



Trend Micro Security Assessment Service à l'intention des partenaires

Trend Micro





Sommaire

- Objectifs
- Trend Micro Security Assessment Services
 - Marketing Email pour tous les partenaires
 - Page Web en marque blanche pour nos partenaires
 - Demande de page Web via le portail partenaires
- Tableau de bord de l'utilisation des services pour les partenaires en marque blanche
- Enregistrement d'offres (Deal Registration) et Incentives
- Ressources de support
- Annexe : processus d'évaluation, étape par étape



Objectifs

- Trend Micro Security Assessment Service est un service d'évaluation convivial qui offre une visibilité sur les menaces présentes sur les segments d'une entreprise. Ce service aide les prospects à mesurer l'efficacité de leur solution actuelle de sécurité des Endpoints et de l'email. Ce service permet aux partenaires d'aider leurs prospects à :
 - Vérifier les menaces par email sur Microsoft 365
 - Rechercher des menaces sur des Endpoints
 - Proposer un rapport final en PDF à l'intention des décideurs
- Accompagner les partenaires pour être reconnus en tant qu'acteur de confiance vis-à-vis de leurs clients, aider les clients à évaluer leur environnement et générer de nouvelles opportunités de vente

Trend Micro Security Assessment Services - Introduction

- Ce service d'évaluation de la sécurité identifie les menaces sur l'ensemble des segments des entreprises.
- Les comptes email de Microsoft 365® et les Endpoints sont analysés à la recherche de menaces ayant contourné les fonctions de sécurité native.
- Ce service met en avant les avantages des solutions email, Endpoint et XDR de Trend Micro.
- Un rapport détaillé au format PDF est généré et mis à disposition pour indiquer toute menace présente au sein des environnements de clients.

1



Connexion à M365 pour analyser les emails

2



Exécution de l'outil Endpoint

3



Mise à disposition du client avec les clients

Notification par email lorsque le rapport est prêt
Lien vers un portail sécurité pour le télécharger



Trend Micro Security Assessment Service pour les partenaires

Trend Micro Security Assessment Services propose les atouts suivants :

- 1 Marketing Email pour tous les partenaires** : utilisez les modèles d'email pour inviter les prospects et clients à utiliser ce service d'évaluation. Le modèle est proposé en co-branding, avec le logo de votre entreprise et vos informations de contact aux côtés de ceux de Trend Micro. Le modèle d'email est disponible depuis le menu Marketing Email du portail partenaires.
- 2 Page Web du service d'évaluation, en marque blanche pour nos partenaires Top-Tier.** Trend Micro offre un service d'évaluation de la sécurité, proposé en marque blanche à nos partenaires. La page Web est proposée en co-branding, avec le logo du partenaire. Nos partenaires Tier-One peuvent demander la création de cette page en marque blanche sur le portail partenaires via le menu Customer Success - > Trend Micro Security Assessment – White-label Request Form.

1 Security Assessment Service - Campagne Emailing

Trend Micro Security Assessment Services

EDM SUBJECT	DATE UPLOADED	LANGUAGE	
1	2020-02-09	English	Preview
2	2020-02-09	English	Pre
3	2020-03-26	English	Pre
4	2020-03-26	English	Pre
5	2020-03-26	English	Pre

Utilisez les modèles d'email pour inciter les prospects et clients à évaluer leur sécurité. Le modèle est proposé en co-branding, avec le logo et le contact de votre entreprise aux côtés de ceux de Trend Micro. Le modèle d'email est disponible dans le portail partenaire (Marketing Portal -> Email Marketing).

Trend Micro Security Assessment Service

Get a detailed view of threats found across segments of your organization.

In our quest to assure everyone is optimally protected against the latest threats, we'd like to invite you to be one of the first to use our **Trend Micro Security Assessment Service**.

[Try it now >](#)

Trend Micro Security Assessment Service lets you:

- Scan Microsoft® Office 365® email inboxes and key endpoints to find threats that may have evaded existing

[Send to Customers](#)

[Send Sample Email to Me](#)

[Download Email in HTML](#)

Send Test will be sent to testpartneremail@testpartner.com.

Subject
Hybrid Cloud/Cloud One - Webinars Complete Series

Description

Upload Date
2020-02-09

Language
English

[Close](#)



Logo
Partenaire

Trend Micro Security Assessment Service

Get a detailed view of threats found across segments of your organization.

In our quest to assure everyone is optimally protected against the latest threats, we'd like to invite you to be one of the first to use our **Trend Micro Security Assessment Service**.

[Try it now >](#)

Trend Micro Security Assessment Service lets you:



- **Scan Microsoft® Office 365® email inboxes and key endpoints** to find threats that may have evaded existing protections and could impact your organization.



- **Receive a report** of your security posture to inform you on how well you are protected against ransomware, phishing threats, business email compromise (BEC), and more.



- **Gain insights** into vulnerabilities in your security strategy and learn how you can implement alternate solutions to fill gaps.



- **Delete your data from the service** immediately after the assessment is finished, leaving you in complete control of your data.



Welcome to the Trend Micro Security Assessment Service

Do you want to know how well your current email and endpoint security is really performing? Run our free Security Assessment Service to see if you are effectively protected against the advanced threats that are impacting organizations today.

Our quick and easy-to-run security assessment provides a detailed view of threats found across segments of your organization.

Here's how it works:

- Your email inboxes and endpoints are scanned to find any threats that may have evaded existing protections
- We provide a snapshot of your security posture in the form of a detailed report, so you can see how well you are protected against threats out there today
- You are invited to speak with a security expert at Trend Micro to learn more about the vulnerabilities in your security strategy and about new solutions that may help fill the gap

Want to learn more?

Check out our **video** which goes into more detail about our free service and how it works.

Already registered?

[Log in](#)

If you are experiencing any problems with the service or have any questions, please **contact** our Technical Support team.

L'email redirige vos prospects et clients vers le site Web suivant : <https://resources.trendmicro.com/security-assessment-service-us.html> pour évaluer la sécurité email et des Endpoints. Merci de consulter l'annexe pour une présentation étape par étape du service d'évaluation.

Sign up today
and get started with your free security assessment

* First Name:

* Last Name:

* Email Address:

* Phone Number:

* Company:

* Number of Employees:

* Job Title:

* Country:

* I agree to the [Terms and Conditions](#)

[START](#)

[Privacy notice](#)
[Data collection disclosure](#)
[Third-party license information](#)

2 Page d'accueil en marque blanche du service d'évaluation

Le service d'évaluation de la sécurité est proposé en marque blanche à nos partenaires. La page d'accueil est proposée en co-branding, avec logo du partenaire.

Nos partenaires Tier-One peuvent demander la création de cette page en marque blanche dans le portail partenaires, via le menu Customer Success -> Trend Micro Security Assessment – White-label Request Form.

zones LLC Security Assessment

zones-assessment.xdr.trendmicro.com/#!/

ZONES
First Choice for IT™

Welcome to the Zones LLC Security Assessment Service

Do you want to know how well your current email and endpoint security is really performing? Run our free Security Assessment Service to see if you are effectively protected against the advanced threats that are impacting organizations today.

Our quick and easy-to-run security assessment provides a detailed view of threats found across segments of your organization.

