Guide des bonnes pratiques Rapport de conformité à la sécurité à l'intention des partenaires

Trend Micro

Sommaire

- Objectifs
- Contenu du rapport de conformité à la sécurité et exemple de rapport
- Étapes préconisées
- Soumettre une demande de rapport via le portail partenaires
- Solutions/opportunités recommandées pour échanger avec les clients
  - Tirer parti du rapport pour présenter au client les opportunités de mise à niveau
- Enregistrement d’offres et Incentives
- Ressources de support

Objectifs

- Ce rapport de conformité à la sécurité* présente le statut de l'environnement Trend Micro Apex One™ / Trend Micro™ OfficeScan™ d'un client et un benchmark par rapport aux meilleures pratiques recommandées de Trend Micro
- Générer des opportunités de mise à niveau ou de services sur la base de ce rapport de conformité
- Produits cibles : Apex One, OfficeScan

*Security Compliance Report

Contenu du rapport de conformité

- Le rapport de conformité à la sécurité indique le statut des Endpoints protégés par Apex One / OfficeScan et donne des recommandations sur les moyens de renforcer le niveau général de la sécurité des environnements de clients.
- Ce rapport de conformité offre :
  - Des préconisations pour améliorer la sécurité réseau qu'offre Apex One
  - Une synthèse sur les versions de l'agent Apex One déployé
  - Une évaluation de la conformité du serveur Apex One (version existante) et une indication des patchs et améliorations disponibles
  - Une synthèse des systèmes d'exploitation protégés

Contenu du rapport de conformité à la sécurité

Infos disponibles :

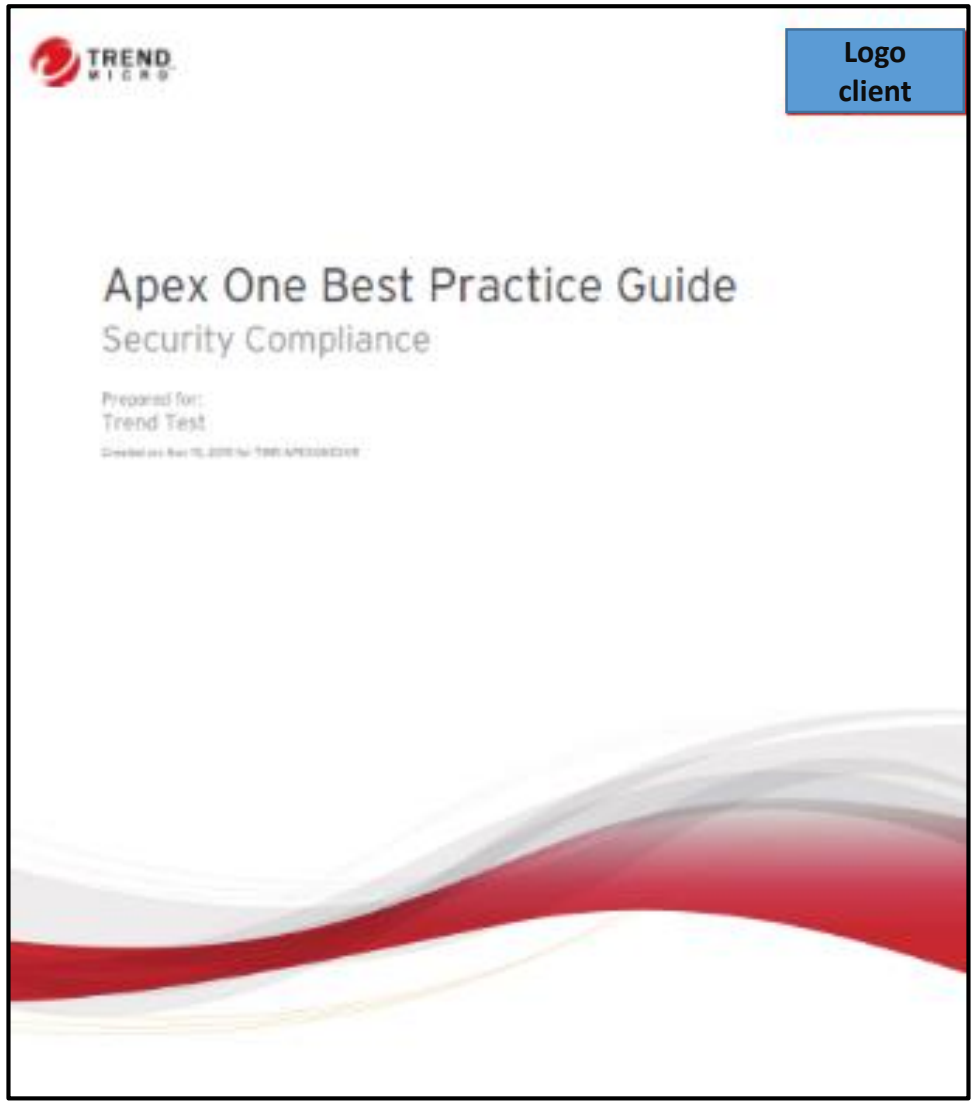
- Conformité des règles de l'agent OfficeScan
- Patchs/correctifs disponible selon la criticité
- Paramètres de sécurité recommandés

