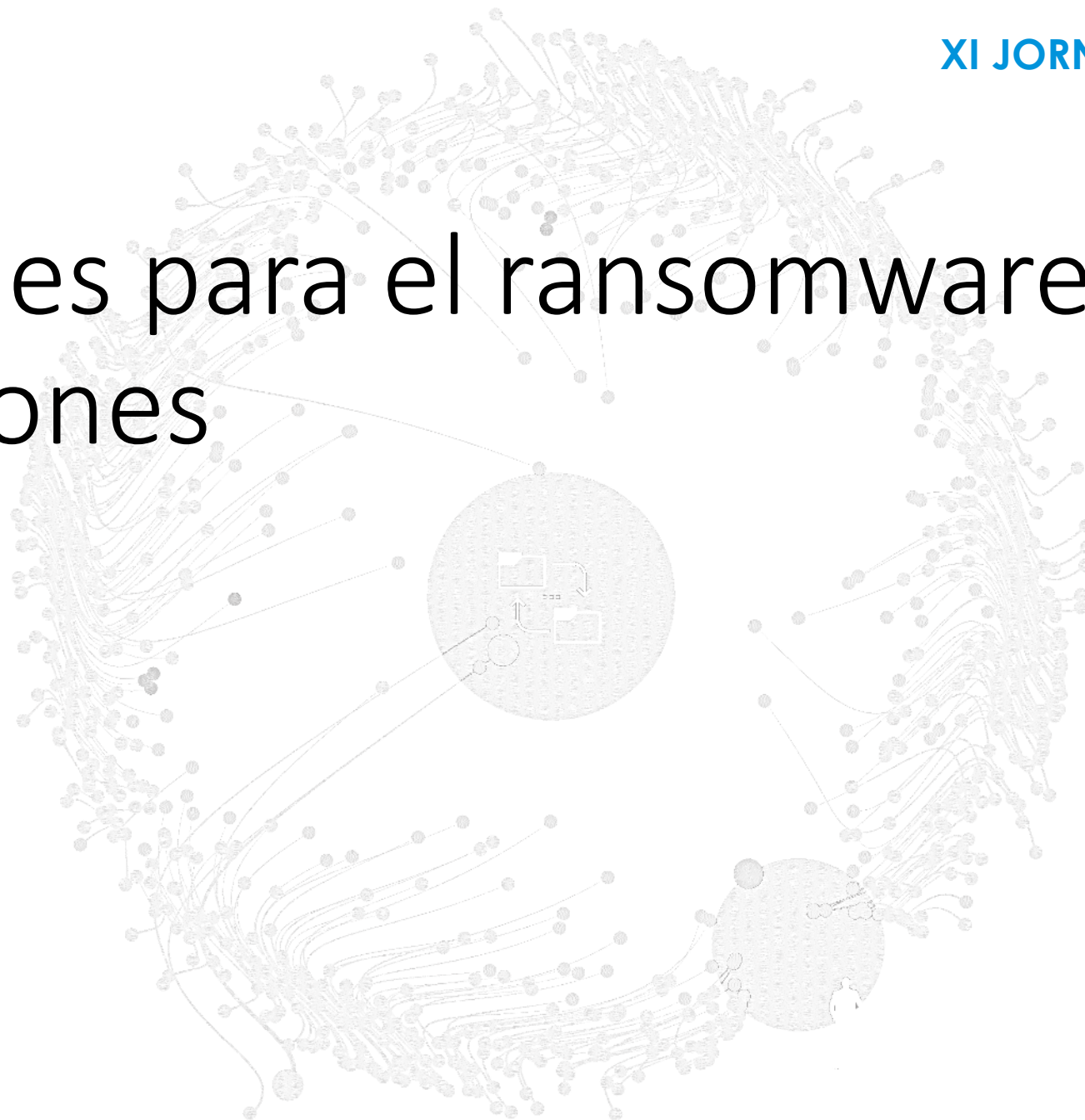
- Similares a los ataques estilo "APT"

- Conseguir claves y contraseñas
- Mapear la red e identificar objetivos

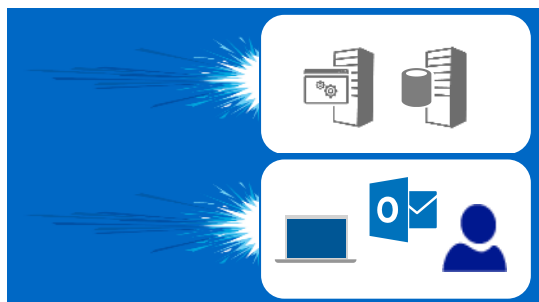
- Los atacantes usan cifrado fuerte

- Si llegan a este punto, los backups offline son la única alternativa

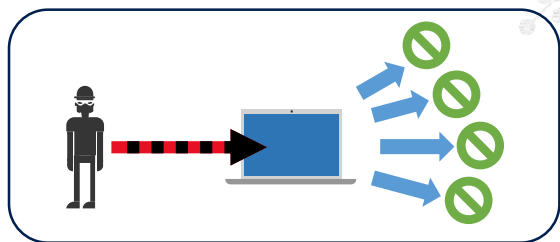
Mitigaciones para el ransomware de organizaciones



Una estrategia pragmática en tres pasos



1. Bloquear los ataques en la primera línea



2. Defensas para contener a los atacantes



3. Backup en caso de emergencia

Defensas primera línea



Defensas para estaciones y usuarios

1. Protecciones del S.O.: Aplicar actualizaciones de seguridad, Applocker, EMET, Windows defender, SmartScreen, Macros firmadas, Exploit Guard...
2. Protecciones para el correo
3. Educación a los usuarios



Defensas para los servidores de internet

1. Aplicar actualizaciones de seguridad
2. Higiene operacional (restringir el uso de credenciales privilegiadas)
3. Higiene en la configuración (Cambiar contraseñas, aplicar hardening)

Defensas en la primera línea

Device Health
attestation
Device Guard
Device Control
Security policies

Protección de
dispositivos

Built-in 2FA
Account lockdown
Credential Guard
Microsoft Passport
Windows Hello ;)

Protección de la
identidad

Device protection /
Drive encryption
Enterprise Data
Protection
Conditional access

Protección de la
información

SmartScreen
AppLocker
Device Guard
Windows Defender
Network/Firewall

Resistencia a
amenazas

Windows Defender
ATP

Detección, investigación y
respuesta a amenazas

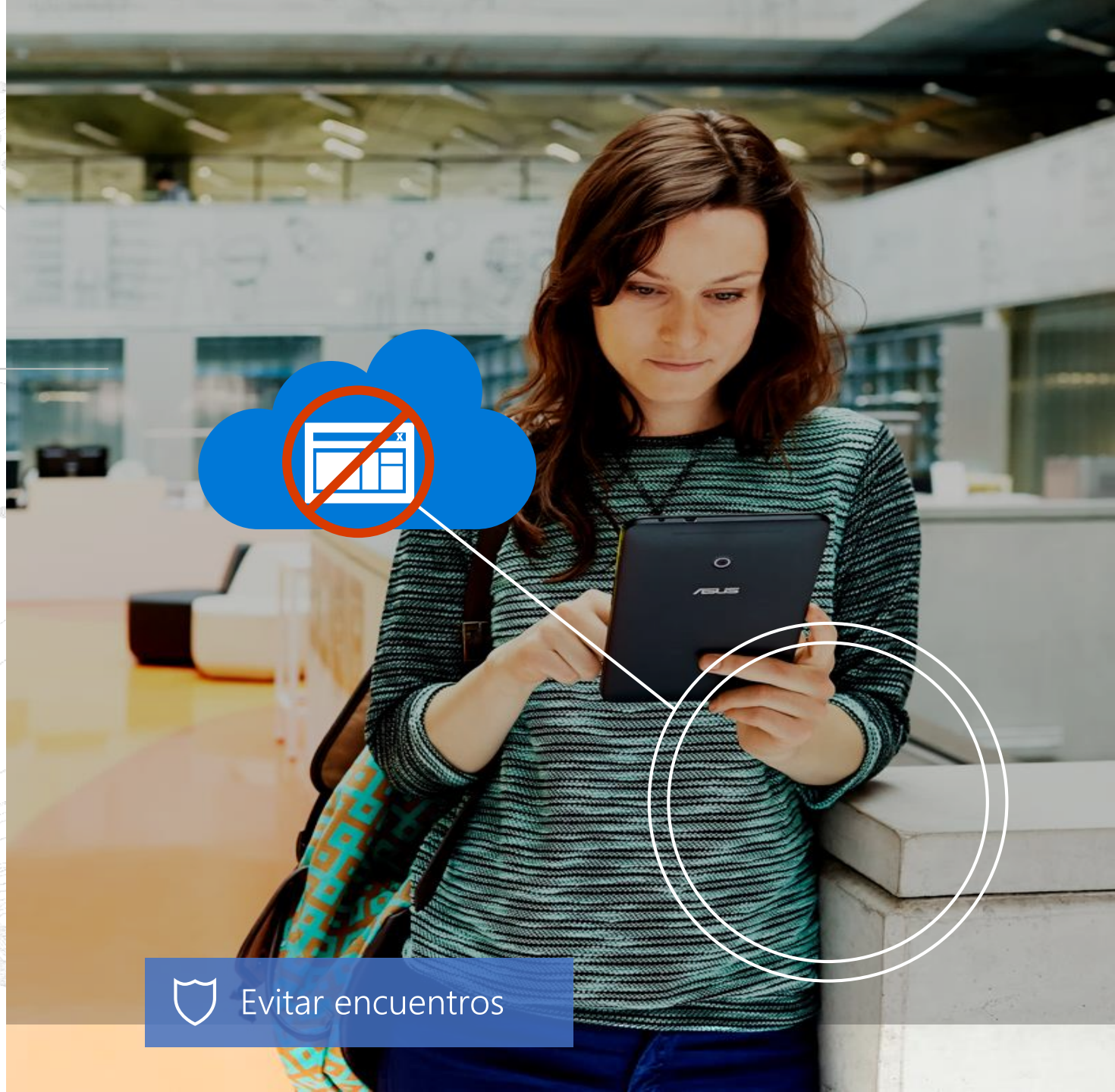
Windows Defender SmartScreen

Usar el poder del **grafo de seguridad inteligente** para evitar encuentros

Tecnología de filtrado de Phishing y malware para Microsoft Edge e Internet Explorer 11