Here's how it works:

1. Your Microsoft® Office 365® email inboxes and endpoints are scanned to find any threats that may have evaded existing protections
2. We provide a snapshot of your security posture in the form of a detailed report, so you can see how well you are protected against threats out there today
3. You are invited to speak with a security expert at Trend Micro to learn more about the vulnerabilities in your security strategy and about new solutions that may help fill the gap

Want to learn more?

Check out our [video](#) which goes into more detail about our free service and how it works.

Try it Now

* First name: * Last name:

* Job title:

* Company name:

* Region:

* Work email address:

We are strongly committed to maintaining the privacy of your personal information. Your email address will only be used for sending messages about the assessment results.

I agree to the Terms and Condition ([EN](#) | [JP](#))

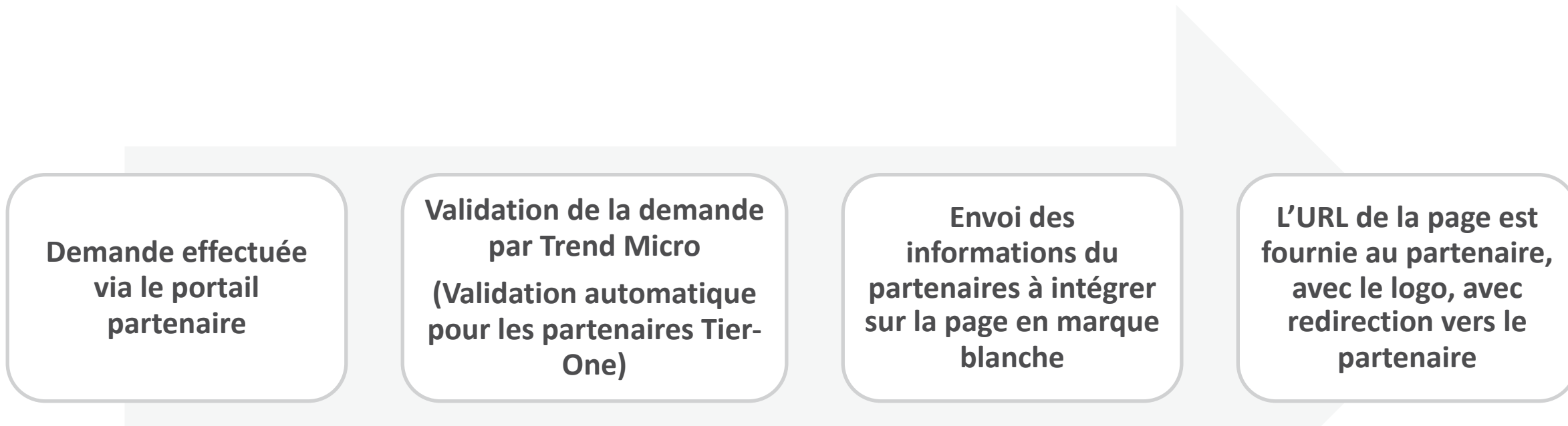
Already registered? [Log On](#)

Copyright © 2020 Trend Micro Incorporated. All rights reserved. [Privacy Notice](#) | [Data Collection Disclosure](#) | [Third-party License Information](#) | **Powered by TREND MICRO**

Exemple Branding
partenaire



Demande de Page Web en marque blanche



**Partenaire Top-tier : Platinum/Gold/Silver,
NCP, Intégrateur systèmes, Distributeur**

Informations du formulaire de demande

Trend Micro Security Assessment Service - White-label Landing Page

Please fill in the website information below. The information will be displayed on the white-label website with URL: <https://<PARTNER>-assessment.xdr.trendmicro.com>

Your application will be reviewed, and the team will reply to you in 3 business days.

*** Company Name** (The name display in the White-label website and URL)

*** Country**

US ▼

Customer Enquiry Email (If not provided, we will use assessment@trendmicro.com)

Sales Contact Email (If not provided, we will use https://www.trendmicro.com/en_us/business/get-info-form.html)

Apex One URL (If not provided, we will use https://www.trendmicro.com/product_trials/service/index/us/165)

Cloud App Security URL (If not provided, we will use https://www.trendmicro.com/product_trials/service/index/us/155)



Tableau de bord de l'utilisation des services pour les partenaires avec une page Web en marque blanche