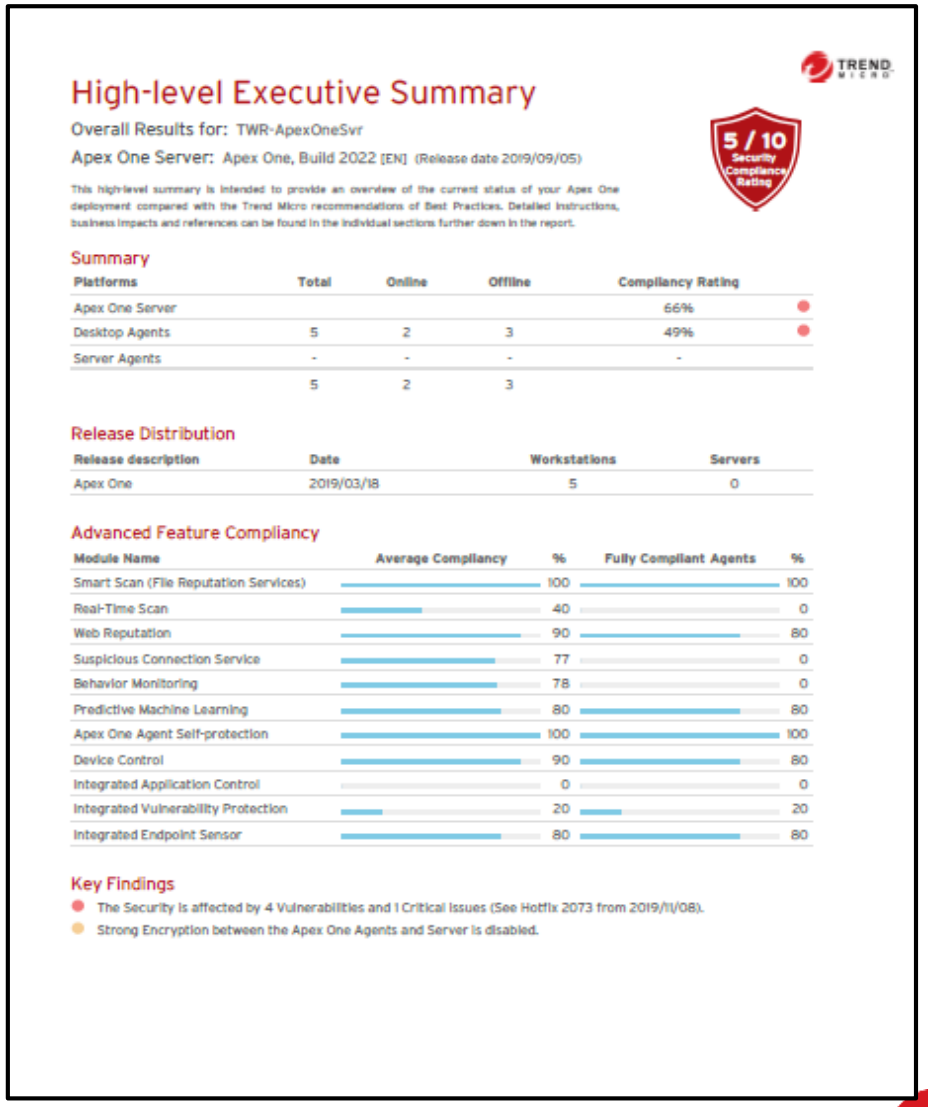
- Score global
- Conformité
- Périmètre de l'environnement
- Recommandations sur les règles
- Recommandations sur les patchs/mises à niveau

Summary

Platforms	Total	Online	Offline	Compliancy Rating
OfficeScan Server				50%
Desktop Agents	550	238	312	75%
Server Agents	-	-	-	-

Guide des bonnes pratiques - Exemple de rapport (1/2)





High-level Executive Summary

Overall Results for: TWR-ApexOneSvr

Apex One Server: Apex One, Build 2022 [EN] (Release date 2019/09/05)

5 / 10 Security Compliance Rating

This high-level summary is intended to provide an overview of the current status of your Apex One deployment compared with the Trend Micro recommendations of Best Practices. Detailed instructions, business impacts and references can be found in the individual sections further down in the report.