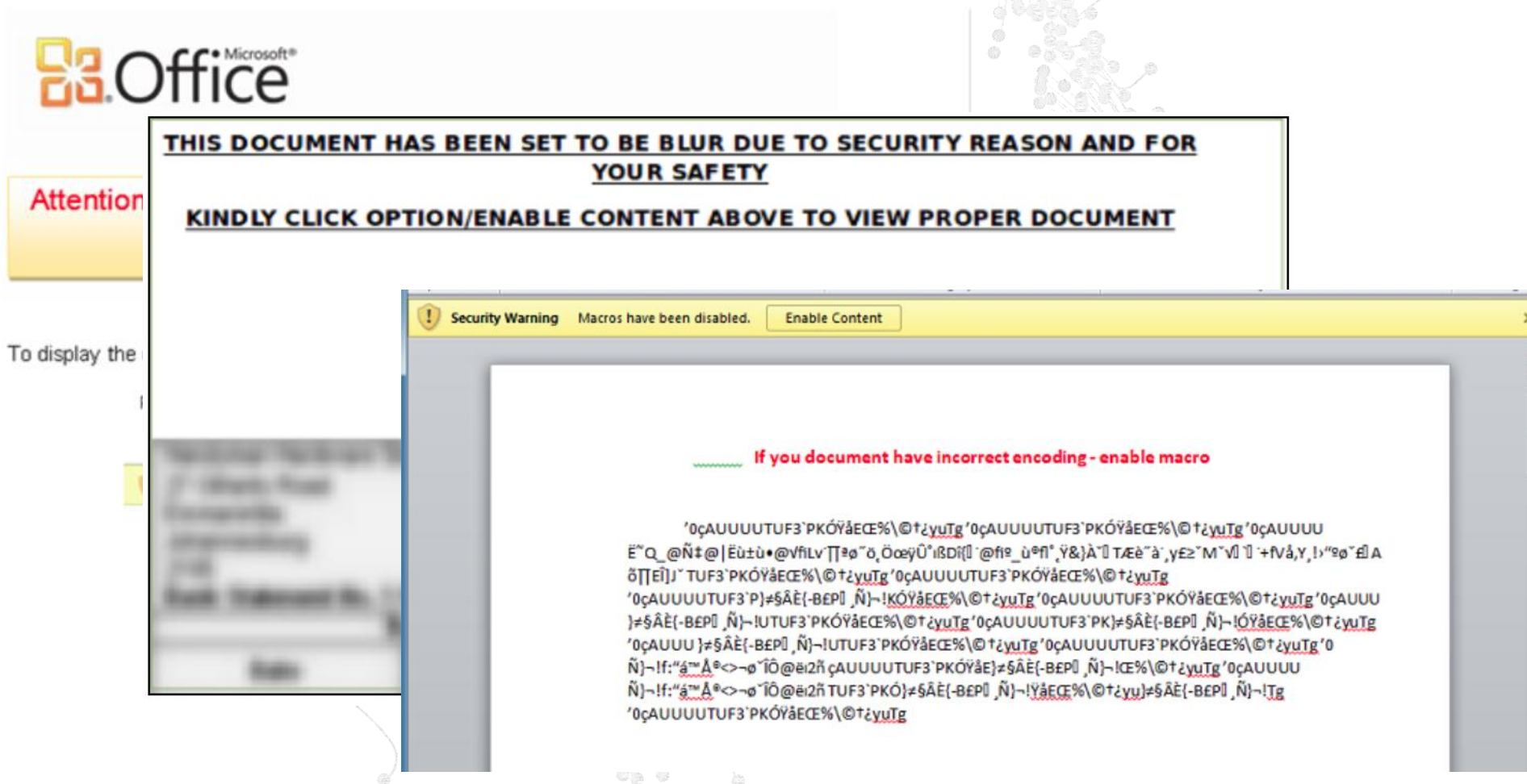
Proporciona protección para las descargas accidentales

El servicio en la nube es actualizado continuamente, sin nada que desplegar



Evitar encuentros

¿Por qué necesitamos macros firmadas?



Windows Defender Exploit Guard

Prevención de ejecución avanzada (HIPS)

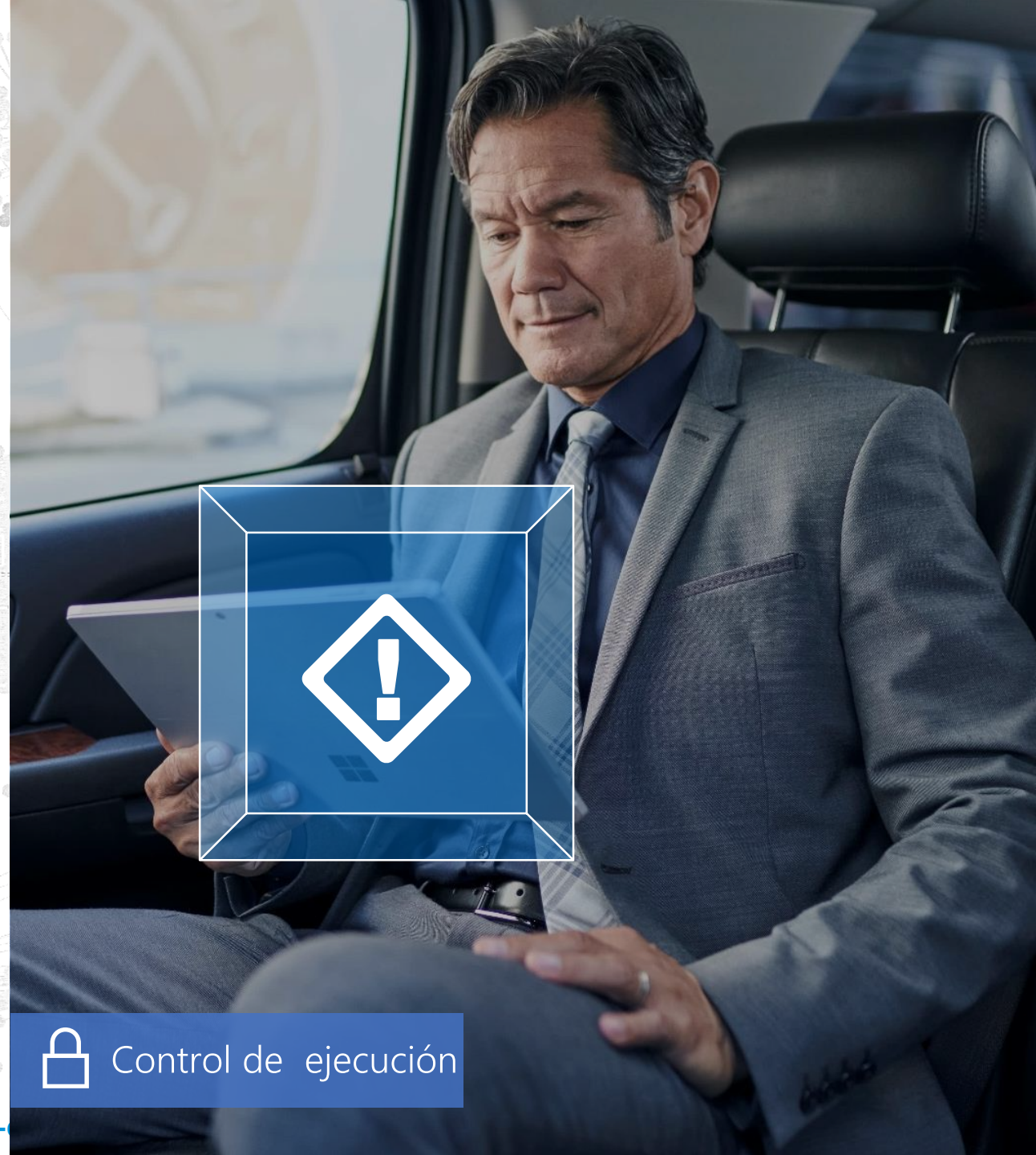
Mitiga vulnerabilidades al hacerlas menos explotables con
Exploit Protection

Bloquea intrusiones al reducir superficie de ataque con
surface area reduction (ASR)

Protege carpetas sensibles de procesos no autorizados
con controlled folder access

Extiende la protección de la red de SmartScreen a
cualquier otra aplicación con **network protection**

Permite a los equipos de seguridad establecer
mitigaciones anti-exploit personalizadas



Control de ejecución

Exploit Protection Mitigations

- Arbitrary Code Guard (ACG)
- Block Low Integrity Images
- Block Remote Images
- Block Untrusted Fonts
- Control Flow Guard (CFG)
- Code Integrity Guard
- Data Execution Prevention (DEP)
- Disable Extension Points
- Disable Win32k System Calls
- Do Not Allow Child Processes
- Export Address Filtering (EAF and EAF+)
- Import Address Filtering (IAF)
- Force Randomization for Images (Mandatory ASLR)
- Randomize Memory Allocations (Bottom-Up ASLR)
- Simulate Execution (SimExec)
- Validate API Invocation (CallerCheck)
- Validate Exception Chains (SEHOP)
- Validate Handle Usage
- Validate Heap Integrity
- Validate Image Dependency Integrity
- Validate Stack Integrity (StackPivot)

Block executable content from email client and webmail

Block Office applications from creating child processes

Block Office applications from creating executable content

Block Office applications from injecting into other processes

Impede JavaScript and VBScript to launch executables

Block execution of potentially obfuscated scripts

Block Win32 imports from Macro code in Office



Virus & threat protection

Connection blocked

Your IT administrator caused Windows Defender Security Center to block this network connection. Contact your IT help desk.