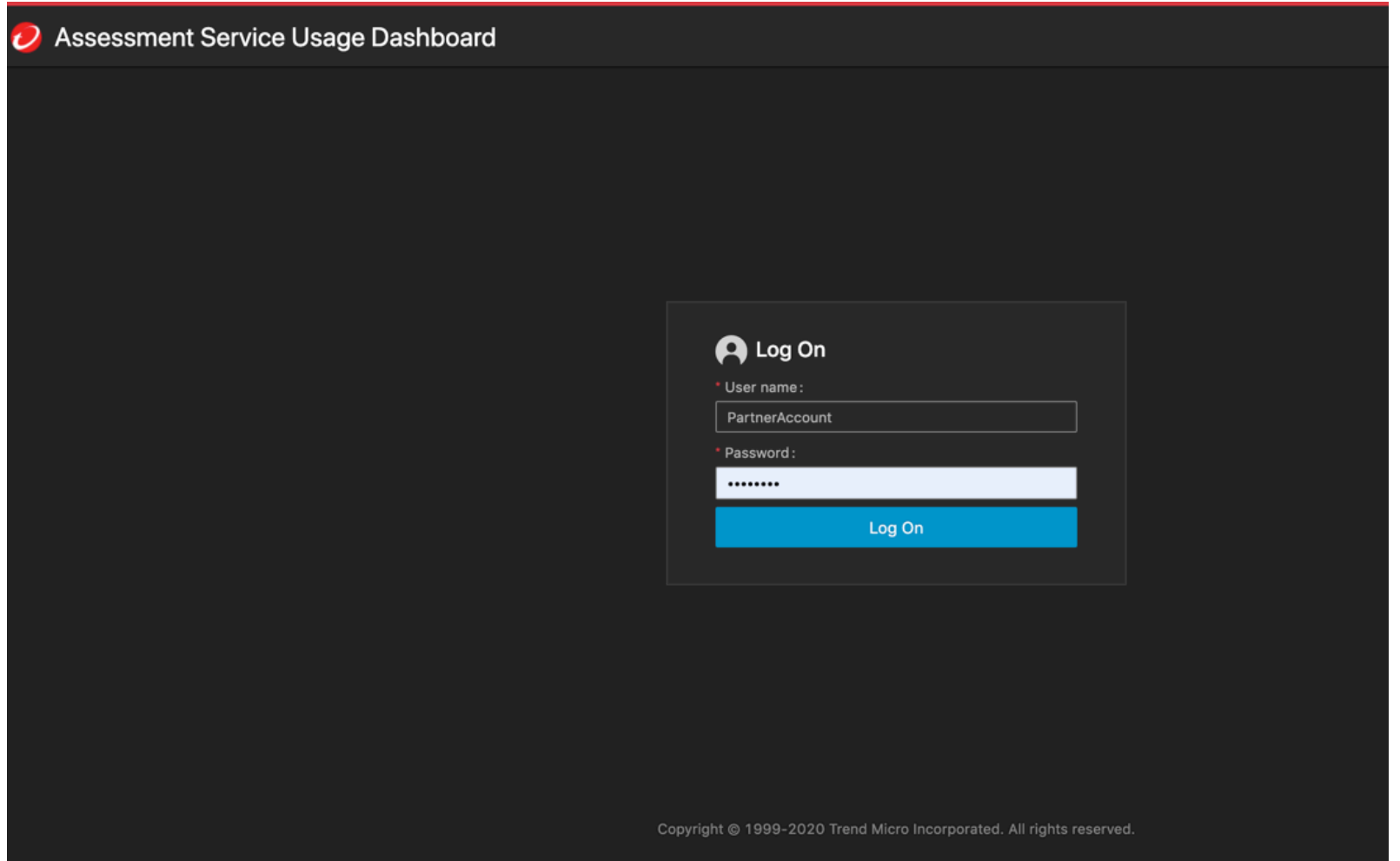


Tableau de bord d'utilisation

Chaque partenaire dispose de son propre tableau de bord. Il accède aux clients enregistrés et aux rapports d'évaluation à partir de son site en marque blanche.

Page du tableau de bord

<https://admin.assessment.trendmicro.com/#/partner>



Assessment Service Usage Dashboard

Log On

* User name :
PartnerAccount

* Password :

Log On

Copyright © 1999-2020 Trend Micro Incorporated. All rights reserved.

Email

Summary

Scan time: (2020-03-18 00:24:38 - 2020-03-18 03:56:31)

1109 Total Mailboxes	5 BEC Messages ▲ Potential cost: \$373,615	56 Phishing Messages	1 Ransomware ▲ Potential cost: \$36,295	52 Malicious Files	167 Malicious URLs
199931 Total Email Messages					

Top Possible Affected Users

	Relative Risk Level	User	Email Address	Job Title (Department)	Associated Endpoints	Reasons
1	● Most at risk	Asim.Khan@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Phishing
2	● Most at risk	Jeffery@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Advanced Spam threats
3	● Most at risk	Tom@xentit.com	Tom@xentit.com	Sales Manager	PC1	Most at risk for Phishing
4	● Most at risk	rkadakia@xentit.com	rkadakia@xentit.com	SVP & CTO	LAPTOP-IARSQLVS	Most at risk for Emergent and Advanced Spam threats
5	● Most at risk	GrantJ@xentit.com	grantj@xentit.com	IT manager(IT Department)	LAPTOP-RUKTBAAF	Most at risk for Phishing, Emergent, and Advanced Spam threats
6	● Most at risk	MariaT@xentit.com	mariat@xentit.com	Finance	GJCQ5IB	Most at risk for Phishing and Advanced Spam threats

The relative risk level reflects the user's exposure to five threat categories in relation to other users in the same environment.

Top Business Email Compromise (BEC) Email Recipients

	Recipient	Subject	Detections	Last Detected
1	"alex bryan"<bryan.alex@navicenthealth.org>	Business report	5	2020-03-18 00:37:13
2	"alex bryan"<bryan.alex@navicenthealth.org>	Request from CEO	5	2020-03-18 00:37:13
3	"alex bryan"<bryan.alex@navicenthealth.org>	Request	5	2020-03-18 00:37:13

Rapport d'évaluation
Microsoft 365

Top Phishing Email Recipients





Top Phishing Email Recipients

	Recipient	Subject	Detections	Last Detected
1	"christopher bryan" <bryan.christopher@navicenthealth.org>	Weekly Report	24	2020-03-18 00:37:13
2	"delladonna.michael" <delladonna.michael@navicenthealth.org>	Log Finding	11	2020-03-18 00:37:13
3	"paul r. johnson"<pjohnson@xentit.com>	Microsoft account	11	2020-03-18 00:37:13
4	"robert jones" <jones.robert02@navicenthealth.org>	Weekly Report	11	2020-03-18 00:37:13

▲ We have noticed certain email threats have made it past your existing security solutions.

i We have noticed certain email threats have made it past your existing security solutions. Threats keep evolving to bypass security solutions. Trend Micro is continuously innovating and evolving our email security solutions to keep up with the latest threats. Ideal for cloud email and collaboration services, Trend Micro™ Cloud App Security is equipped to keep your organization safe. Trend Micro™ Cloud App Security offers advanced threat and data protection to secure email in Microsoft® Office 365®, Gmail™, and across cloud file-sharing services like Box and Dropbox™. CAS combines machine learning, document exploit detection, and behavior analysis to uncover unknown threats such as ransomware and business email compromise (BEC). Learn more about [Trend Micro™ Cloud App Security](#)

Rapport d'évaluation
Microsoft 365

Download PDF Report

Start Endpoint Assessment →

Restart Assessment


Delete My Data




Endpoint Assessment (Note: The tool will expire on 2020-05-07 14:12:38)

Data Collection Disclosure


You can deploy the endpoint assessment tool using any of the following methods.


Send Download Link

The service sends a download link and deployment instructions to specified users.


Copy Download Link

Send a download link and deployment instructions to users using your preferred application.


Download Assessment Tool

Download and run the tool on endpoints using your preferred system utility.

[View Deployment Instructions](#)

[Copy User List](#)

Endpoints with Collected Data

▲ If deployed correctly, the assessment tool automatically collects and uploads data to the service. Whenever the assessment tool uploads data, the following table displays a timestamp and the service sends a notification to the registered email address.

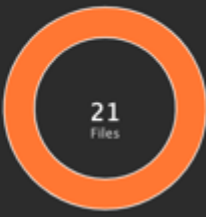
Possible Compromised Endpoint	Data Uploaded
1 EC2AMAZ-HCPPBUT	2020-03-12 16:54:01
2 LMT-01	2020-03-12 17:25:01
3 PC02	2020-03-13 08:31:01
4 DB-01	2020-03-12 11:25:01

[Stop Assessment and Generate Report →](#)



Endpoint ayant été évalués

5
Total Endpoints



● Malicious: 0
● Suspicious: 21



● Malicious: 0
● Suspicious: 1

P920 | IP address: 192.168.0.110 | Operation system: Windows 7 6.1.7601

● Malicious Threats (0)

● Suspicious Threats (5)

- File: C:\Program Files\MiniTool Partition Wizard 11\updatechecker.exe
- File: C:\temp\oABDMb.tmp
- File: C:\Program Files (x86)\Zyxel\Zyxel One Network Utility\tftpd32_svc.exe
- File: C:\Program Files (x86)\QNAP\Qfinder\QfinderPro.exe
- File: C:\Program Files\E-MailRelay\emailrelay-service.exe

LUK-06 | IP address: 192.168.0.111 | Operation system: Windows 7 6.1.7601

● Malicious Threats (0)

● Suspicious Threats (4)

- File: C:\Program Files (x86)\ouMb.tmp
- File: C:\windows\local\temp\eicar.exe
- Process: C:\windows\local\temp\checker.exe
- File: C:\temp\afcdstc\Osfm-00000157.bin

LUK-01 | IP address: 192.168.0.112 | Operation system: Windows 7 6.1.7601

● Malicious Threats (0)

● Suspicious Threats (5)

- File: C:\temp\local.tmp
- File: C:\temp\afb872bx.exe
- File: C:\temp\cgec.exe
- File: C:\temp\ou67Mb.tmp