Summary

Platforms	Total	Online	Offline	Compliancy Rating
Apex One Server				66%
Desktop Agents	5	2	3	49%
Server Agents	-	-	-	-
	5	2	3	

Release Distribution

Release description	Date	Workstations	Servers
Apex One	2019/03/18	5	0

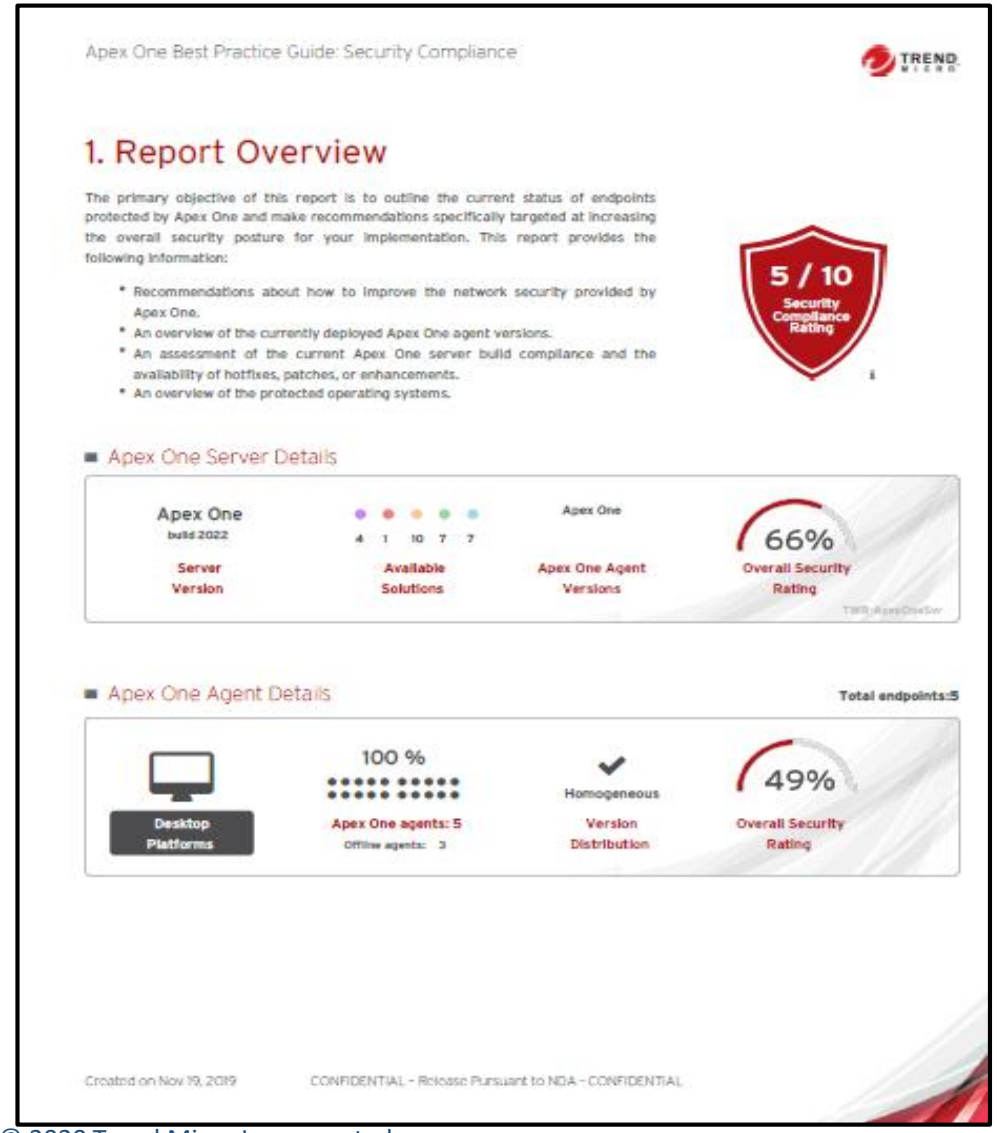
Advanced Feature Compliancy

Module Name	Average Compliancy %	Fully Compliant Agents %
Smart Scan (File Reputation Services)	100	100
Real-Time Scan	40	0
Web Reputation	90	80
Suspicious Connection Service	77	0
Behavior Monitoring	78	0
Predictive Machine Learning	80	80
Apex One Agent Self-protection	100	100
Device Control	90	80
Integrated Application Control	0	0
Integrated Vulnerability Protection	20	20
Integrated Endpoint Sensor	80	80

Key Findings

- The Security is affected by 4 Vulnerabilities and 1 Critical Issues (See Hotfix 2073 from 2019/11/08).
- Strong Encryption between the Apex One Agents and Server is disabled.

Guide des bonnes pratiques - Exemple de rapport (2/2)



Apex One Best Practice Guide: Security Compliance

1. Report Overview

The primary objective of this report is to outline 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.

5 / 10
Security Compliance Rating

Apex One Server Details

Apex One
build 2022
Server Version

4 1 10 7 7
Available Solutions

Apex One
Apex One Agent Versions

66%
Overall Security Rating

Apex One Agent Details

Total endpoints:5

Desktop Platforms

100 %
Apex One agents: 5
Offline agents: 3

Homogeneous
Version Distribution

49%
Overall Security Rating

Created on Nov 19, 2019 CONFIDENTIAL - Release Pursuant to NDA - CONFIDENTIAL

Smart Scan (File Reputation Services)

Fully compliant agents: 5/5 (100%)

Apex One agents using Smart Scan leverage light-weight patterns and cloud reputation queries to provide the same protection provided by conventional anti-malware and anti-spyware patterns. Smart Scan agents perform scanning locally and if the local scan is unable to determine the risk of a file, a query is sent to Smart Protection sources. Smart Scan agents cache the query results to improve scan operations.

100%
Average Compliancy

Real-Time Scan

Fully compliant agents: 0/5 (0%)

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks.

40%
Average Compliancy

Web Reputation

Fully compliant agents: 4/5 (80%)

Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. When a user attempts to access a website, the Apex One agent queries a smart protection source to ascertain the risk level of the content.

90%
Average Compliancy

Suspicious Connection Service

Fully compliant agents: 0/5 (0%)

