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-Attacken (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

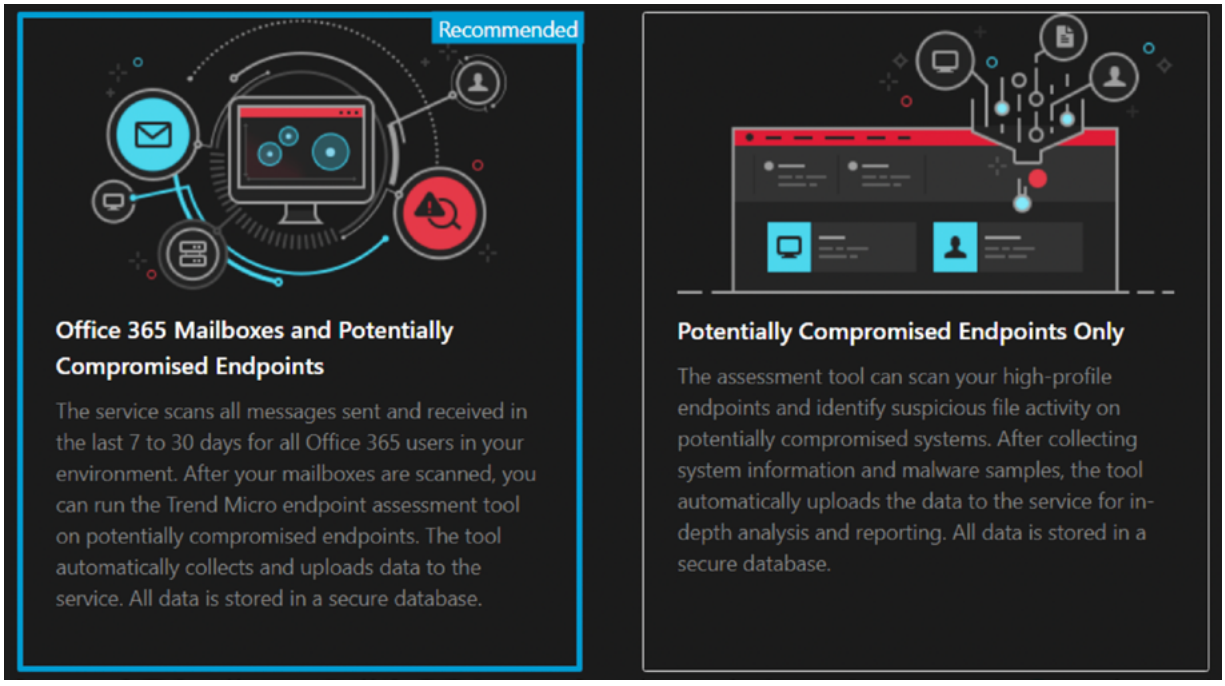
Sie können das Security Assessment für ihre Kunden mit Ihrem Logo und Ihren Kontaktdaten individualisieren und eine entsprechende Bewerbung starten.

- Security Assessment mit partnerspezifiischer URL oder Sie nutzen das allgemeine Trend Micro Security Assessment für Kunden

2. Möglichkeiten des Kunden durch die Anmeldung zum Security Assessments

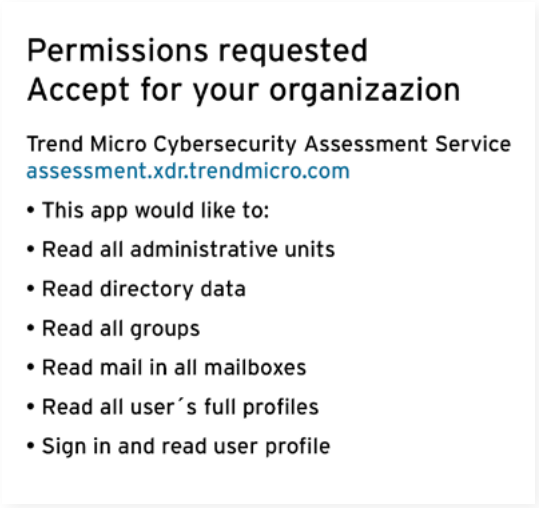
Nach der Eingabe ihrer Kontaktinformationen haben Kunden die Wahl zwischen drei Optionen:

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



Scan von Mailboxen und/oder Endpunkten

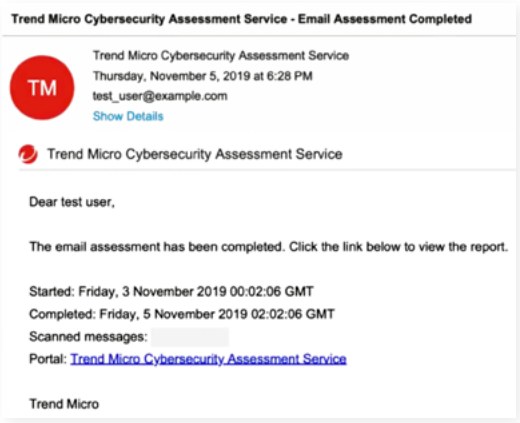
Für den Scan muss der Kunde die entsprechenden Berechtigungen an Trend Micro vergeben. **Trend Micro speichert keine Office 365 Credentials.**



Freigabe durch den Kunden

3. Durchführung und Dauer

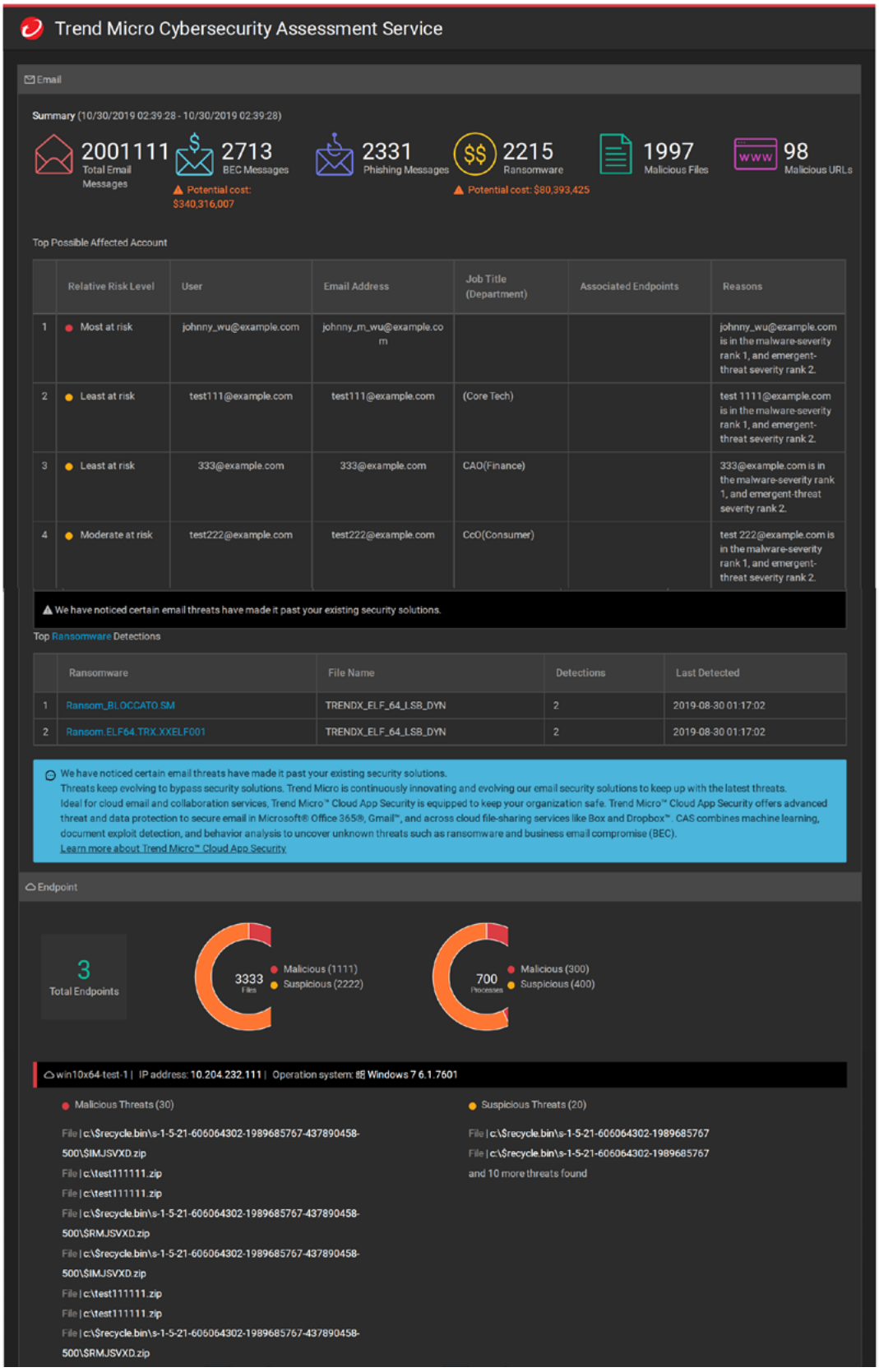
Nach dem Start überprüft das Security Assessment alle ein- und ausgegangenen E-Mail-Nachrichten von Office 365 Anwendern aus den letzten 7 bis 30 Tagen. Abhängig von der Anzahl an Mailboxen sowie an Mails und Mailgrößen kann dieser Vorgang zwischen einigen Stunden und mehreren Tagen in Anspruch nehmen.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