Rapport d'évaluation des Endpoints



Évaluation Microsoft 365 Exemple de rapport

Email

Summary

Scan time: (2020-03-17 16:24:38 - 2020-03-17 19:56:31) (UTC+00)

- 1109 Total Mailboxes
- 199931 Total Email Messages
- 5 BEC Messages
▲ Potential cost: \$373,615
- 56 Phishing Messages
- 1 Ransomware
▲ Potential cost: \$36,295
- 52 Malicious Files
- 167 Malicious URLs

Top Possible Affected Users

	Relative Risk Level	User	Email Address	Job Title (Department)	Associated Endpoints	Reasons
1	● Most at risk	Asim.Khan@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Phishing
2	● Most at risk	Jeffery@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Advanced Spam threats
3	● Most at risk	Tom@xentit.com	Tom@xentit.com	Sales Manager	PC1	Most at risk for Phishing
4	● Most at risk	rkadakia@xentit.com	rkadakia@xentit.com	SVP & CTO	LAPTOP-IARSQVLS	Most at risk for Emergent and Advanced Spam threats
5	● Most at risk	Grant.J@xentit.com	grantj@xentit.com	IT manager(IT Department)	LAPTOP-RUKTBAAF	Most at risk for Phishing, Emergent, and Advanced Spam threats
6	● Most at risk	Maria.T@xentit.com	maria.t@xentit.com	Finance	GJCQ5IB	Most at risk for Phishing and Advanced Spam threats

The relative risk level reflects the user's exposure to five threat categories in relation to other users in the same environment.

Top Business Email Compromise (BEC) Email Recipients

	Recipient	Subject	Detections	Last Detected
1	"alex.bryan"<bryan.alex@navicenthealth.org>	Business report	5	2020-03-17 16:37:13 (UTC+00)
2	"alex.bryan"<bryan.alex@navicenthealth.org>	Request from CEO	5	2020-03-17 16:37:13 (UTC+00)
3	"alex.bryan"<bryan.alex@navicenthealth.org>	Request	5	2020-03-17 16:37:13 (UTC+00)

Top Phishing Email Recipients

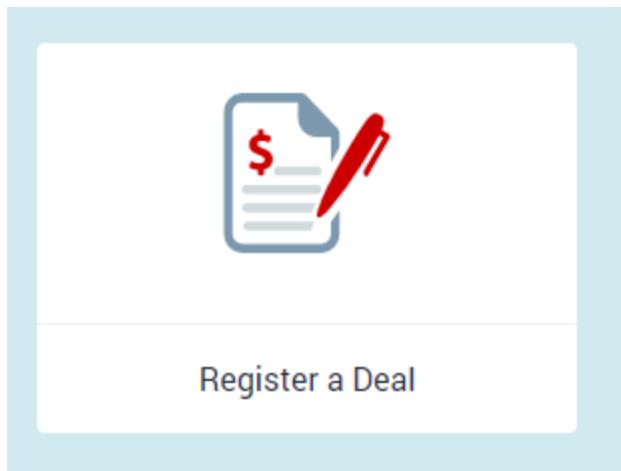
	Recipient	Subject	Detections	Last Detected
1	"christopher.bryan"<bryan.christopher@navicenthealth.org>	Weekly Report	24	2020-03-17 16:37:13 (UTC+00)
2	"delladonna.michael"<delladonna.michael@navicenthealth.org>	Log Finding	11	2020-03-17 16:37:13 (UTC+00)
3	"paul.r.johnson"<pjohnson@xentit.com>	Microsoft account	11	2020-03-17 16:37:13 (UTC+00)
4	"robert.jones"<jones.robert02@navicenthealth.org>	Weekly Report	11	2020-03-17 16:37:13 (UTC+00)

▲ We have noticed certain email threats have made it past your existing security solutions.

● We have noticed certain email threats have made it past your existing security solutions. Threats keep evolving to bypass security solutions. Trend Micro is continuously innovating and evolving our email security solutions to keep up with the latest threats. Ideal for cloud email and collaboration services, Trend Micro™ Cloud App Security is equipped to keep your organization safe. Trend Micro™ Cloud App Security offers advanced threat and data protection to secure email in Microsoft® Office 365®, Gmail™, and across cloud file-sharing services like Box and Dropbox™. CAS combines machine learning, document exploit detection, and behavior analysis to uncover unknown threats such as ransomware and business email compromise (BEC). Learn more about [Trend Micro™ Cloud App Security](#)

Enregistrement d'offres et Incentives

Enregistrez l'offre via le portail partenaire et indiquez « Security Assessment » pour obtenir une remise supplémentaire une fois approuvé.



Additional Information

* Opportunity Source

Channel Marketing ▼

Campaign Comments

Security Assessment

Code campagne AMEA Deal Registration to TM : 2020AMEAO365SAC



Ressources de support

- Vidéo : [Trend Micro Security Assessment Service - vidéo](#)
- Présentation client
- Vidéo : [Utilisation des campagnes marketing Trend Micro via le portail partenaires](#)
- Base de connaissances : [Trend Micro Security Assessment Service est désormais disponible](#)
- Base de connaissances : [Recueil des données dans le cadre de Trend Micro Security Assessment Service](#)
- Base de connaissances : [Nouvelles fonctionnalités de Trend Micro Security Assessment Services](#)
- Fiche solution : [Fiche solution sur les évaluations et bonnes pratiques Trend Micro](#)
- Support par email : partnersupport@trendmicro.com



Menaces sur les Endpoints détectées et neutralisées dans le monde en 2018 par Trend Micro. Créé avec des données réelles par l'artiste

[Stefanie Posaver.](#)

THE ART OF CYBERSECURITY



Inscription au processus d'évaluation, étape par étape

Welcome to the Trend Micro Security Assessment Service

Do you want to know how well your current email and endpoint security is really performing? Run our free Security Assessment Service to see if you are effectively protected against the advanced threats that are impacting organizations today.

Our quick and easy-to-run security assessment provides a detailed view of threats found across segments of your organization.

Here's how it works:

- Your Microsoft® Office 365® email inboxes and endpoints are scanned to find any threats that may have evaded existing protections
- We provide a snapshot of your security posture in the form of a detailed report, so you can see how well you are protected against threats out there today
- You are invited to speak with a security expert at Trend Micro to learn more about the vulnerabilities in your security strategy and about new solutions that may help fill the gap

Want to learn more?

Check out our [video](#) which goes into more detail about our free service and how it works.

Already registered?

[Log in](#)

If you are experiencing any problems with the service or have any questions, please **contact** our Technical Support team.

Sign up today
and get started with your free security assessment

• First Name:
Rachel

• Last Name:
Jin

• Email Address:
rachel_jin@trendmicro.com

• Phone Number:
86-13655177974

• Company:
Trend Micro

• Number of Employees:
7000

• Job Title:
Product Manager

• Country:
United States

• State:
TX

I agree to the [Terms and Conditions](#)

START

Privacy notice
Data collection details
Third-party license information

Your Security Assessment Service credentials



Connect

Today at 13:57

To: Rachel Jin (PM-CN)



SECURITY ASSESSMENT SERVICE

Read more about [The Art of Cybersecurity](#)

Dear Rachel,

Thank you for signing up to the Trend Micro™ Security Assessment Service. Please find below your unique link and confirmation code required to access this free service. Keep this information handy as it may be required for future log-in.