The Suspicious Connection Service manages the User-defined and Global IP C&C lists, and monitors the behavior of connections that endpoints make to potential C&C servers.

77%
Average Compliancy

Behavior Monitoring

Fully compliant agents: 0/5 (0%)

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or installed software. Through use of Malware Behavior Blocking and Event Monitoring, Behavior Monitoring protects endpoints against unconventional threats, such as ransomware attacks.

78%
Average Compliancy

Predictive Machine Learning

Fully compliant agents: 4/5 (80%)

Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis or behavioral process and script analysis to detect emerging unknown security risks.

80%
Average Compliancy

Apex One Agent Self-protection

Fully compliant agents: 5/5 (100%)

Apex One agent self-protection provides ways for the Apex One agent to protect the processes and other resources required to function properly. Self-protection helps thwart attempts by programs or actual users to disable anti-malware protection.

100%
Average Compliancy

Device Control

Fully compliant agents: 4/5 (80%)

Device Control regulates access to external storage devices and network resources connected to endpoints. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

90%
Average Compliancy

Created on Nov 19, 2019 CONFIDENTIAL - Release Pursuant to NDA - CONFIDENTIAL

Apex One Best Practice Guide: Security Compliance

Integrated Application Control

Fully compliant agents: 0/5 (0%)

Integration with Application Control provides Apex One users with advanced application blocking and endpoint lockdown capabilities. You can run application inventories and create policy rules that only allow specific applications to execute on your endpoints. You can also create application control rules based on application category, vendor, or version.

0%
Average Compliancy

Integrated Vulnerability Protection

Fully compliant agents: 1/5 (20%)

Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with recommended Intrusion Prevention rules based on your network performance and security priorities.

20%
Average Compliancy

Integrated Endpoint Sensor

Fully compliant agents: 4/5 (80%)

Integration with Endpoint Sensor allows you to monitor, record, and perform both current and historical security investigations on your Apex One endpoints. Use the Apex Central console and perform preliminary investigations to locate at-risk endpoints before executing an in-depth Root Cause Analysis to identify the attack vectors.