Windows Defender Security Center



Controlled folder access

Protect your files and folders from unauthorized changes 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](#)



5:18 PM

8/10/2017



Demo: Control de la ejecución

Bloqueando ataques "sin ficheros" con Windows Defender Exploit Guard



Recycle Bin



Type here to search



USB DRIVE (D:)

FileHomeShareViewManage

USB DRIVE (D:)

Search USB DRIVE (D:)

Quick access

Desktop

Downloads

Documents

Pictures

IgniteDemo

Music

Screenshots

Videos

OneDrive

This PC

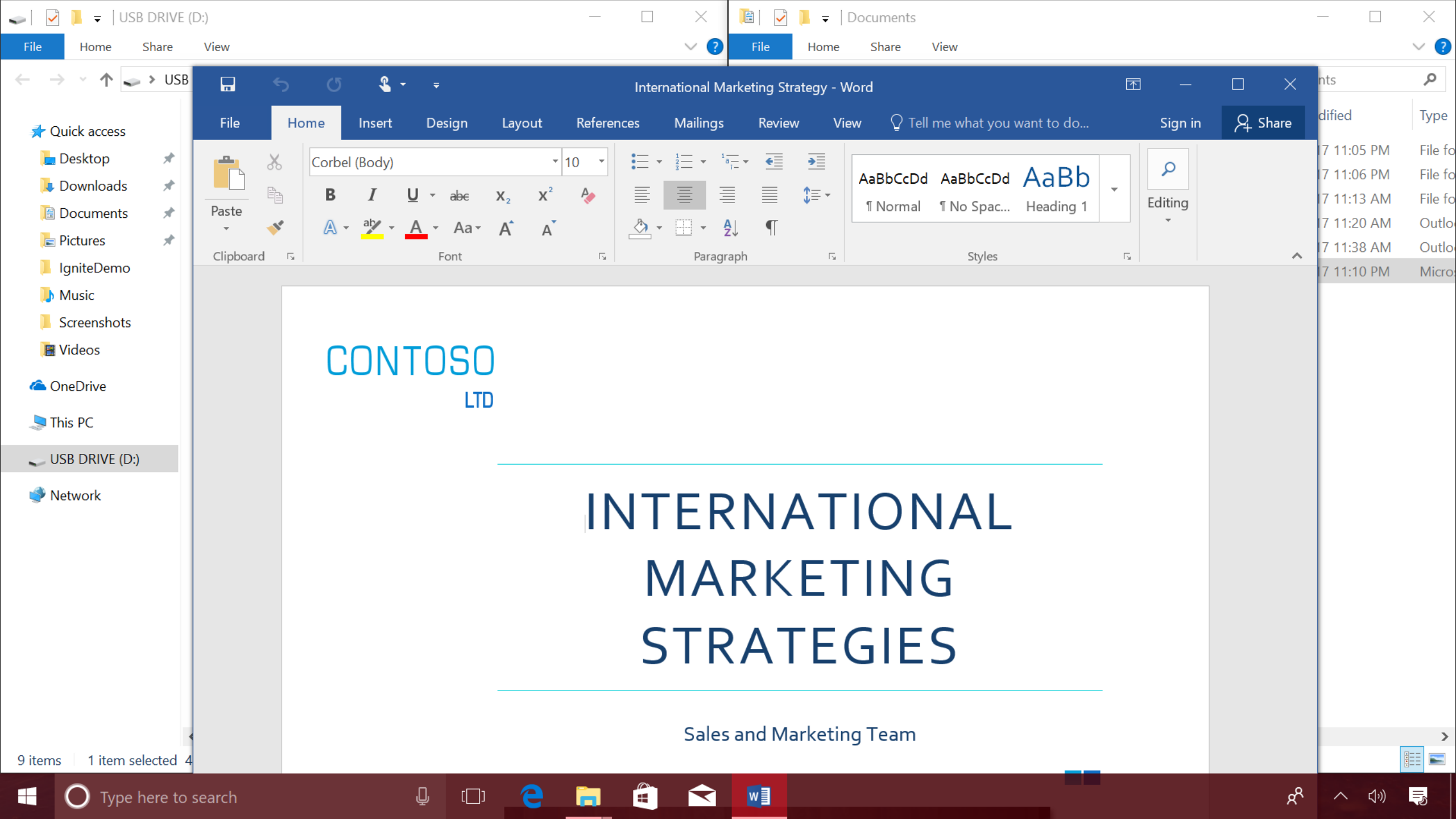
USB DRIVE (D:)

Network

Name	Date modified	Type
European Expansion	9/14/2017 1:51 AM	Micro
International Marketing Strategy	9/14/2017 1:51 AM	Micro
Pricing Guidelines for XT1000	9/14/2017 1:51 AM	Micro
Projected Revenues Northwest and California	9/14/2017 1:51 AM	Micro
Proseware Project Budget Audit	9/14/2017 1:51 AM	Micro
Q3 Sales and Marketing Expense Report Audit	9/14/2017 1:51 AM	Micro
RD And Engineering Costs Q1	9/14/2017 1:51 AM	Micro
RD Expense Report	9/14/2017 1:51 AM	Micro
RD Expenses Q1 to Q3	9/14/2017 1:51 AM	Micro

9 items





C:\demo\help_decrypt.l

file:///C:/demo/help_dec

Your files were .encrypted!

Follow instructions to decrypt your files and pay me bitcoins!



Windows taskbar: Type here to search, microphone, network, Edge, File Explorer, Store, Mail, Word.

Demo

File Home Share View

This PC > Windows (C:) > Demo

Search Demo

Name	Date modified	Type
All Japan Revenues By City.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Annual Financial Report (DRAFT).docx.encrypted!	9/17/2017 10:18 PM	EN
Audit of Small Business Sales.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Contoso Patent App 150219a.docx.encrypted!	9/17/2017 10:18 PM	EN
Contoso Patent Template.docx.encrypted!	9/17/2017 10:18 PM	EN
Contoso Purchasing Data - Q1 - Copy.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Contoso Purchasing Permissions - Confidential....	9/17/2017 10:18 PM	EN
Contoso Purchasing Permissions - Q1.docx.encrypted!	9/17/2017 10:18 PM	EN
Contoso Purchasing Permissions.docx.encrypted!	9/17/2017 10:18 PM	EN
Employee Data - Q1 KJ copy.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Employee Health Accounts - Q3.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Employee Health Accounts.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Employee Travel - Q1.xlsx.encrypted!	9/17/2017 10:18 PM	EN
Employee Travel - Q3.xlsx.encrypted!	9/17/2017 10:18 PM	EN
European Expansion.pptx.encrypted!	9/17/2017 10:18 PM	EN
help_decrypt	9/17/2017 10:18 PM	HT
help_decrypt	9/17/2017 10:18 PM	Di
help_decrypt	9/17/2017 10:18 PM	VB
Pricing Guidelines for XT1000.docx.encrypted!	9/17/2017 10:18 PM	EN
Projected Revenues Northwest and California.xls...	9/17/2017 10:18 PM	EN
Proseware Project Budget Audit.docx.encrypted!	9/17/2017 10:18 PM	EN
Q3 Sales and Marketing Expense Report Audit....	9/17/2017 10:18 PM	EN
RD And Engineering Costs Q1.xlsx.encrypted!	9/17/2017 10:18 PM	EN
RD Expense Report.pptx.encrypted!	9/17/2017 10:18 PM	EN

27 items

Windows taskbar: Type here to search, microphone, network, Edge, File Explorer, Store, Mail, Word.



+ New

 Dashboard All resources Intune Azure Active Directory Resource groups App Services Function Apps SQL databases Azure Cosmos DB Virtual machines Load balancers Storage accounts Virtual networks Monitor

More services >

Attack Surface Reduction



Create rules to reduce the attack surface on the managed devices. You can block running of suspicious executables in macros, scripts and emails or you can allow them while still auditing.