Email: rachel_jin@trendmicro.com

Confirmation code: ilsFHG

Trend Micro Security Assessment Service



Sincerely yours,
The Trend Micro Team





Présentation pas à pas Évaluation de la sécurité de Microsoft 365

Select an assessment plan for your organization.

Recommended



Office 365 Mailboxes and Potentially Compromised Endpoints

The service scans all messages sent and received in the last 7 to 30 days for all Office 365 users in your environment. After your mailboxes are scanned, you can run the Trend Micro endpoint assessment tool on potentially compromised endpoints. The tool automatically collects and uploads data to the service. All data is stored in a secure database.



Potentially Compromised Endpoints Only

The assessment tool can scan your high-profile endpoints and identify suspicious file activity on potentially compromised systems. After collecting system information and malware samples, the tool automatically uploads the data to the service for in-depth analysis and reporting. All data is stored in a secure database.

Types d'évaluation :


- ✓ Évaluation Microsoft 365
- ✓ Évaluation des Endpoints

Next →





Trend Micro Security Assessment Service

 [Contact Trend Micro](#)

Trend Micro Security Assessment Service needs permission to access mailboxes for assessment scanning. If you are a global administrator of this Office 365 domain, click "Grant Permission" to open the Office 365 permissions page, and then click "Accept".


Important:

- ⓘ Trend Micro does NOT access and store your Office 365 credentials.
- ⓘ Clicking "Accept" on the Office 365 page temporarily grants the application the permissions required to complete the assessment.

[Grant Permission](#)





 Microsoft

Sign in

rachel_jin@TrendCASDemo.onmicrosoft.com

No account? [Create one!](#)

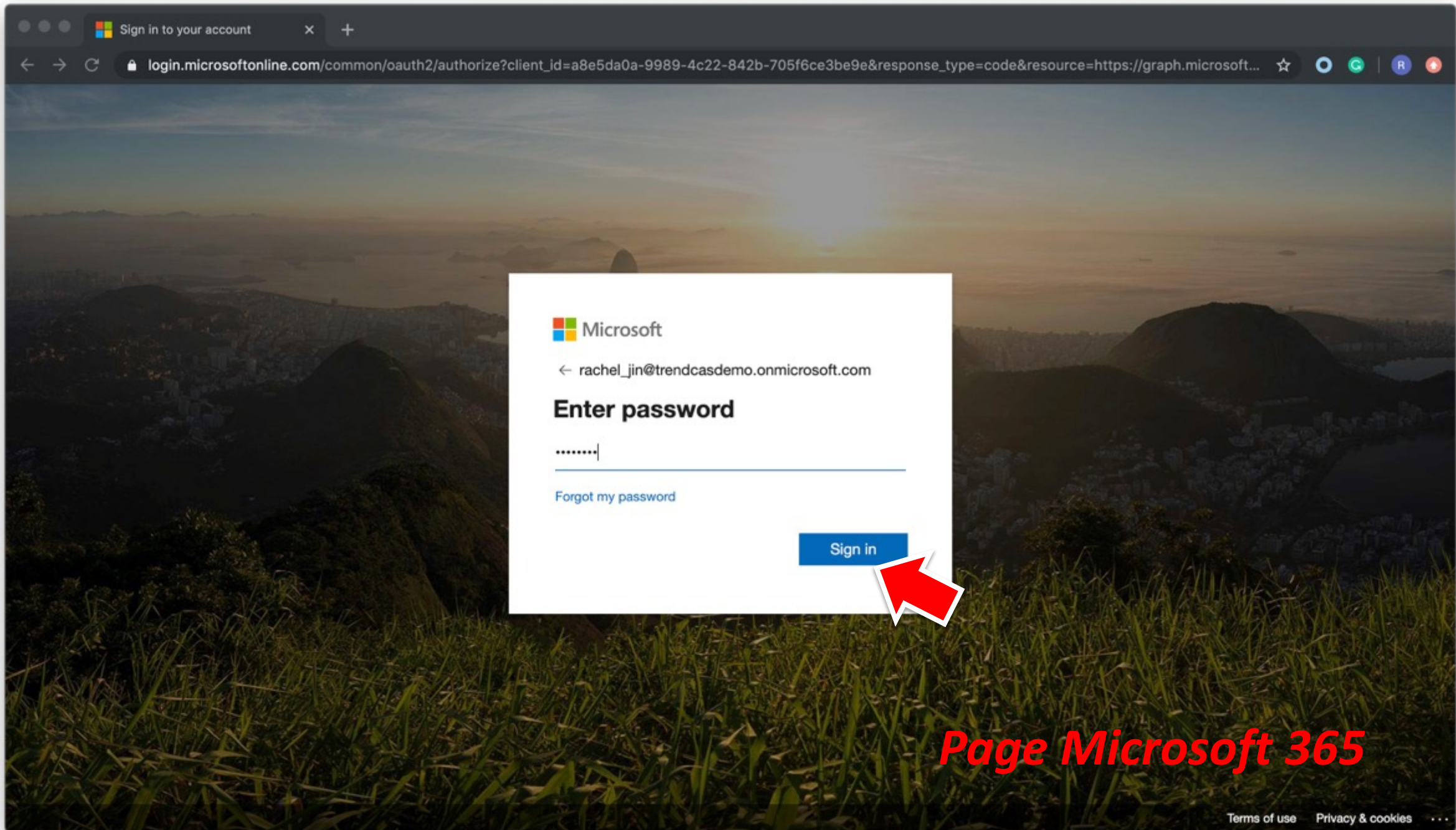
Can't access your account?

[Sign-in options](#)

[Back](#) [Next](#)



Page Microsoft 365



← rachel_jin@trendcasdemo.onmicrosoft.com

Enter password

.....|

[Forgot my password](#)

Sign in



Page Microsoft 365



rachel_jin@trendcasdemo.onmicrosoft.com

Permissions requested Accept for your organization

Trend Micro Cybersecurity Assessment Service
assessment.xdr.trendmicro.com

- This app would like to:
- ✓ Read all administrative units
 - ✓ Read directory data
 - ✓ Read all groups
 - ✓ Read mail in all mailboxes
 - ✓ Read all users' full profiles
 - ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Cancel Accept



Page Microsoft 365

● Permission granted successfully.

Assessment Scope

🔍 All Office 365 users in your environment.

✉ Messages sent and received in the last 7 to 30 days (including spam)

⌚ Depending on the complexity of your environment, the email assessment may take between a few hours and a few days to complete. The results will be sent to your mailbox for review.

← Back

Start Email Assessment →





Email Assessment In Progress

Scanned email messages: 68

Scanned mailboxes: 5/1109

Depending on the complexity of your environment, the email assessment may take between a few hours and a few days to complete. The results will be sent to your mailbox (rachel_jin@trendmicro.com) for review.
You can close the Assessment Portal.

