

TREND MICRO SECURITY ASSESSMENT

Mehrwerte & Möglichkeiten für Trend Micro Partner

Als Trend Micro Partner können Sie das Security Assessment allen Kunden zur Verfügung stellen, die Microsoft® Office 365® einsetzen. Über ein spezielles Dashboard sind Sie als Partner jederzeit über die Nutzung des Security Assessments durch ihre Kunden informiert.

Der Service ist

- Kostenfrei
- Unverbindlich
- In allen Bestandteilen DSGVO-konform
- Unabhängig von derzeit eingesetzten Email- und Endpunktsicherheitslösungen

Mehrwerte für Sie als Partner

- Positionierung als Experte, um mögliche Sicherheitslücken bei Ihren Kunden in Office 365 zu schließen
- Mehrwert-Dienst adressiert echte Kundenbedürfnisse
- Einfache Durchführung über Web-Interface <https://assessment.xdr.trendmicro.com>
- Individualisierung unterstreicht Partner-Kompetenzen <https://success.trendmicro.com/solution/000244645-How-to-Setup-White-labeled-Cybersecurity-Assessment-Service-Portal-for-Partners>
- Kundenrelevanz unabhängig von vorhandenen Email-Sicherheitslösungen
- Gesprächseinstieg für Zusatzgeschäfte / Ad-ons
- Alle Daten sind für Sie übersichtlich im Dashboard

Zusätzliche Umsatzpotenziale für Sie

- **Cloud App Security**
Identifiziert mehr Email-Bedrohungen u.a. durch den Einsatz von ausgeklügelten Erkennungsverfahren wie Business Email Compromise sowie durch den Vergleich von bekannten Angriffsmustern mit Zero-Day-Attacks (bspw. mit Hilfe von Machine Learning Technologien) basierend auf einer der umfangreichsten Threat-Information-Datenbanken der Welt. Cloud App Security bietet neben der Analyse von Exchange Online, SharePoint Online, OneDrive und Teams, zusätzlich die Analyse von Nicht-Microsoft-Services wie bspw. Gmail, Google Drive, Dropbox und verhindert dadurch Datenverluste sowie die Verbreitung von Bedrohungen.
- **XDR for Users Bundle**
Kombiniert Cloud App Security mit XDR für Endpunkte
- **Worry-Free XDR**
Gut positioniert im MSP-Umfeld. Die Lösung bietet Erkennungs- und Reaktionsfunktionen für E-Mails und Endpunkte. So können Sie gezielte Angriffe schneller erkennen und effektiver darauf reagieren.

Mehrwerte für Ihre Kunden

- Schwachstellen-Analyse von Office 365 E-Mails und Endpunkten
- Report (PDF) über gefundene Bedrohungen
- Minimierung von Sicherheitsrisiken mit Trend Micro Lösungen

Facts & Figures

- Trend Micro blockiert 12,7 Mio. hochgefährliche Malware, die durch die in Office 365-inkludierten Security-Elemente nicht blockiert wurden. [Cloud App Security Report 2019](#)
- Die mit 94% stark überwiegende Angriffsmethode für Malware sind E-Mails.

