

Trend Micro™

# CUSTOMER SUCCESS SERVICES

Soyez reconnus en tant que partenaire de confiance par vos clients

Trend Micro propose ses Customer Success Services à l'intention de ses partenaires pour les positionner en tant que prestataire de confiance vis-à-vis de leurs clients. En tirant parti de **Trend Micro™ Security Assessment Service** (évaluation de la sécurité) et des **Best Practice Guides** (guides de bonnes pratiques), nos partenaires revendeurs et d'intégration sont outillés pour évaluer la sécurité des environnements de leurs clients et prospects, mais aussi pour les guider dans la mise en œuvre des bonnes pratiques de sécurité.

## TREND MICRO SECURITY ASSESSMENT SERVICE

Cet audit de sécurité, rapide et simple, permet aux partenaires d'offrir à leurs prospects une visibilité détaillée sur les menaces email et Endpoints présentes sur tous les segments de leur entreprise. Les performances et la pertinence de la sécurité email et Endpoint en place sont ainsi évalués.

Avec Security Assessment Service, nos partenaires disposent d'un moyen simple pour aider les prospects à :

- Vérifier les menaces par email sur Microsoft 365®
- Analyser les Endpoints à la recherche de menaces
- Offrir un rapport de synthèse à l'intention des décideurs chez le prospect

Nous offrons à nos clients un pack marketing sur **Security Assessment Service** comprenant :

- **Marketing email** : utilisez ce modèle email pour inciter vos prospects et clients à évaluer leur sécurité. Cet email peut être utilisé en co-branding avec le logo du partenaire et ses informations de contact, aux côtés de ceux de Trend Micro. Ce modèle est disponible sur le portail partenaires, **dans la rubrique "Email Marketing"**.

| EDM | SUBJECT   | DATE UPLOADED | LANGUAGE |         |
|-----|---|---------------|----------|---------|
| 1   | <b>Trend Micro Security Assessment Service</b>          | 2020-02-09    | English  | Preview |
| 2   | Hybrid Cloud/Cloud One - Cloud Workload Security Leader | 2020-02-09    | English  | Pre     |
| 3   | Hybrid Cloud/Cloud One - Conformity                     | 2020-03-26    | English  | Pre     |
| 4   | Hybrid Cloud/Cloud One - Conformity Free Trial          | 2020-03-26    | English  | Pre     |
| 5   | Hybrid Cloud/Cloud One - Conformity's Knowledge Base    | 2020-03-26    | English  | Pre     |

### 1. Modèle d'invitation par email

- **Page d'accueil en marque blanche pour Security Assessment** : Trend Micro propose à ses partenaires son service d'évaluation en marque blanche. La page d'accueil du service est proposée en co-branding, avec le logo et l'icône du partenaire. Nos partenaires peuvent demander la création de cette page co-brandée à partir du portail partenaires, rubrique "Security Assessment White-label Request Form".

The screenshot shows a web browser window with the URL `Test LLC-assessment.xdr.trendmicro.com/#/`. The page features a dark background with a network diagram. The main heading is "Welcome to the Test LLC Security Assessment Service". A red box highlights the "Test LLC" logo in the top left. A red box highlights the URL in the browser's address bar. A red box highlights the "Test LLC" logo in the top left of the page content. A red box highlights the Trend Micro logo in the bottom right corner. The page includes a "Try it Now" form with fields for First name, Last name, Job title, Company name, Region (dropdowns for United States and AK), and Work email address. A "START" button is at the bottom of the form. A red box highlights the "START" button. A red box highlights the "Log On" link. A red box highlights the "Sample Partner Branding" button. A red box highlights the "I agree to the Terms and Condition" checkbox. A red box highlights the "Privacy Notice" link. A red box highlights the "Data Collection Disclosure" link. A red box highlights the "Third-party License Information" link. A red box highlights the "Powered by Trend Micro" logo.

## 2. Page d'accueil Security Assessment en marque blanche

### Trend Micro Security Assessment offre les services suivants à ses clients :

- **Évaluation de l'email** : le service analyse tous les messages envoyés et reçus sur les 15 à 30 derniers jours, sur l'ensemble des utilisateurs de Microsoft 365® du client. En fin d'analyse, un rapport offre des résultats détaillés de l'évaluation et indique le nombre total d'emails analysés, ainsi que les principaux utilisateurs impactés.
- **Évaluation des Endpoints** : le service s'exécute sur des Endpoints potentiellement piratés et identifiés dans le rapport d'évaluation de l'email. Il identifie les activités suspectes, recueille des informations systèmes et des échantillons de menaces, puis utilise ces données à des fins d'analyse et de reporting en profondeur. La synthèse affiche le nombre total d'Endpoints analysés et le nombre total d'éléments malveillants et suspects identifiés.