Learn more about [Trend Micro Email Security Solutions](#)

Trend Micro Security Assessment Service - Email Assessment Completed



Trend Micro Security Assessment Service <no-reply@assessment.xdr.trendmicro.com>

Today at 14:41

To: Rachel Jin (PM-CN)

This message was sent from outside of Trend Micro. Please do not click links or open attachments unless you recognise the source of this email and know the content is safe.



Trend Micro Security Assessment Service

Dear Rachel,

The email assessment has been completed. Click the link below to view the report.

Started: 2020-04-07 06:20:29(UTC+00)

Completed: 2020-04-07 06:40:39(UTC+00)

Scanned messages: 199931

Confirmation number: ilsFHG

Portal: [Trend Micro Security Assessment Service](#)

Trend Micro.

Email

Summary

Scan time: (2020-03-18 00:24:38 - 2020-03-18 03:56:31)

1109 Total Mailboxes	5 BEC Messages ▲ Potential cost: \$373,615	56 Phishing Messages	1 Ransomware ▲ Potential cost: \$36,295	52 Malicious Files	167 Malicious URLs
199931 Total Email Messages					

Top Possible Affected Users

	Relative Risk Level	User	Email Address	Job Title (Department)	Associated Endpoints	Reasons
1	● Most at risk	Asim.Khan@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Phishing
2	● Most at risk	Jeffery@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Advanced Spam threats
3	● Most at risk	Tom@xentit.com	Tom@xentit.com	Sales Manager	PC1	Most at risk for Phishing
4	● Most at risk	rkadakia@xentit.com	rkadakia@xentit.com	SVP & CTO	LAPTOP-IARSQLVS	Most at risk for Emergent and Advanced Spam threats
5	● Most at risk	GrantJ@xentit.com	grantj@xentit.com	IT manager(IT Department)	LAPTOP-RUKTBAAF	Most at risk for Phishing, Emergent, and Advanced Spam threats
6	● Most at risk	MariaT@xentit.com	mariat@xentit.com	Finance	GJCQ5IB	Most at risk for Phishing and Advanced Spam threats

The relative risk level reflects the user's exposure to five threat categories in relation to other users in the same environment.

Top Business Email Compromise (BEC) Email Recipients

	Recipient	Subject	Detections	Last Detected
1	"alex bryan"<bryan.alex@navicenthealth.org>	Business report	5	2020-03-18 00:37:13
2	"alex bryan"<bryan.alex@navicenthealth.org>	Request from CEO	5	2020-03-18 00:37:13
3	"alex bryan"<bryan.alex@navicenthealth.org>	Request	5	2020-03-18 00:37:13

Rapport d'évaluation
Microsoft 365

Top Phishing Email Recipients





Top Phishing Email Recipients

	Recipient	Subject	Detections	Last Detected
1	"christopher bryan" <bryan.christopher@navicenthealth.org>	Weekly Report	24	2020-03-18 00:37:13
2	"delladonna.michael" <delladonna.michael@navicenthealth.org>	Log Finding	11	2020-03-18 00:37:13
3	"paul r. johnson"<pjohnson@xentit.com>	Microsoft account	11	2020-03-18 00:37:13
4	"robert jones" <jones.robert02@navicenthealth.org>	Weekly Report	11	2020-03-18 00:37:13

▲ We have noticed certain email threats have made it past your existing security solutions.

i We have noticed certain email threats have made it past your existing security solutions. Threats keep evolving to bypass security solutions. Trend Micro is continuously innovating and evolving our email security solutions to keep up with the latest threats. Ideal for cloud email and collaboration services, Trend Micro™ Cloud App Security is equipped to keep your organization safe. Trend Micro™ Cloud App Security offers advanced threat and data protection to secure email in Microsoft® Office 365®, Gmail™, and across cloud file-sharing services like Box and Dropbox™. CAS combines machine learning, document exploit detection, and behavior analysis to uncover unknown threats such as ransomware and business email compromise (BEC). Learn more about [Trend Micro™ Cloud App Security](#)

Rapport d'évaluation
Microsoft 365

Download PDF Report

Start Endpoint Assessment →

Restart Assessment

Delete My Data



Présentation pas à pas Évaluation de la sécurité des Endpoints

Select an assessment plan for your organization.

Recommended



Office 365 Mailboxes and Potentially Compromised Endpoints

The service scans all messages sent and received in the last 7 to 30 days for all Office 365 users in your environment. After your mailboxes are scanned, you can run the Trend Micro endpoint assessment tool on potentially compromised endpoints. The tool automatically collects and uploads data to the service. All data is stored in a secure database.



Potentially Compromised Endpoints Only

The assessment tool can scan your high-profile endpoints and identify suspicious file activity on potentially compromised systems. After collecting system information and malware samples, the tool automatically uploads the data to the service for in-depth analysis and reporting. All data is stored in a secure database.

Types d'évaluation :

- ✓ Microsoft 365 Assessment
- ✓ Évaluation des Endpoints




Next →


Endpoint Assessment (Note: The tool will expire on 2020-05-07 14:12:38)

Data Collection Disclosure


You can deploy the endpoint assessment tool using any of the following methods.


Send Download Link

The service sends a download link and deployment instructions to specified users.


Copy Download Link

Send a download link and deployment instructions to users using your preferred application.


Download Assessment Tool

Download and run the tool on endpoints using your preferred system utility.

[View Deployment Instructions](#)

3 méthodes pour déployer l'outil d'évaluation des Endpoints

[Copy User List](#)

Endpoints with Collected Data

▲ If deployed correctly, the assessment tool automatically collects and uploads data to the service. Whenever the assessment tool uploads data, the following table displays a timestamp and the service sends a notification to the registered email address.

Possible Compromised Endpoint

Data Uploaded

No Data

[Stop Assessment and Generate Report →](#)

Endpoint Assessment (Note: The tool will expire on 2020-05-07 14:12:38)

[Data Collection Disclosure](#)

You can deploy the endpoint assessment tool using any of the following methods.



Send Download Link

The service sends a download link and deployment instructions to specified users.



Copy Download Link

Send a download link and deployment instructions to users using your preferred application.



Download Assessment Tool

Download and run the tool on endpoints using your preferred system utility.

[View Deployment Instructions](#)

[Copy User List](#)

Endpoints with Collected Data

▲ If deployed correctly, the assessment tool automatically collects and uploads data to the service. Whenever the assessment tool uploads data, the following table displays a timestamp and the service sends a notification to the registered email address.

Possible Compromised Endpoint	Data Uploaded
1 EC2AMAZ-HCPPBUT	2020-03-12 16:54:01
2 LMT-01	2020-03-12 17:25:01
3 PC02	2020-03-13 08:31:01
4 DB-01	2020-03-12 11:25:01

[Stop Assessment and Generate Report →](#)



Endpoints qui ont été évalués

Trend Micro Security Assessment Service - Final Report Generated



Trend Micro Security Assessment Service <no-reply@assessment.xdr.trendmicro.com>

Today at 14:52

To: Rachel Jin (PM-CN)

This message was sent from outside of Trend Micro. Please do not click links or open attachments unless you recognise the source of this email and know the content is safe.

Trend Micro Security Assessment Service

Dear Rachel,

The final report has been generated. Click the link below to view and download the report.