Quelle: Verizon DDIR 2019

1. Bewerbung und Bekanntmachung des Security Assessments

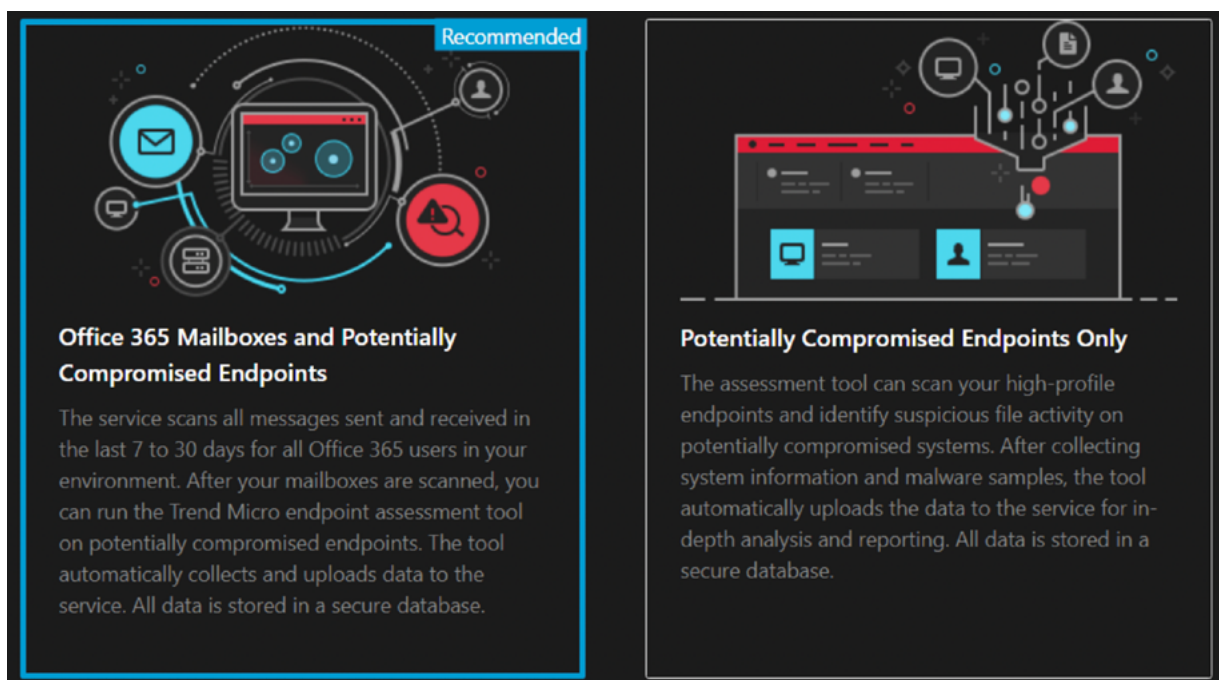
Sie können das Security Assessment für ihre Kunden mit Ihrem Logo und Ihren Kontaktdaten individualisieren und eine entsprechende Bewerbung starten.

- [Security Assessment mit partnerspezifischer URL](#) oder Sie nutzen das allgemeine [Trend Micro Security Assessment für Kunden](#)

2. Möglichkeiten des Kunden durch die Anmeldung zum Security Assessments

Nach der Eingabe ihrer Kontaktinformationen haben Kunden die Wahl zwischen drei Optionen:

- Scan von Office 365 Mailboxen und potenziell gefährdeten Endpunkten
- Nur Scan von Office 365 Mailboxen
- Nur Scan von potenziell gefährdeten Endpunkten



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.

Scan von Mailboxen und/oder Endpunkten

Für den Scan muss der Kunde die entsprechenden Berechtigungen an Trend Micro vergeben. Trend Micro speichert keine Office 365 Credentials.

Permissions requested Accept for your organization

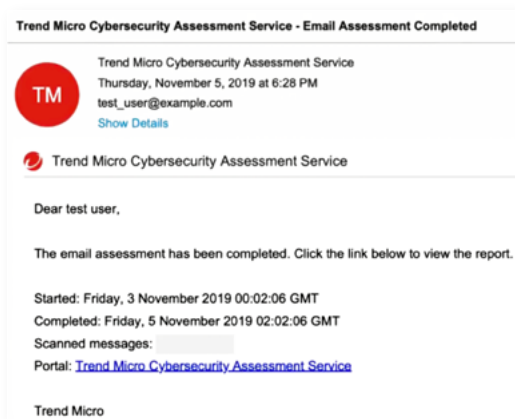
Trend Micro Cybersecurity Assessment Service
assessment.xdr.trendmicro.com

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

Freigabe durch den Kunden

3. Durchführung und Dauer

Nach dem Start überprüft das Security Assessment alle ein- und ausgegangenen E-Mail-Nachrichten von Office 365 Anwendern aus den letzten 7 bis 30 Tagen. Abhängig von der Anzahl an Mailboxen sowie an Mails und Mailgrößen kann dieser Vorgang zwischen einigen Stunden und mehreren Tagen in Anspruch nehmen. Nach Abschluss des Scans erhält der Kunde eine Benachrichtigung per E-Mail.



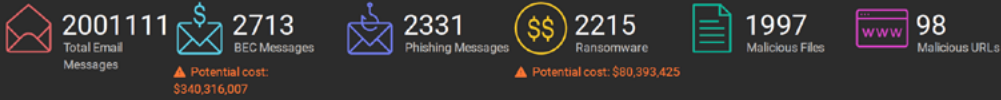
Benachrichtigung über beendeten Email-Scan

Im Anschluss an den Email-Scan können Kunden einen zusätzlichen Scan potenziell gefährdeter Endpunkte mit dem Trend Micro Anti-Threat Toolkit durchführen. Während des Scans werden weitere Informationen gesammelt, im Hintergrund mit den Daten aus dem E-Mail-Scan korreliert (Stichwort „XDR“) und in einem finalen Report zusammengefasst, welcher dem Kunden als PDF zur Verfügung gestellt wird. Die gesamte Datenerhebung und Verarbeitung ist DSGVO-konform. Alle Daten werden automatisch nach 30 Tagen gelöscht oder auf Kundenwunsch auch sofort. Nach Löschung der Daten ist kein Zugriff auf die Ergebnisse mehr möglich, daher empfehlen wir den sofortigen Download des PDFs.