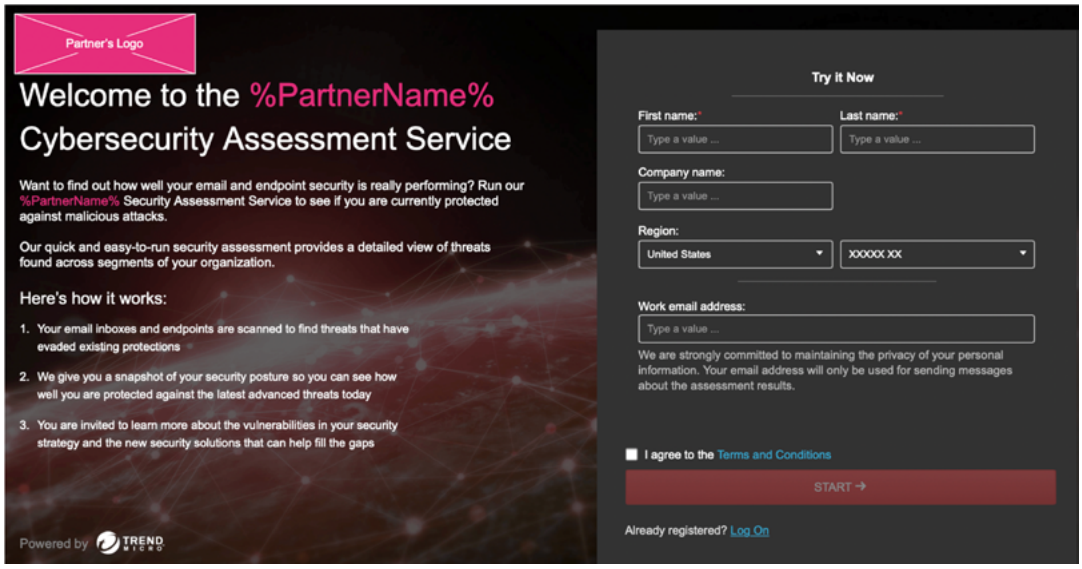
Auszug und Beispiel eines Assessment Reports für Kunden

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



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