80%
Average Compliancy

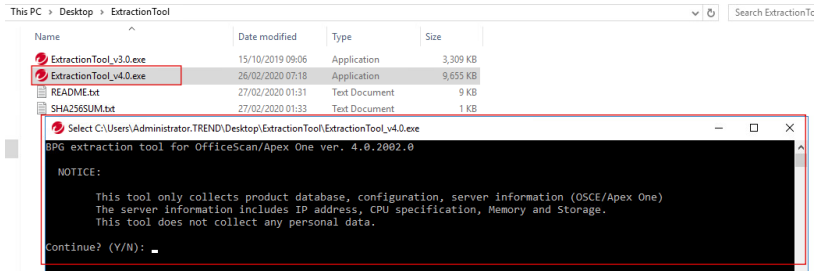
Étapes recommandées

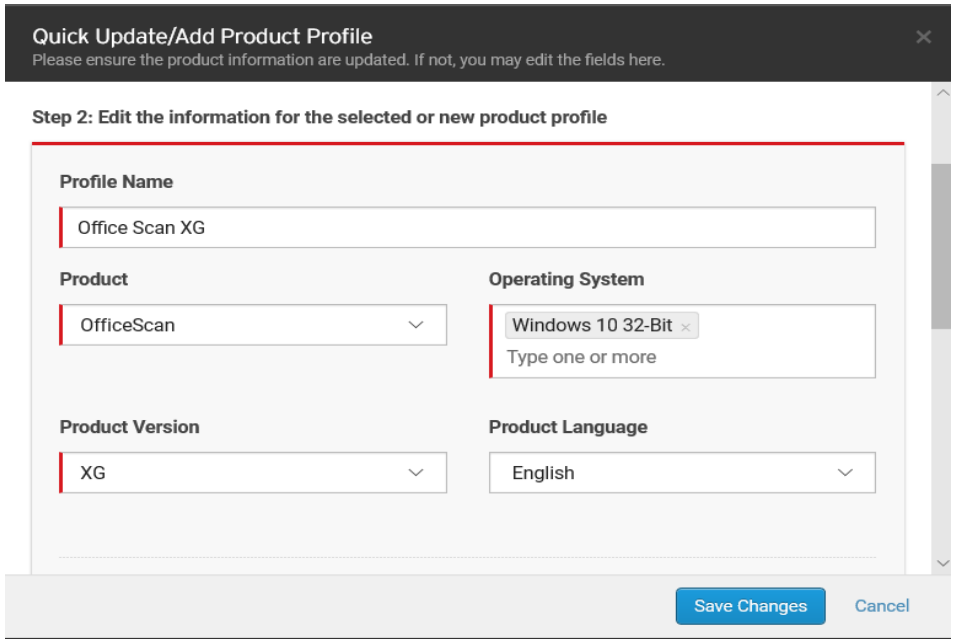
- Utiliser la présentation « Guide des bonnes pratiques - Présentation Client » pour sensibiliser les clients
- Signer un accord avec le client si celui-ci souhaite réaliser une évaluation
- Télécharger l'outil d'extraction.
- Authentification au portail partenaires pour faire une demande de rapport de conformité. Dans la base de connaissance : Comment générer un rapport de bonnes pratiques pour Apex One ou OfficeScan pour connaître comment soumettre une demande, étape par étape.
- Un rapport de conformité est généré par Trend Micro suite à la demande. Le statut de la demande peut être vérifié dans le menu MySupport -> Support Requests. Vous recevrez un email vous indiquant la disponibilité su rapport en téléchargement. Le rapport PDF est disponible dans Support Requests -> File Attachments.
- Pour les clients de Trend Micro Apex One™ SaaS, merci d'ouvrir une demande de support. Un de nos ingénieurs Support générera un rapport de conformité pour l'instance Apex One SaaS de votre client.
- Le rapport permet d'identifier toute opportunité de mise à niveau ou de service. A consulter dans notre base de connaissance : Créer un rapport BPG (Best Practice Guide) et utiliser ma checklist de migration Trend Micro Apex One.
- Partagez les résultats du rapport avec vos clients pour définir un plan d'actions.
- Enregistrez l'offre (Deal Registration) sur le portail partenaire et indiquez le code « BPG Compliance Report » pour obtenir une remise supplémentaire.