[Learn more about Attack Surface Reduction](#)

Attack Surface Reduction rules

Rules to prevent Office Macro threats

Office apps injecting into other processes ⓘ

Block ▼

Office apps/macros creating executable content ⓘ

Block ▼

Office apps launching child processes ⓘ

Audit only ▼

Win32 imports from Office macro code ⓘ

Block ▼

Rules to prevent script threats

Obfuscated js/vbs/ps/macro code ⓘ

Block ▼

js/vbs executing payload downloaded from Internet ⓘ

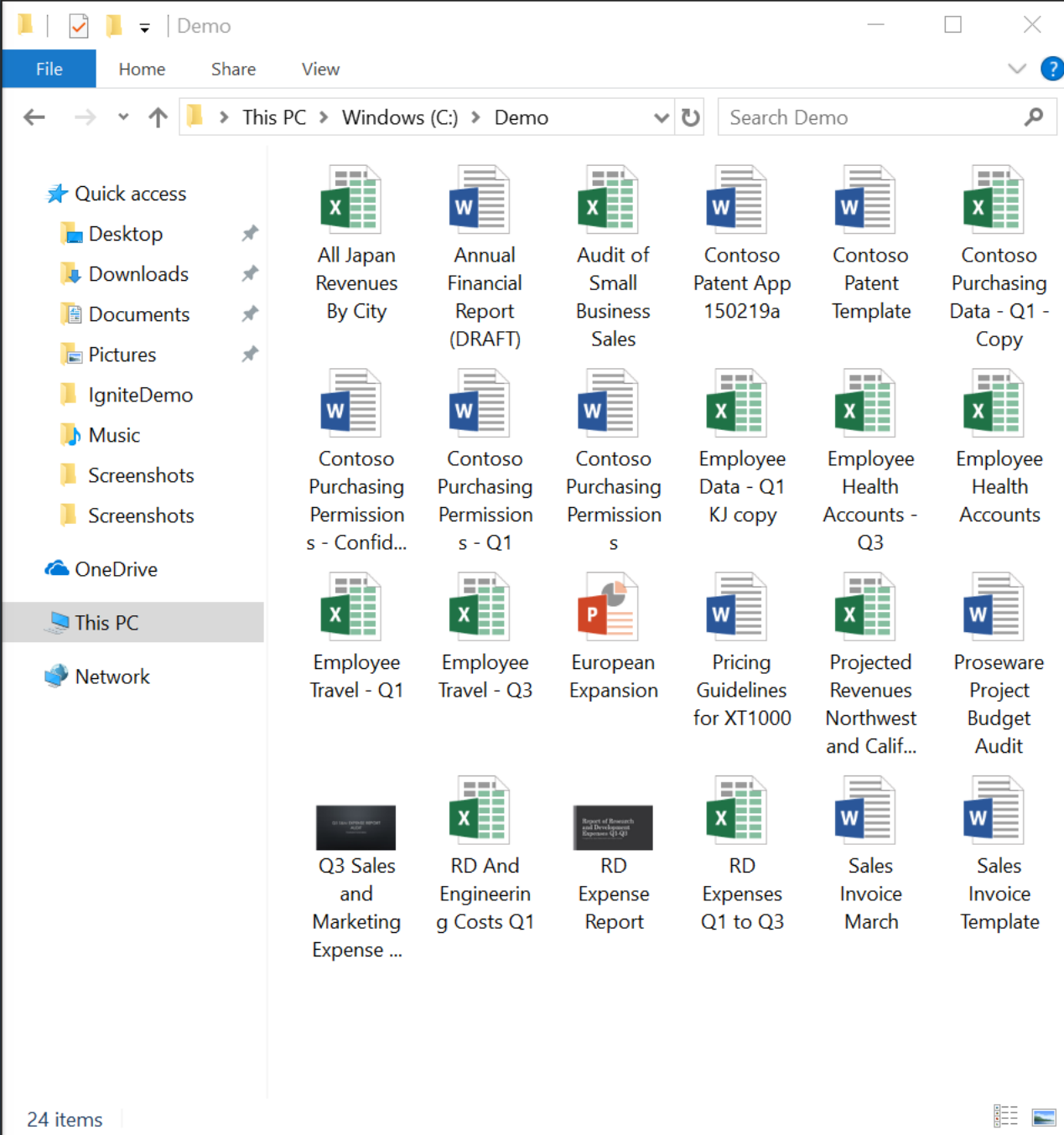
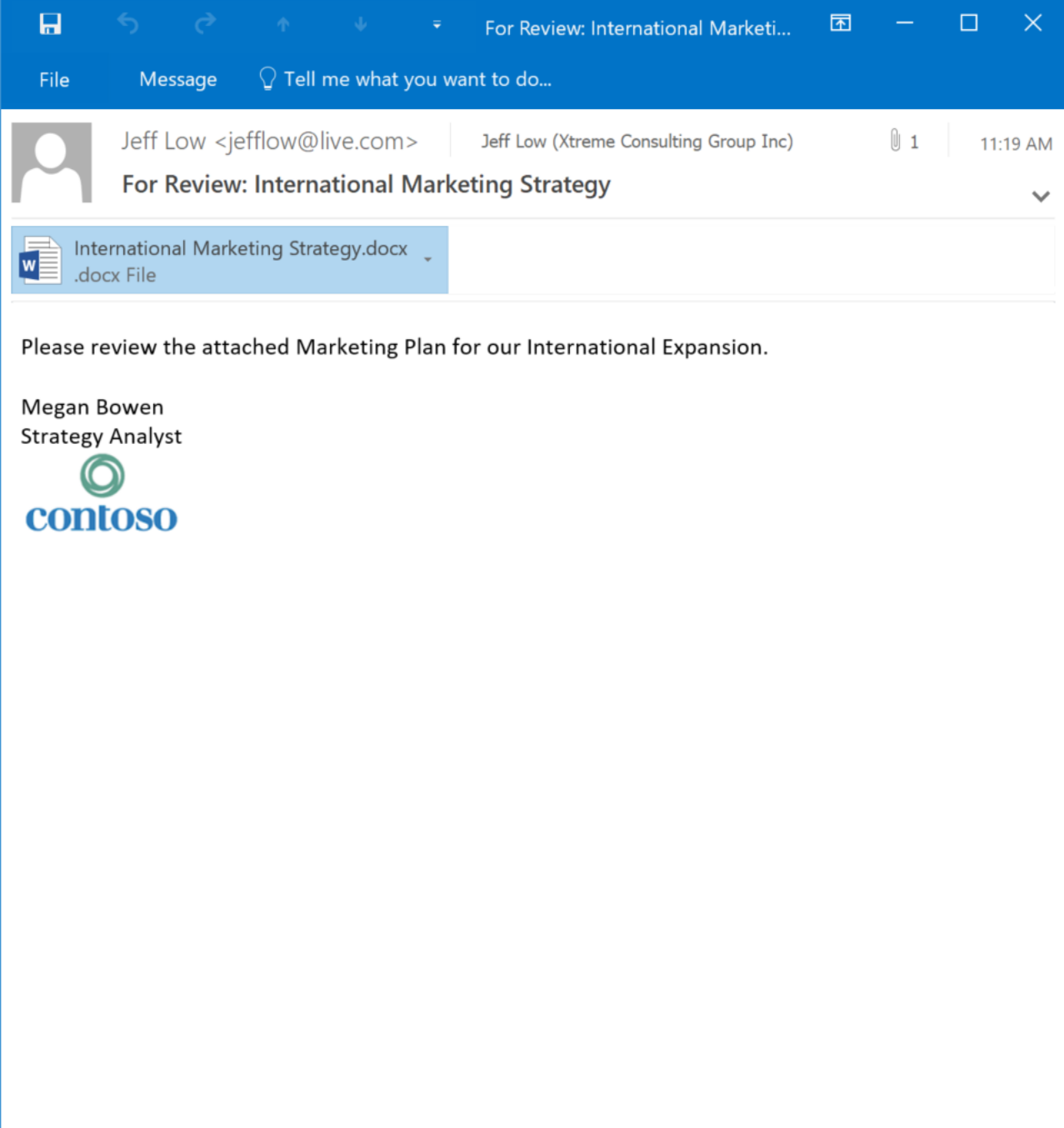
Block ▼