**Trend Micro Security Assessment Service**

**Summary**

- 1109 Total Mailboxes
- 5 BCC Messages
- 56 Phishing Messages
- 1 Ransomware
- 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@...com | Sales Manager             | PC-MAX               | Most at risk for Phishing                                      |
| 2                   | Most at risk | Jeffery@...com   | Sales Manager             | PC-MAX               | Most at risk for Advanced Spam threats                         |
| 3                   | Most at risk | Tom@...com       | Sales Manager             | PCI                  | Most at risk for Phishing                                      |
| 4                   | Most at risk | rkadik@...com    | SVP & CTO                 | LAPTOP-IAR5QLVS      | Most at risk for Emergent and Advanced Spam threats            |
| 5                   | Most at risk | Grant@...com     | IT manager(IT Department) | LAPTOP-BUK2BAAF      | Most at risk for Phishing, Emergent, and Advanced Spam threats |
| 6                   | Most at risk | MariaT@...com    | Finance                   | GJ005B               | Most at risk for Phishing and Advanced Spam threats            |

**Top Business Email Compromises (BEC) Email Recipients**

| Recipient                       | Subject          | Detections | Last Detected                |
|---------------------------------|------------------|------------|------------------------------|
| 'Siles bryan@bryan.alex@...com' | Business report  | 5          | 2020-03-17 16:37:13 (UTC+00) |
| 'Siles bryan@bryan.alex@...com' | Request from CEO | 5          | 2020-03-17 16:37:13 (UTC+00) |
| 'Siles bryan@bryan.alex@...com' | Request          | 5          | 2020-03-17 16:37:13 (UTC+00) |

**Top Phishing Email Recipients**

| Recipient                   | Subject           | Detections | Last Detected                |
|-----------------------------|-------------------|------------|------------------------------|
| 'christopher bryan@...com'  | Weekly Report     | 24         | 2020-03-17 16:37:13 (UTC+00) |
| 'yellidonna.michael@...com' | Log Finding       | 11         | 2020-03-17 16:37:13 (UTC+00) |
| 'yobert.johnson@...com'     | Microsoft account | 11         | 2020-03-17 16:37:13 (UTC+00) |
| 'yobert.johnson@...com'     | Weekly Report     | 11         | 2020-03-17 16:37:13 (UTC+00) |

3.1. Évaluation des Endpoints - Exemple de rapport

**Trend Micro Security Assessment Service**

**Potentially Compromised Endpoints (Threat Indicator Assessment)**

**Summary**

- 18 Total endpoints
- 12 Affected endpoints
- 11 Typos
- 0 Keylogger
- 3 Other Malware

**Affected Endpoints**

| Endpoint name       | IP address | Operating system    | Detections |
|---------------------|------------|---------------------|------------|
| 1. In-test endpoint | 10.1.123.1 | Microsoft windows 7 | 1          |
| 2. In-test endpoint | 10.1.123.1 | Microsoft windows 7 | 2          |

**Typos**

| Detection name             | Endpoint name    | File path      | File created        | Last accessed       |
|----------------------------|------------------|----------------|---------------------|---------------------|
| 1. W002 Malicious THROGARO | in-test endpoint | c:\windows.com | 2020-04-06 07:06:22 | 2020-04-06 07:06:22 |
| 2. W002 Malicious THROGARO | in-test endpoint | c:\windows.com | 2020-04-06 07:06:22 | 2020-04-06 07:06:22 |

**Keylogger**

| Detection name              | Endpoint name    | File path      | File created        | Last accessed       |
|-----------------------------|------------------|----------------|---------------------|---------------------|
| 1. W002 Malicious Keylogger | in-test endpoint | c:\windows.com | 2020-04-06 07:06:22 | 2020-04-06 07:06:22 |
| 2. W002 Malicious Keylogger | in-test endpoint | c:\windows.com | 2020-04-06 07:06:22 | 2020-04-06 07:06:22 |

**Other Malware**

| Type       | Detection name         | Endpoint name    | File path      | File created        | Last accessed       |
|------------|------------------------|------------------|----------------|---------------------|---------------------|
| 1. Spyware | W002 Malicious Spyware | in-test endpoint | c:\windows.com | 2020-04-06 07:06:22 | 2020-04-06 07:06:22 |
| 2. Spyware | W002 Malicious Spyware | in-test endpoint | c:\windows.com | 2020-04-06 07:06:22 | 2020-04-06 07:06:22 |

**Details**

In-test endpoint | Detections: 14 | IP address: 10.1.123.1 | Operating system: Microsoft windows 7