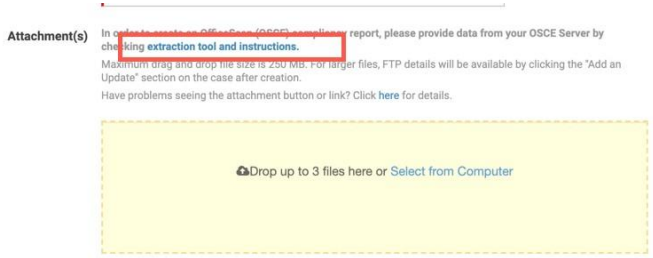
Demande de support BPG via le portail partenaires (1/2)

Base de connaissance : Comment générer un rapport de guide sur les meilleures pratiques (BPC) pour Apex One ou OfficeScan pour connaître les étapes d'une soumission d'une demande.

1. Connectez-vous au portail partenaire pour créer une demande de support.
2. Renseignez vos informations de compte client
3. Sélectionnez « Ajouter un nouveau profil » et indiquez le nom souhaité.
   - Sélectionnez OfficeScan dans la section produit.
4. Téléchargez l'outil d'extraction et exécutez-le sur votre serveur OfficeScan
5. Dézippez et exécutez ExtractionTool_v4.0.exe. Plus d'informations dans le fichier README.txt. Suivez les fenêtres à l'écran pour finaliser.



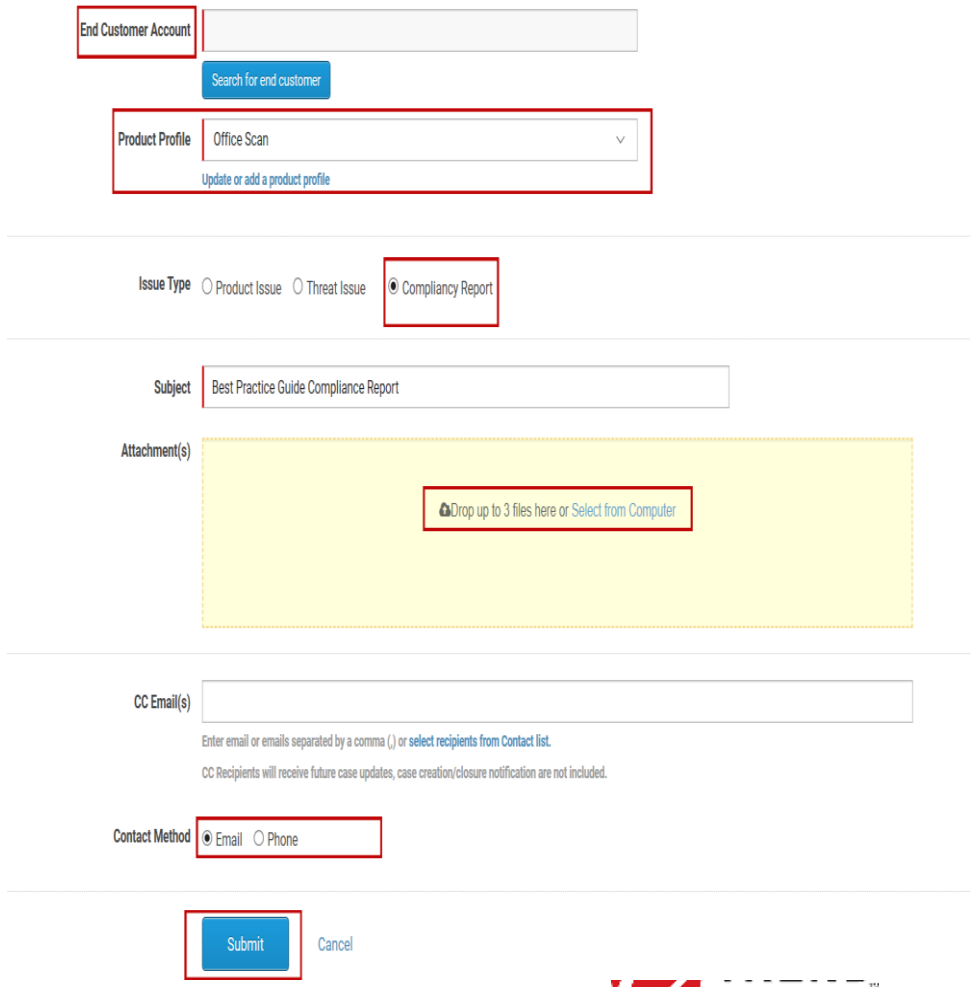




Demande de support BPG via le portail partenaires(2/2)

Base de connaissance : Comment générer un rapport de guide sur les meilleures pratiques (BPC) pour Apex One ou OfficeScan pour connaître les étapes d'une soumission d'une demande.