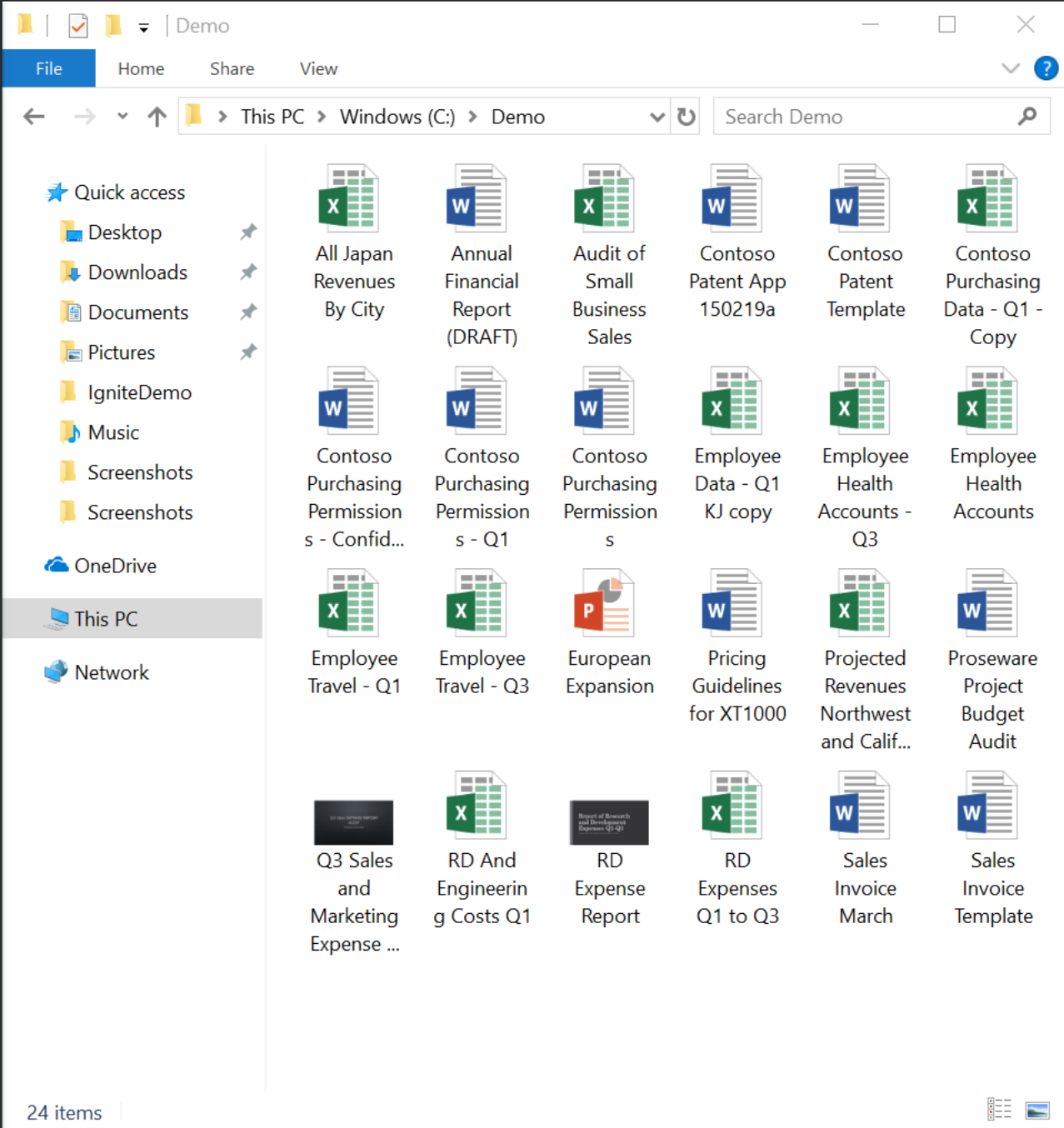
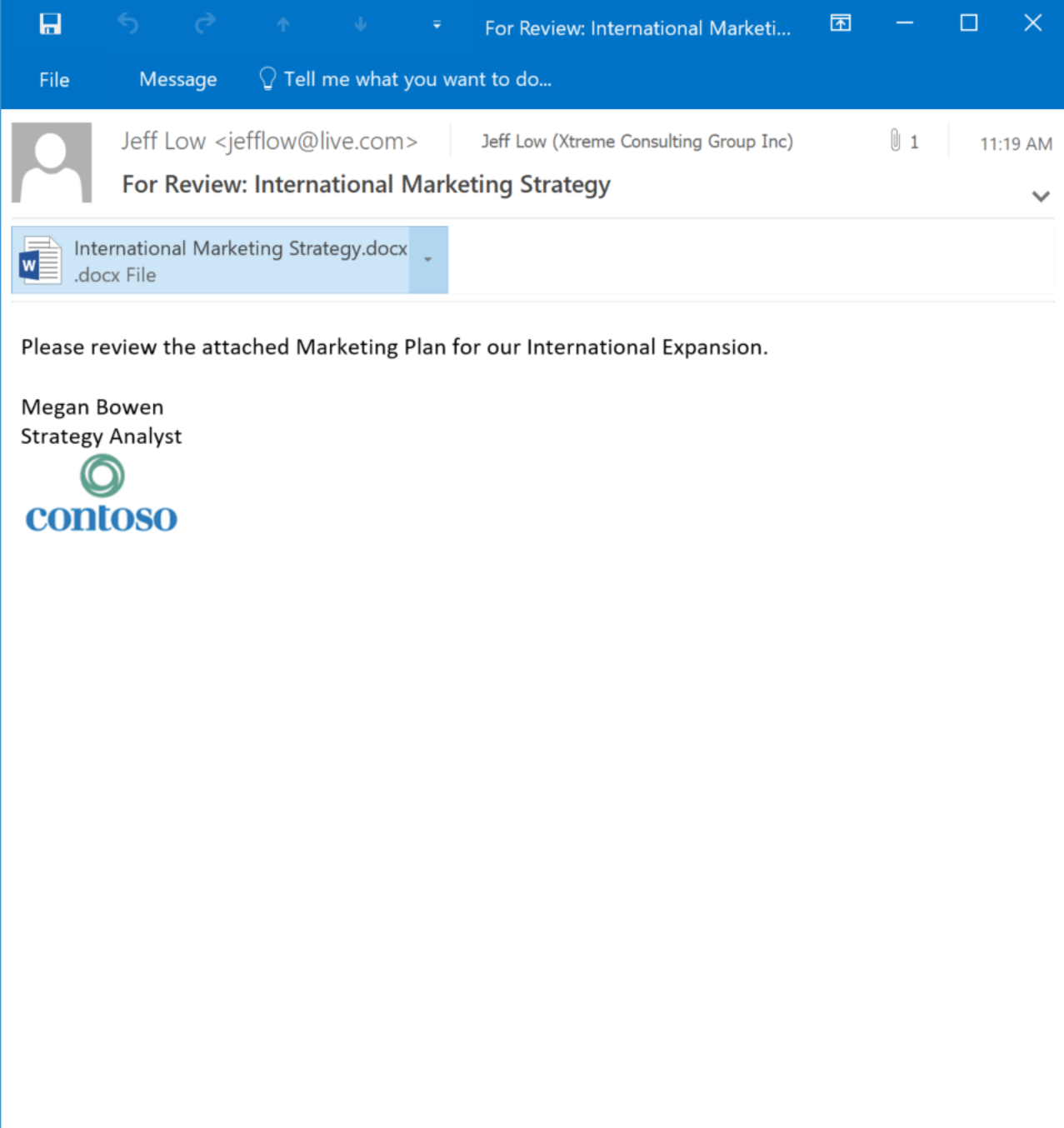
Rules to prevent email threats

Execution of executable content (exe, dll, ps, js, vbs, etc.)
dropped from email (webmail/mail client) ⓘ

Block ▼

OK







Demo:

Bloqueando el acceso de procesos no confiables a ficheros mediante Windows Defender **controlled folder access**



Recycle Bin



Type here to search



←

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

Notifications

Windows Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.

Change notification settings

📁 | 📄 | 📁 | ▾ | Demo

File Home Share View

← → ▾ ↑ 📁 > This PC > Windows (C:) > Demo ▾ ↻ 🔍 Search Demo 🔍

▼ ⭐ Quick access

📁 Desktop ⚡

📁 Downloads ⚡

📁 Documents ⚡

📁 Pictures ⚡

📁 IgniteDemo

📁 Music

📁 Screenshots

📁 Screenshots

> ☁ OneDrive

> 💻 This PC

> 🌐 Network

📄 X All Japan Revenues By City

📄 W Annual Financial Report (DRAFT)

📄 X Audit of Small Business Sales

📄 W Contoso Patent App 150219a

📄 W Contoso Patent Template

📄 X Contoso Purchasing Data - Q1 - Copy

📄 W Contoso Purchasing Permissions - Confid...

📄 W Contoso Purchasing Permissions - Q1

📄 W Contoso Purchasing Permissions

📄 X Employee Data - Q1 KJ copy

📄 X Employee Health Accounts - Q3

📄 X Employee Health Accounts

📄 X Employee Travel - Q1

📄 X Employee Travel - Q3

📄 P European Expansion

📄 W Pricing Guidelines for XT1000

📄 X Projected Revenues Northwest and Calif...

📄 W Proseware Project Budget Audit

📄 Q3 Sales and Marketing Expense ...