- W002 Malicious THROGARO - c:\windows.com (File created: 2020-04-06 07:06:22 | Last accessed: 2020-04-06 07:06:22)
- W002 Malicious THROGARO - c:\windows.com (File created: 2020-04-06 07:06:22 | Last accessed: 2020-04-06 07:06:22)
- W002 Malicious THROGARO - c:\windows.com (File created: 2020-04-06 07:06:22 | Last accessed: 2020-04-06 07:06:22)
- W002 Malicious Keylogger - c:\windows.com (File created: 2020-04-06 07:06:22 | Last accessed: 2020-04-06 07:06:22)
- W002 Malicious Keylogger - c:\windows.com (File created: 2020-04-06 07:06:22 | Last accessed: 2020-04-06 07:06:22)

**Are you seeking protection from future threat campaigns?**

**Do you want to take a broader perspective on detection and response?**

3.2. Évaluation des Endpoints - Exemple de rapport

## BEST PRACTICE GUIDE

### Rapport de sécurité et de conformité pour Trend Micro Apex One™ et Trend Micro™ OfficeScan™

Ce rapport fournit une synthèse du statut des environnements Trend Micro Apex One™ et Trend Micro™ OfficeScan™ d'un client, en conformité avec les bonnes pratiques recommandées par Trend Micro.

En exécutant cet outil avec l'aide du partenaire, les clients bénéficient d'avantages concrets :

- Une évaluation du statut actuel de leur solution de sécurité Endpoint, ainsi que des recommandations de bonnes pratiques pour maximiser leur niveau de sécurité.
- Les clients s'assurent que Trend Micro Apex One™ et Trend Micro™ OfficeScan™ exécutent leurs analyses de manière régulière et que ces solutions sont configurées avec les services pertinents, des composants actualisés et des paramètres cohérents.
- Un rapport qui détaille les recommandations et pré-requis pour une migration vers Trend Micro Apex One™ (clients d'OfficeScan).

**High-level Executive Summary**

Overall Results for: WAYNE-HSU-SQL2016

Apex One Server: Apex One, Build 1071 (EN) (release date 2019/04/03)

**5/10 Security Rating**

**Summary**

| Platforms       | Total    | Online   | Offline  | Compliance Rating |
|-----------------|----------|----------|----------|-------------------|
| Apex One Server | 1        | 1        | 0        | 50%               |
| Desktop Agents  | 2        | 1        | 1        | 50%               |
| Server Agents   | 1        | 1        | 0        | 50%               |
| <b>Total</b>    | <b>3</b> | <b>2</b> | <b>1</b> |                   |

**Agent Release Distribution**

| Release description | Workstations | Servers |
|---------------------|--------------|---------|
| 14.0.x.x.x.x.x.x    | 2            | 1       |

**Advanced Feature Compliancy**

| Module Name                           | Average Compliancy | %   | Fully Compliant Agents | %   |
|---------------------------------------|--------------------|-----|------------------------|-----|
| Smart Scan (File Reputation Services) | 100                | 100 | 100                    | 100 |
| Real-Time Scan                        | 50                 | 0   | 0                      | 0   |
| Web Reputation                        | 100                | 100 | 100                    | 100 |
| Suspicious Connection Service         | 83                 | 0   | 0                      | 0   |
| Behavior Monitoring                   | 78                 | 0   | 0                      | 0   |
| Predictive Machine Learning           | 100                | 100 | 100                    | 100 |
| Apex One Agent Self-protection        | 100                | 100 | 100                    | 100 |
| Device Control                        | 100                | 100 | 100                    | 100 |
| Integrated Application Control        | 0                  | 0   | 0                      | 0   |

**Key Findings**

- The Security is affected by 9 Vulnerabilities and 1 Critical Issue (See Hostry\_2170 from 2020/05/28).
- Having outdated Product versions may not offer all users the benefit of advanced Apex One features.
- Strong Encryption between the Apex One Agents and Server is disabled.

Apex One Best Practice Guide: Security Compliance

**1. Report Overview**

The primary objective of this report is to provide the current status of endpoints protected by Apex One and make recommendations specifically targeted at increasing the overall security posture for your implementation. This report provides the following information:

- Recommendations about how to improve the network security provided by Apex One.
- An overview of the currently deployed Apex One agent versions.
- An assessment of the current Apex One server build compliance and the availability of hotfixes, patches, or enhancements.
- An overview of the protected operating systems.