[Weitere Informationen](#)

Email

Summary (10/30/2019 02:39:28 - 10/30/2019 02:39:28)



Top Possible Affected Account

	Relative Risk Level	User	Email Address	Job Title (Department)	Associated Endpoints	Reasons
1	Most at risk	johnny_wu@example.com	johnny_m_wu@example.com			johnny_wu@example.com is in the malware-severity rank 1, and emergent-threat severity rank 2.
2	Least at risk	test111@example.com	test111@example.com	(Core Tech)		test1111@example.com is in the malware-severity rank 1, and emergent-threat severity rank 2.
3	Least at risk	333@example.com	333@example.com	CAO(Finance)		333@example.com is in the malware-severity rank 1, and emergent-threat severity rank 2.
4	Moderate at risk	test222@example.com	test222@example.com	CcO(Consumer)		test222@example.com is in the malware-severity rank 1, and emergent-threat severity rank 2.

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

Top Ransomware Detections

	Ransomware	File Name	Detections	Last Detected
1	Ransom_BLOCCATO.SM	TRENDX_ELF_64_LSB_DYN	2	2019-08-30 01:17:02
2	Ransom.ELF64.TRX.XXELF001	TRENDX_ELF_64_LSB_DYN	2	2019-08-30 01:17:02

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.](#)

Endpoint

3
Total Endpoints

3333
Files

- Malicious (1111)
- Suspicious (2222)

700
Processes

- Malicious (300)
- Suspicious (400)

win10x64-test-1 | IP address: 10.204.232.111 | Operation system: Windows 7 6.1.7601

Malicious Threats (30)

- File |c:\\$recycle.bin\5-21-606064302-1989685767-437890458-500\SIMJSVXD.zip
- File |c:\test111111.zip
- File |c:\test111111.zip
- File |c:\\$recycle.bin\5-21-606064302-1989685767-437890458-500\SRMJSVXD.zip
- File |c:\\$recycle.bin\5-21-606064302-1989685767-437890458-500\SIMJSVXD.zip
- File |c:\test111111.zip
- File |c:\test111111.zip
- File |c:\\$recycle.bin\5-21-606064302-1989685767-437890458-500\SRMJSVXD.zip

Suspicious Threats (20)

- File |c:\\$recycle.bin\5-21-606064302-1989685767
- File |c:\\$recycle.bin\5-21-606064302-1989685767 and 10 more threats found

Auszug und Beispiel eines Assessment Reports für Kunden

4. Optionen zur Individualisierung durch Partner

Trend Micro bietet Partnern die Möglichkeit, das Security Assessment durch Einbindung des eigenen Logos zu individualisieren und über partnerspezifische URLs (z.B. <https://PARTNER.assessment.xdr.trendmicro.com>) ihren Kunden zur Verfügung zu stellen. Zudem können Partner eigene Kontaktadressen in die Kundenkommunikation einbinden. Weitere Informationen zum Thema finden Sie unter dem Stichwort „[Whitelabeling](#)“.

Für das Whitelabeling benötigt Trend Micro neben Ihren Unternehmensinformationen eine Logo-Datei, die folgende Anforderungen erfüllen sollte:

- SVG Dateiformat
- Mindestens 120x40 Pixel
- Landscape-Ausrichtung
- Weißer oder schwarzer Hintergrund

Partner's Logo

Welcome to the %PartnerName% Cybersecurity Assessment Service

Want to find out how well your email and endpoint security is really performing? Run our %PartnerName% Security Assessment Service to see if you are currently protected against malicious attacks.

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 email inboxes and endpoints are scanned to find threats that have evaded existing protections
2. We give you a snapshot of your security posture so you can see how well you are protected against the latest advanced threats today
3. You are invited to learn more about the vulnerabilities in your security strategy and the new security solutions that can help fill the gaps

Powered by TREND MICRO

Try it Now

First name: *

Last name: *

Company name:

Region:

Work email address:

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

START ->

Already registered? [Log On](#)

Anmeldeseite mit Platzhaltern für Partner-Logo und Namen

5. Weitere Informationen

In den folgenden YouTube-Videos erhalten Sie weitere Informationen zum Security Assessment Service.

- [Vorstellung Security Assessment Service](#)
- [Anleitung Security Assessment](#)



©2020 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo, Deep Security, Trend Micro Deep Security AntiVirus for VDI, Trend Micro Deep Security Virtual Patch und Trend Micro Control Manager sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen-bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.