📄 X RD And Engineering Costs Q1

📄 RD Expense

📄 X RD Expenses

📄 W Sales Invoice

📄 W Sales Invoice

24 items

🏠

🔍 Type here to search

🗨️

🖥️

📧

📁

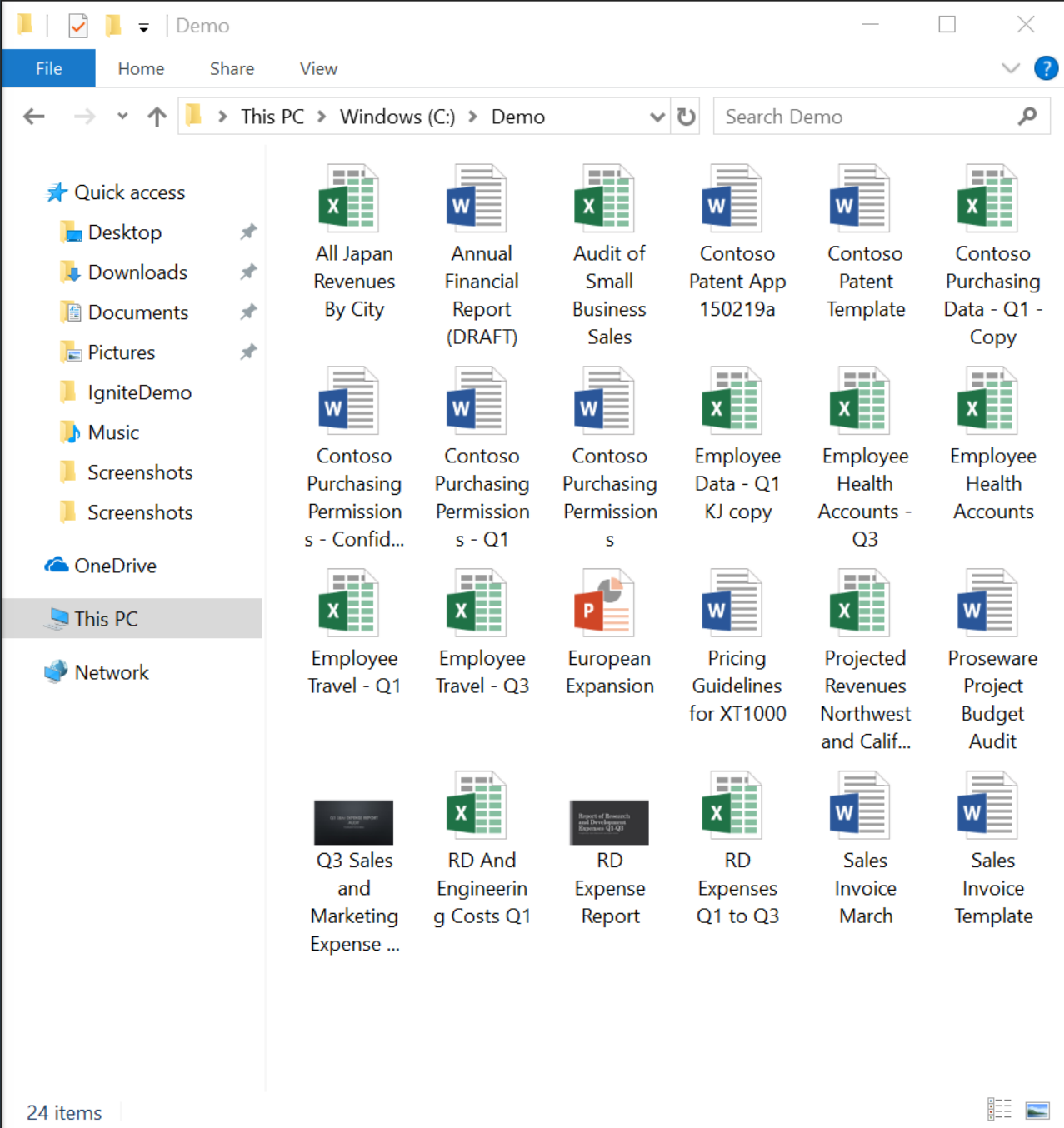
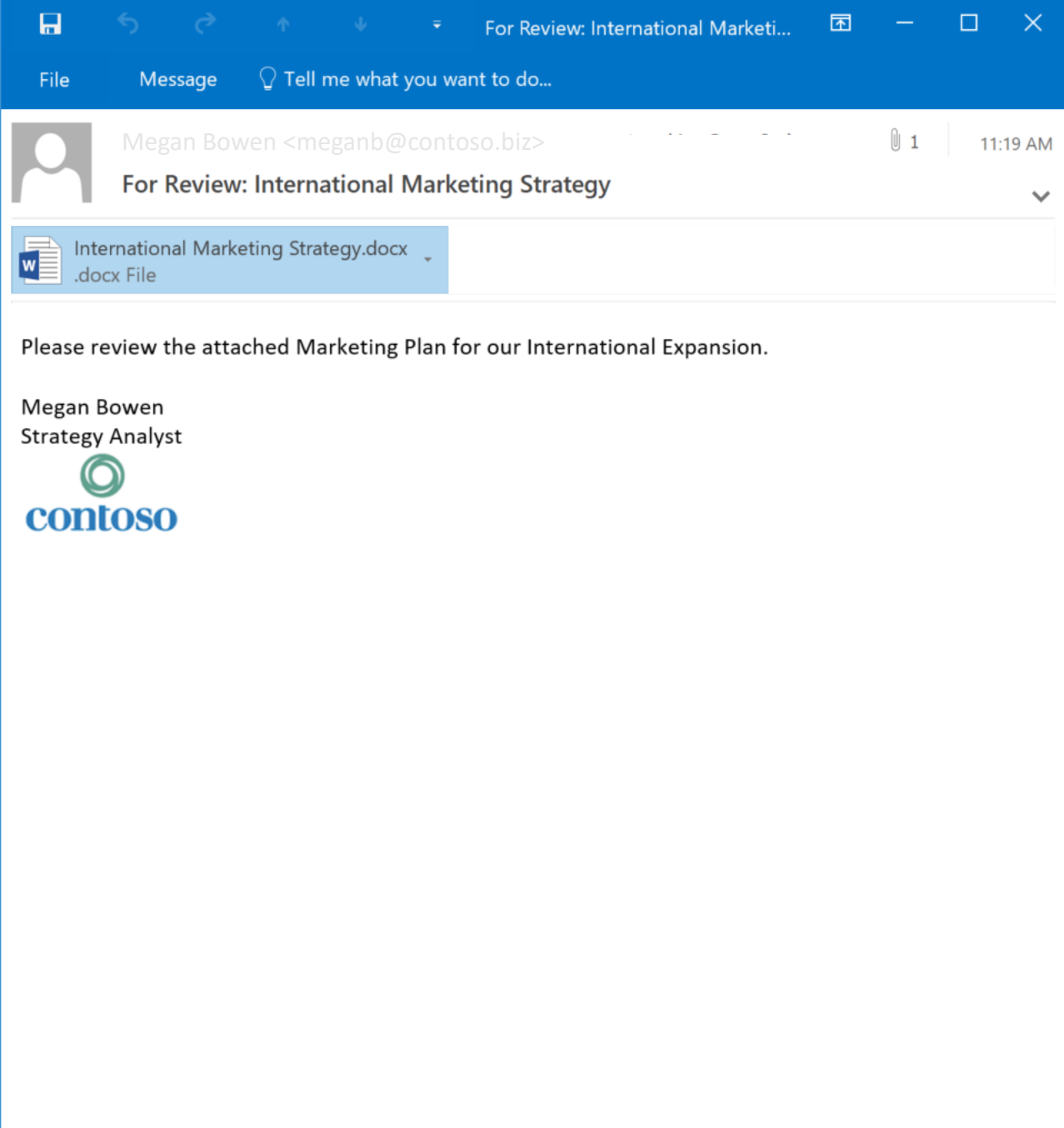
🛡️