**Apex One Server Details**

Apex One Build 1071 | 14.0.x.9999

Available Solutions: 58/35 | Apex One Agent Versions: 50% Overall Security Rating

**Apex One Agent Details**

67% Desktop Platforms | 56% Overall Security Rating

Apex One agents: 2 | Version Distribution: Homogeneous

Created on Jun 11, 2020 | CONFIDENTIAL - Release Pursuant to NDA - CONFIDENTIAL

### 4. Sécurité et conformité - Exemple de rapport Trend Micro Apex One™ et OfficeScan

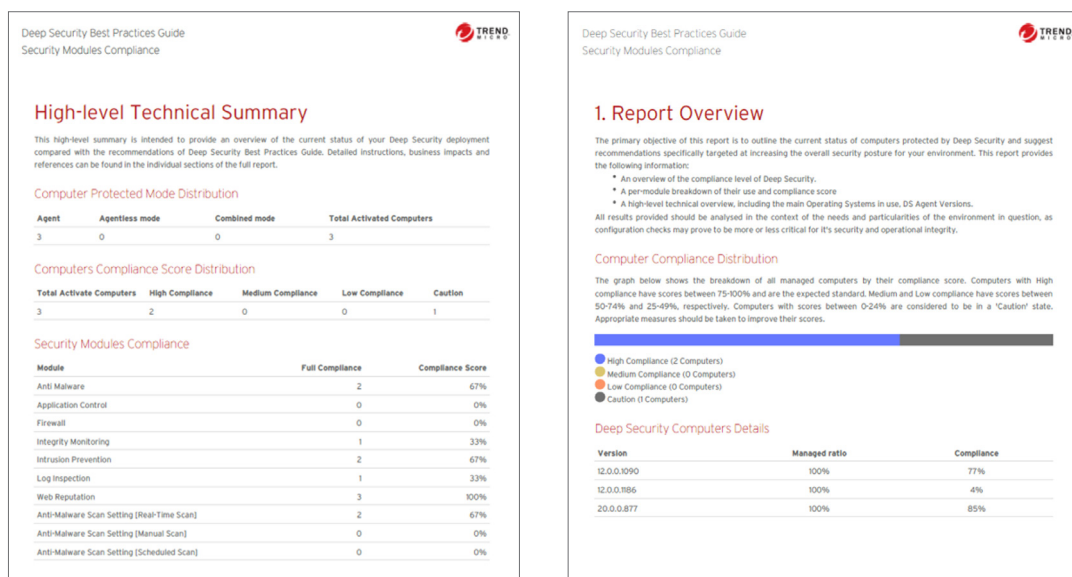
## Rapport de sécurité et de conformité pour Trend Micro Deep Security™

Ce rapport de synthèse donne une vue d'ensemble du statut de l'environnement Deep Security, selon des critères définies par les recommandations du guide des bonnes pratiques pour Deep Security. Des instructions et une description des impacts métiers font l'objet de sections détaillées dans ce rapport.

En exécutant cet outil avec l'aide du partenaire, les clients disposent d'avantages concrets :

- Une synthèse technique globale, notamment sur les principaux systèmes d'exploitation utilisés et les versions de l'agent Trend Micro™ Deep Security™.
- Une synthèse du niveau de conformité de Deep Security.
- Un audit sur l'utilisation de chaque module et un score de conformité pour chacun d'entre eux.

Tous les résultats obtenus doivent être analysés en prenant en compte les besoins et spécificités de l'environnement évalué, puisque les évaluations de conformité peuvent être plus ou moins essentielles pour la sécurité et l'opérationnel de cet environnement.



### 5. Exemple de rapport de sécurité et de conformité pour Trend Micro Deep Security™

Si vous souhaitez utiliser nos services d'évaluation pour accompagner vos clients et prospects, merci de soumettre votre demande via le portail partenaires.

Nous avons conçu des documents de formation pour apporter à nos partenaires davantage d'informations sur ces évaluations de sécurité et le guide de bonnes pratiques.

Connectez-vous au **Portail partenaires** et téléchargez ces documents dans la rubrique "**Customer Success**". Vous pourriez bénéficier de remises supplémentaires en enregistrant une opportunité d'affaire suite de l'utilisation de Trend Micro Security Assessment Service ou du guide des bonnes pratiques. N'oubliez pas d'enregistrer une telle opportunité (Deal Registration), ni de mentionner votre utilisation de ces services et outils.

Trend Micro aide ses partenaires à se positionner en tant que partenaires de confiance vis-à-vis de leurs clients et prospects.

Pour toute question ou demande de support, merci de nous contacter sur [partnersupport@trendmicro.com](mailto:partnersupport@trendmicro.com)

Pour toute information sur les données personnelles que nous recueillons et les raisons pour lesquelles nous les recueillons, merci de consulter notre charte de confidentialité sur : <https://www.trendmicro.com/privacy>



©2020, Trend Micro Incorporated. Tous droits réservés. Trend Micro et le logo Trend Micro sont des marques déposées ou des marques commerciales de Trend Micro Incorporated. Toutes les autres marques et nom de produit ou d'entreprise sont susceptibles d'être déposés et appartiennent à leurs détenteurs respectifs. Les informations présentées dans ce document sont susceptibles d'être modifiées sans préavis. Données non contractuelles. [DSO]\_Customer\_Success\_Services\_Datasheet\_201116FR]