Generated: 2020-04-07 06:52:09(UTC+00)

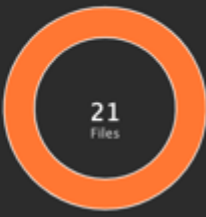
Expiration: 2020-05-07 06:52:09(UTC+00) (Please download the report before this date.)

Confirmation number: ilsFHG

Portal: [Trend Micro Security Assessment Service](#)

Trend Micro. | [Contact Trend Micro Sales](#)

5
Total Endpoints



P920 | IP address: 192.168.0.110 | Operation system: Windows 7 6.1.7601

● Malicious Threats (0)

● Suspicious Threats (5)

- File: C:\Program Files\MiniTool Partition Wizard 11\updatechecker.exe
- File: C:\temp\oABDMb.tmp
- File: C:\Program Files (x86)\Zyxel\Zyxel One Network Utility\tftpd32_svc.exe
- File: C:\Program Files (x86)\QNAP\Qfinder\QfinderPro.exe
- File: C:\Program Files\E-MailRelay\emailrelay-service.exe

LUK-06 | IP address: 192.168.0.111 | Operation system: Windows 7 6.1.7601

● Malicious Threats (0)

● Suspicious Threats (4)

- File: C:\Program Files (x86)\ouMb.tmp
- File: C:\windows\local\temp\eicar.exe
- Process: C:\windows\local\temp\checker.exe
- File: C:\temp\afcdstc\Osfm-00000157.bin

LUK-01 | IP address: 192.168.0.112 | Operation system: Windows 7 6.1.7601

● Malicious Threats (0)

● Suspicious Threats (5)

- File: C:\temp\local.tmp
- File: C:\temp\afb872bx.exe
- File: C:\temp\cgec.exe
- File: C:\temp\ou67Mb.tmp

Rapport d'évaluation des Endpoints





LUK-02 | IP address: 192.168.0.115 | Operation system: Windows 7 6.1.7601

Malicious Threats (0)

Suspicious Threats (6)

- File: C:\Program Files\MiniTool Partition Wizard 11\updatechecker.exe
- File: C:\windows\local\temp\eicar.exe
- File: C:\temp\updater.exe
- File: C:\temp\fad99822dcgew2\Osfm-000002r4efd7.bin
- File: C:\temp\Osfm-00000127.bin
- File: C:\temp\Osfm-00000138.bin

LUK-03 | IP address: 192.168.0.118 | Operation system: Windows 7 6.1.7601

Malicious Threats (0)


Suspicious Threats (4)

- File: C:\Program Files\vcd09e.exe
- File: C:\temp\eic009ar.bin
- File: C:\temp\SVH0st.exe
- File: C:\windows\temp\wtpaf7.bin

Rapport d'évaluation des Endpoints

We have noticed that some endpoint threats have made it past your existing security solutions. We know that threats continue to evolve, that's why Trend Micro consistently adapts to help protect you from the latest evolution of advanced threats. Trend Micro Apex One™ provides automated, insightful, and all-in-one protection for endpoints across your organization. We utilize a blend of advanced threat protection techniques to eliminate security gaps across any user activity and endpoint, while offering integrated add-on capabilities for advanced endpoint and email investigations. [Learn more about Trend Micro Apex One™](#)

Trend Micro™ XDR for Users is a comprehensive SaaS bundle that combines endpoint protection via Trend Micro Apex One™ as a Service, email protection via Trend Micro™ Cloud App Security and advanced investigation capabilities through integrated detection and response capabilities, ideal for customers looking for one offering to meet all their endpoint detection, email detection, and investigation requirements. [Learn more about Trend Micro™ XDR for Users](#)

[Contact Expert](#)
[Try Apex One™](#)
[Try Cloud App Security](#)
[Download PDF Report](#)
[Restart Assessment](#)
[Delete My Data](#)






Présentation pas à pas

Rapport final



Évaluation Microsoft 365 Exemple de rapport

Email

Summary

1109 Total Mailboxes

5 BEC Messages
▲ Potential cost: \$373,615

56 Phishing Messages

1 Ransomware
▲ Potential cost: \$36,295

Scan time: (2020-03-17 16:24:38 - 2020-03-17 19:56:31) (UTC+00)

52 Malicious Files

167 Malicious URLs

199931 Total Email Messages

Top Possible Affected Users

	Relative Risk Level	User	Email Address	Job Title (Department)	Associated Endpoints	Reasons
1	● Most at risk	Asim.Khan@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Phishing
2	● Most at risk	Jeffery@xentit.com	asim.khan@xentit.com	Sales Manager	PC-MAK	Most at risk for Advanced Spam threats
3	● Most at risk	Tom@xentit.com	Tom@xentit.com	Sales Manager	PC1	Most at risk for Phishing
4	● Most at risk	rkadakia@xentit.com	rkadakia@xentit.com	SVP & CTO	LAPTOP-IARSQLYS	Most at risk for Emergent and Advanced Spam threats
5	● Most at risk	Grant.J@xentit.com	grantj@xentit.com	IT manager(IT Department)	LAPTOP-RUKTBAAF	Most at risk for Phishing, Emergent, and Advanced Spam threats
6	● Most at risk	Maria.T@xentit.com	maria.t@xentit.com	Finance	GJCQ5IB	Most at risk for Phishing and Advanced Spam threats

The relative risk level reflects the user's exposure to five threat categories in relation to other users in the same environment.

Top Business Email Compromise (BEC) Email Recipients

	Recipient	Subject	Detections	Last Detected
1	"alex.bryan"<bryan.alex@navicenthealth.org>	Business report	5	2020-03-17 16:37:13 (UTC+00)
2	"alex.bryan"<bryan.alex@navicenthealth.org>	Request from CEO	5	2020-03-17 16:37:13 (UTC+00)
3	"alex.bryan"<bryan.alex@navicenthealth.org>	Request	5	2020-03-17 16:37:13 (UTC+00)