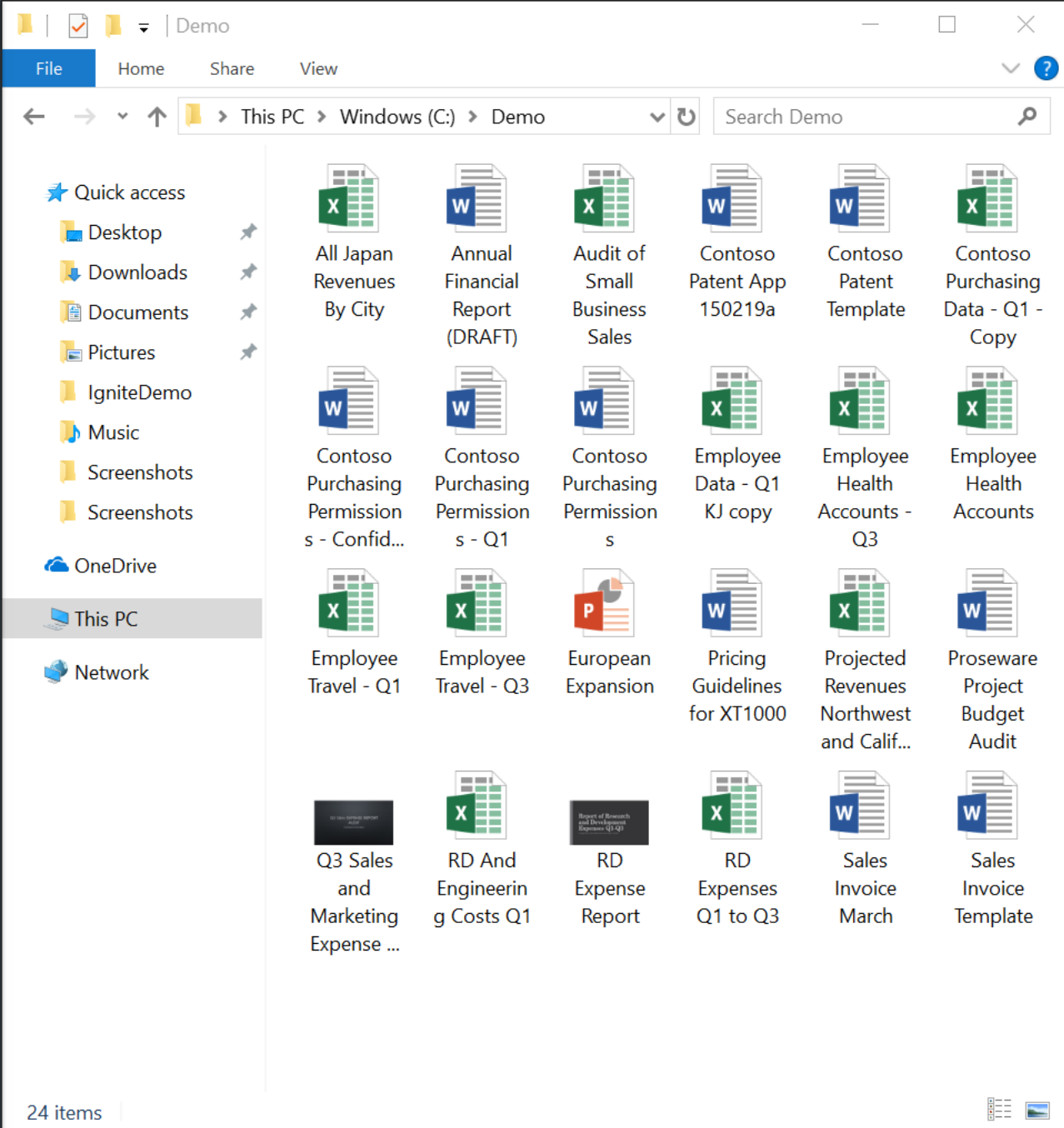
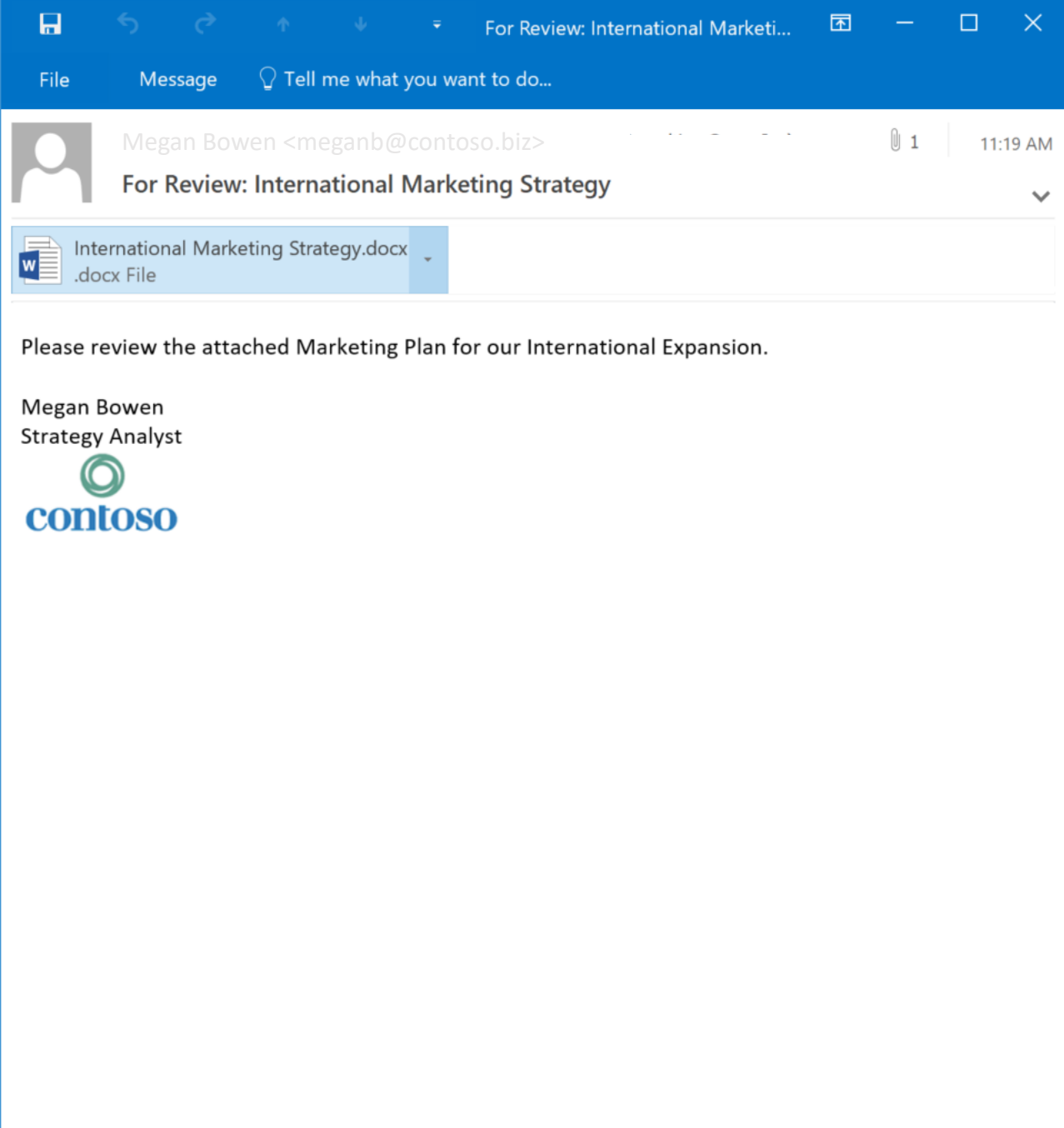
👤

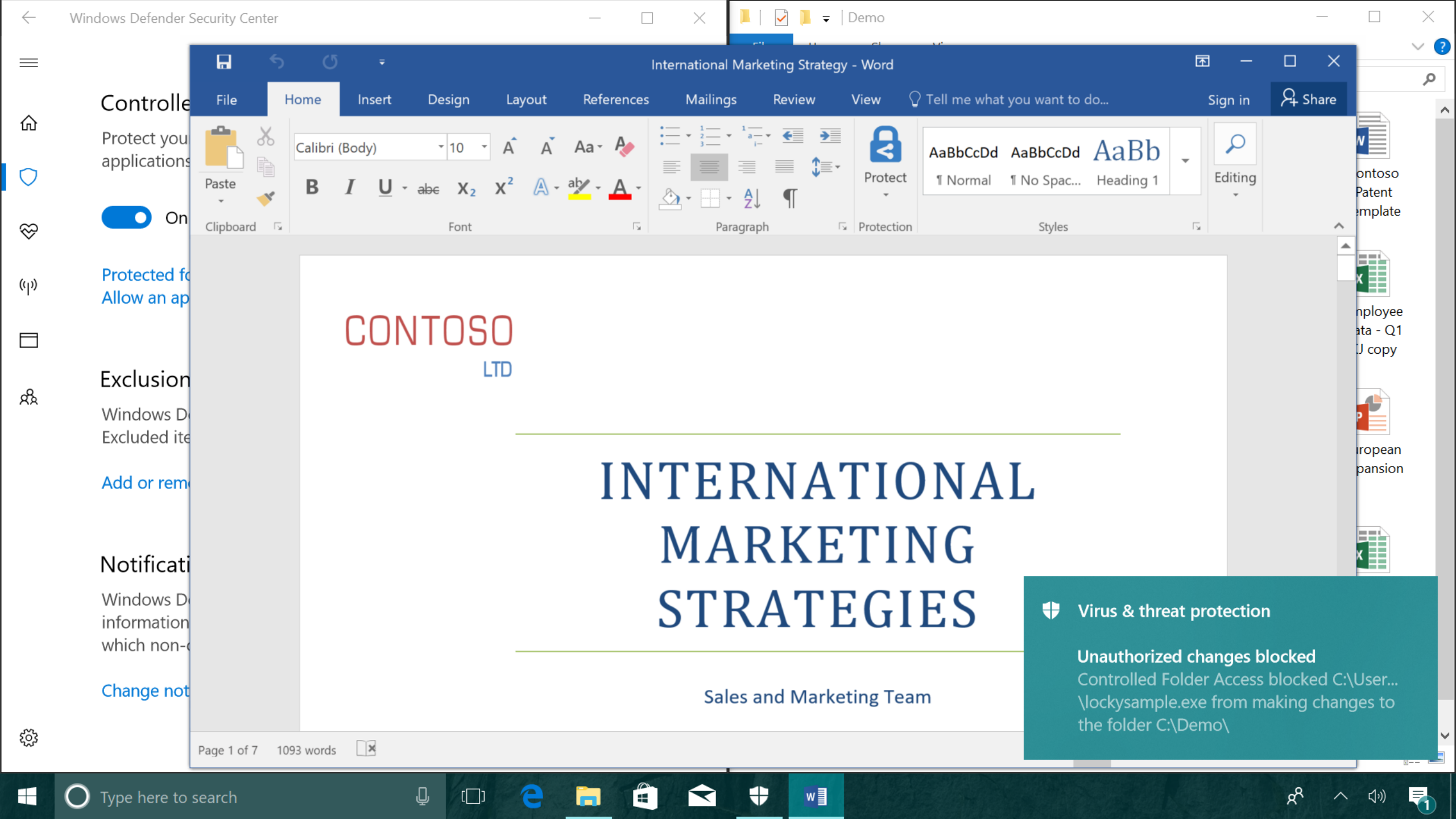
⬆️

🔊

💬







CONTOSO
LTD

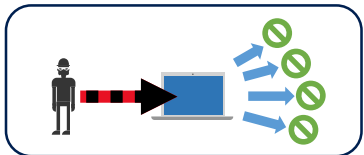
INTERNATIONAL MARKETING STRATEGIES

Sales and Marketing Team

Virus & threat protection

Unauthorized changes blocked

Controlled Folder Access blocked C:\User...\lockysample.exe from making changes to the folder C:\Demo\

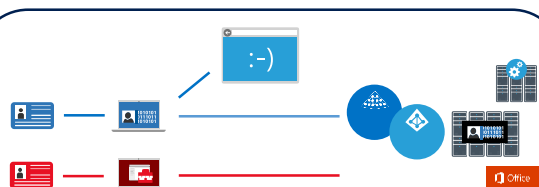


Defensas para contener a los atacantes



1. Eliminar accesos excesivos en carpetas compartidas

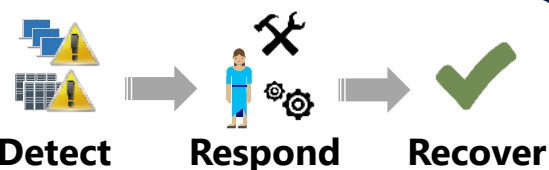
- Tanto por SMB como Sharepoint u otros a grupos extensos (todos...)