7. En quelques minutes, l'analyse de conformité du serveur OfficeScan est réalisée. Un répertoire compressé est créé.
8. Téléchargez les fichiers dans la section affichée.
9. Renseignez l'adresse email sur laquelle sera envoyé le rapport.
10. Cliquez sur Submit.
11. Un message attestant de l'envoi de la demande s'affiche, vous indiquant qu'une nouvelle demande de support est créé, ainsi que la référence de la demande.
12. Une fois le rapport généré, vous recevrez un email vous indiquant qu'il est téléchargeable.



Solutions/opportunités recommandées pour les clients

- Mise à niveau vers la version la plus récente
- Migration vers une suite qui dispose de fonctionnalités supplémentaires
- Services Professionnels (support pour la mise à niveau)
- Add-on Trend Micro™ XDR
- Service Trend Micro™ MDR
- Connected Threat Defense - Trend Micro™ Deep Discovery™

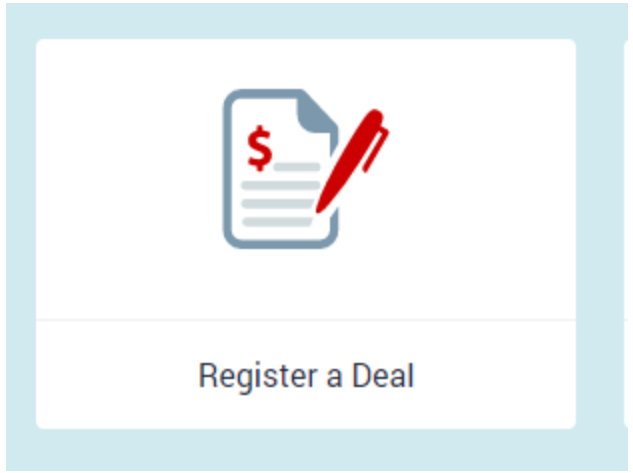
Un rapport pour échanger avec le client sur les opportunités de mise à niveau - Checklist de migration Apex One

Après la création du rapport BPG, cliquez sur la Section 4 pour obtenir directement la checklist de migration Apex One.

Section 4.1	Vérifiez que votre système d'exploitation est compatible avec Apex One et que HTTPS est activé.
Section 4.2	Vérifiez vos agents et assurez-vous que le système d'exploitation de vos Endpoints est compatible avec Apex One. Répertoriez les systèmes d'exploitation qui ne sont pas compatibles, et notez pour chaque OS s'il existe une version ou un patch du système d'exploitation qui est compatible. Cette section indique également si la version de l'agent OfficeScan permet une migration vers Apex One ou pas.
Section 4.3	Vérifie votre serveur SQL. Si vous souhaitez utiliser Apex One avec Endpoint Sensor, vous êtes informé si votre version de SQL Server est compatible et si votre SQL Server Browser et SQL TCP/IP sont activés. Endpoint Sensor nécessite l'activation de SQL Full Text Search

Enregistrement d’offres et Incentives

Enregistrez l’offre (Deal Registration) via le portail partenaire et indiquez « BPG Compliance Report » pour obtenir une remise supplémentaire une fois approuvé.



Ressources de support

- Fiche solution des évaluations et des meilleures pratiques Trend Micro
- Guide des meilleures pratiques - Présentation client
- Accord client pour réaliser un rapport de conformité BPG
- Support par email : partnersupport@trendmicro.com
- Base de connaissances : les étapes pour soumettre une demande de support - rapport de conformité via le portail
  - Générer un rapport de guide sur les meilleures pratiques (BPG) pour Apex One ou OfficeScan.
- Base de connaissances : vous permet de consulter le rapport de conformité BPG et de se migrer vers Apex One.
  - Créer un rapport BPG et utiliser ma checklist de migration Trend Micro Apex One.


TREND MICRO
THE ART OF CYBERSECURITY
La mutation des environnements Trend Micro— des environnements sur site vers le SaaS. **Créé avec des données réelles par l'artiste Stefanie Posavec.**