Top Phishing Email Recipients

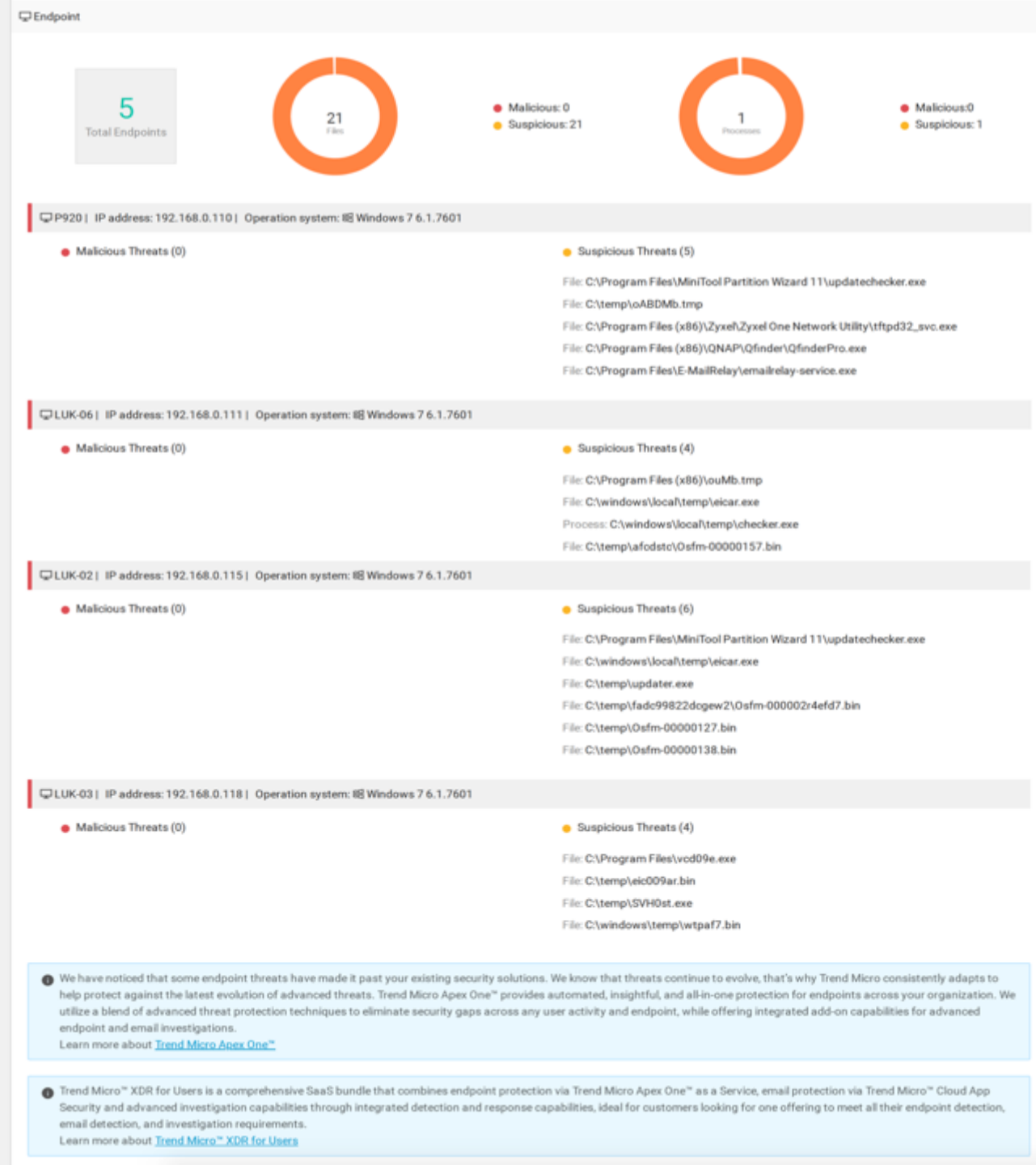
	Recipient	Subject	Detections	Last Detected
1	"christopher.bryan"<bryan.christopher@navicenthealth.org>	Weekly Report	24	2020-03-17 16:37:13 (UTC+00)
2	"delladonna.michael"<delladonna.michael@navicenthealth.org>	Log Finding	11	2020-03-17 16:37:13 (UTC+00)
3	"paul.r.johnson"<pjohnson@xentit.com>	Microsoft account	11	2020-03-17 16:37:13 (UTC+00)
4	"robert.jones"<jones.robert02@navicenthealth.org>	Weekly Report	11	2020-03-17 16:37:13 (UTC+00)

▲ We have noticed certain email threats have made it past your existing security solutions.

● We have noticed certain email threats have made it past your existing security solutions. Threats keep evolving to bypass security solutions. Trend Micro is continuously innovating and evolving our email security solutions to keep up with the latest threats. Ideal for cloud email and collaboration services, Trend Micro™ Cloud App Security is equipped to keep your organization safe. Trend Micro™ Cloud App Security offers advanced threat and data protection to secure email in Microsoft® Office 365®, Gmail™, and across cloud file-sharing services like Box and Dropbox™. CAS combines machine learning, document exploit detection, and behavior analysis to uncover unknown threats such as ransomware and business email compromise (BEC). Learn more about [Trend Micro™ Cloud App Security](#)



Évaluation des Endpoints - Exemple de rapport





Processus d'évaluation, étape par étape

Suppression des données

Trend Micro Cybersecurity Assessment Service

Endpoint

2
Hosts Scanned



PC-TEST-05 | IP address: 10.204.232.4 | Operation System: Windows 10 10.0.17134 | User:

Malicious Security Threat (0) Suspicious Security Threat (0)

NJ-HONGYING-YU1 | IP address: 172.17.175.209;10.64.162.83 | Operation System: Windows 10 10.0.16299 | User:

Malicious Security Threat (0) Suspicious Security Threat (0)

Your current security measures have successfully kept threats out of your organization at this time. However, this scan only assessed a segment of your endpoints. You may still have certain threats impacting additional endpoints. Threats keep evolving to bypass security solutions. Trend Micro is continuously innovating and evolving our endpoint security solutions to keep up with the latest threats. Apex One™ provides automated, insightful, and all-in-one protection for endpoints across your organization. We utilize a blend of advanced threat protection techniques to eliminate security gaps across any user activity and endpoint, while offering integrated add-on capabilities for advanced endpoint and email investigations.

Trend Micro™ XDR for Users is a comprehensive SaaS bundle that combines endpoint protection via Trend Micro Apex One™ as a Service, email protection via Trend Micro™ Cloud App Security and advanced investigation capabilities through integrated detection and response capabilities, ideal for customers looking for one offering to meet all their endpoint detection, email detection, and investigation requirements.
Check more information of [Trend Micro Apex One™](#)

- Contact Expert
- Try Apex One™
- Try Cloud App Security
- Download PDF Report
- Delete My Data

Top Business Email Compromise (BEC) Email Recipients

Recipient	Subject	Detections	Last Detected
Your current security measures have successfully kept threats out of your organization at this time.			

Top Phishing Email Recipients

Recipient	Subject	Detections	Last Detected
1	"rachel jin" <rachel_jin@trendcasdemo.onmicrosoft.com>	5	2019-11-12 20:09:26

Top Ransomware Detections

Ransomware	File	Detections	Last Detected
Your current security measures have successfully kept threats out of your organization at this time.			

Delete Data

All collected data and assessment results will be permanently deleted. You will no longer be able to view and download the report.

If you wish to continue, specify your confirmation number and then click "Confirm."

Confirm Cancel



i We have noticed certain email threats have made it past your existing security solutions. Threats keep evolving to bypass security solutions. Trend Micro is continuously innovating and evolving our email security solutions to keep up with the latest threats. Ideal for cloud email and collaboration services, Trend Micro™ Cloud App Security is equipped to keep your organization safe. Trend Micro™ Cloud App Security offers advanced threat and data protection to secure email in Microsoft® Office 365®, Gmail™, and across cloud file-sharing services like Box and Dropbox™. CAS combines machine learning, document exploit detection, and behavior analysis to uncover unknown threats such as ransomware and business email compromise (BEC). Learn more about [Trend Micro™ Cloud App Security](#)

Download PDF Report

Start Endpoint Assessment →



Delete My Data



Trend Micro Cybersecurity Ass x +

assessment.xdr.trendmicro.com/#/info?infoid=1

Trend Micro Cybersecurity Assessment Service [Contact Trend Micro](#)

  **Data Deleted**

Thank you for using the Trend Micro Cybersecurity Assessment Service. All your data has been deleted.

[Trend Micro Support](#)