2. Roadmap Securing Privileged Access (SPA)

- Estaciones de administración, LAPS, JIT usando PAM, + MFA, ATA, JEA, Hardening, ESAE, Device Guard, Shielded VMs

<http://aka.ms/sparoadmap>



3. Operaciones de seguridad: Detección y limpieza rápida

- Usa detección basada en la nube como **Defender ATP + Hexadite**
- Asegura la disponibilidad de investigadores 24*7



Backup en caso de emergencia

- Buenas practicas de recuperación de desastres
 - Los backups deben incluir todos los datos críticos
 - Los backups deben ser probados periódicamente
- Los backups deben ser inaccesibles a los atacantes
 - Backup Offline
 - Evitar que las cuentas de administración puedan borrar o sobrescribir las copias online
- La nube ofrece capacidades de backup offsite nativas
 - Resistencia natural al ransomware



Demo:

Recuperación de desastres

Recuperando ficheros en caso de ransomware con OneDrive for Business



Recycle Bin



Type here to search



 Search

- Rob Lefferts
- 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](#)

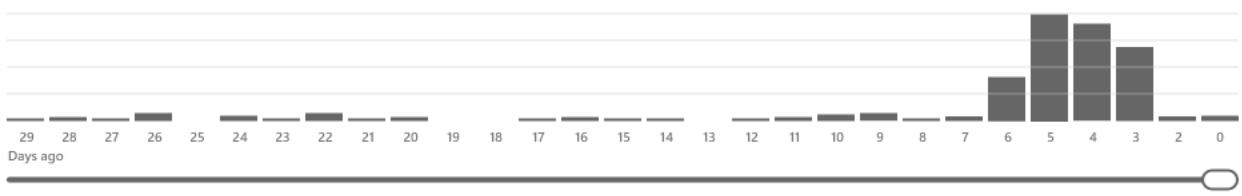
Restore my OneDrive

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

Today

Restore



Change ↓	File name
☐ ^ Today 9/24/2017 (30)	
☐ ↑ Uploaded by Kat Larson 11:19:03 AM	 Next Generation V1
☐ ↑ 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

- Rob Lefferts
- 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](#)

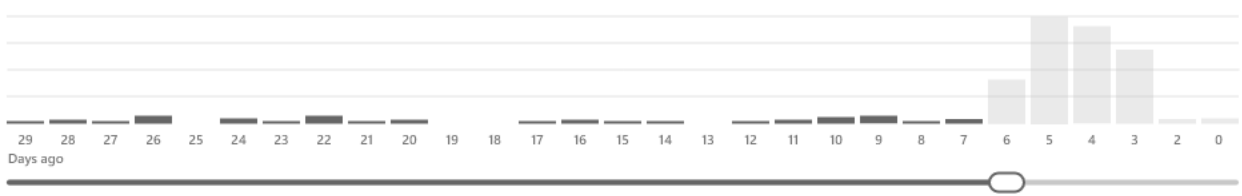
Restore my OneDrive

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



Change ↓	File name
☐ ^ 6 days ago 9/18/2017 (40020)	
☒  Renamed by Kat Larson 3:34:03 AM	 Next Generation V1 > 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

 Search

- Rob Lefferts
- 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

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 ago	
☒	Renamed by Kat Larson 10:19:03 AM	Worcestershire Initiative
☒	Deleted by Razeena Javan 9:51:03 PM	Buffer API Docs
☒	Deleted 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

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

 Search

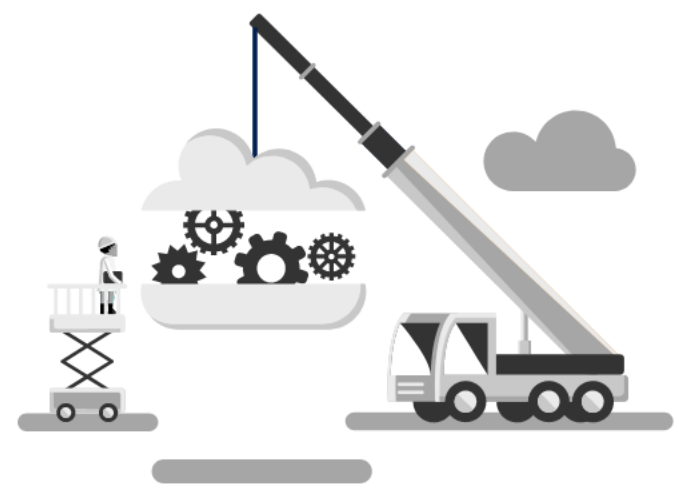
- Rob Lefferts
- Files
- Recent
- Shared with me
- Discover
- Recycle bin
- Contoso 
- Groups bring teams together.
Join one or create your own.
- OneDrive admin
- Get the OneDrive apps
- Return to classic OneDrive

Your OneDrive is being restored to how it existed on 8/12/2017, 3:45:01 PM
You can [view your files](#) but are set to read only until this process completes.

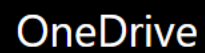
Cancel

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.



Your OneDrive is being restored
[View previous restores](#)



Restoring your OneDrive

Sort



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](#)

① Your OneDrive is being restored to how it existed on 8/12/2017, 3:45:01 PM
You can [view your files](#) but are set to read only until this process completes.

Files

✓	 Name ↓	Date Modified	Modified By	Sharing
	 Commissioned Research	Yesterday, 3:34pm	Kat Larson	Private
	 Brainstorms	Yesterday, 3:34pm	Kat Larson	Private
	 Executive share outs	Yesterday, 3:34pm	Kat Larson	Private
	 Native Juices Project	Yesterday, 3:34pm	Kat Larson	Private
	 WE23435EWRTRT.WNCRY	Yesterday, 3:34pm	Kat Larson	Private
	 WE23432323RTRT.WNCRY	Yesterday, 3:34pm	Kat Larson	Private
	 WE23435Ehujedr.WNCRY	Yesterday, 3:34pm	Kat Larson	Private
	 WE23239WUOEUD.WNCRY	Yesterday, 3:34pm	Kat Larson	Private
	 QFSFS2134345.WNCRY	Yesterday, 3:34pm	Kat Larson	Private
	 BTWE23osd23.WNCRY	Yesterday, 3:34pm	Kat Larson	Private

Progress

Uploading 1 item to Files

16.3 MB/203 MB

 Search

 New 

 Upload 

 Flow 

 Sync

 Restoring your OneDrive

 Sort 





✓ Your OneDrive has been restored to how it existed on 8/12/2017, 3:45:01 PM
You can [view the report here](#).

Rob Lefferts

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](#)

Files

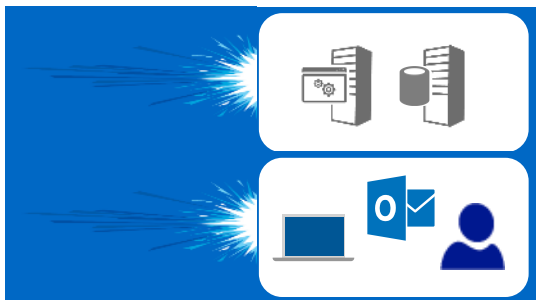
✓ 	Name ↓	Date Modified	Modified By	Sharing
	Commissioned Research	Yesterday, 3:34pm	Kat Larson	Private
	Brainstorms	Mar 22, 8:15am	Kat Larson	Private
	Executive share outs	Aug 18, 10:23am	Kat Larson	Private
	Native Juices Project	Jul 23 2016, 2:22pm	Kat Larson	Private
	Next Generation V1	Jun 24 2016, 4:16pm	Kat Larson	Private
	Trigon Business Designs	Jun 21 2016, 10:24am	Elsa Angelovaa	Public Share
	PK Brainstorming Notes	Jun 9 2016, 4:16pm	Kat Larson	Private
	Buffer API Docs	May 11 2016, 1:22pm	Kat Larson	Private
	Figaro.DAT	May 5 2016, 11:23am	Kat Larson	Private
	Budget 2017	May 5 2016, 11:23am	Kat Larson	Private

Progress

Restoring your OneDrive

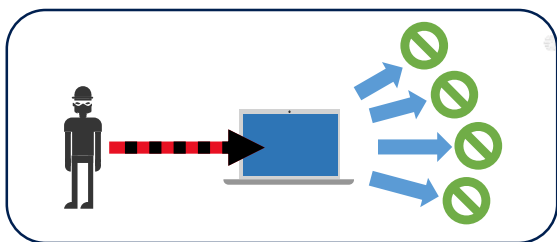
Restore completed. [View the report](#).

Una estrategia pragmática de tres pasos



1. Bloquear los ataques en la primera línea

- Subir el coste de comprometer los endpoints
 - Servidores cara a internet
 - Estaciones de trabajo y usuarios



2. Defensas para contener a los atacantes

- Asumir que las defensas fallaran
- Subir el coste de moverse por el entorno para el atacante
- Respuesta rápida para detectar las amenazas y bloquear el ataque



3. Backup en caso de emergencia

- Asumir que todas las defensas pueden fallar
- Restaurar datos desde backups que no están accesibles a los atacantes

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

