Guide des Bonnes Pratiques - Rapport de conformité et de sécurité pour Deep Security

Brief partenaires

Sommaire

- Objectifs
- Contenu du rapport de conformité et de sécurité, éléments de scoring et exemple de rapport
- Processus et étapes préconisés
- Comment soumettre une demande de support BPG via le portail partenaires
- Solutions/opportunités recommandées pour échanger avec les clients
- Ressources de support

Objectifs

- L'objectif du rapport de conformité et de sécurité (security compliance report) pour Deep Security est de fournir une synthèse du statut de l’environnement client Deep Security, ainsi que des recommandations en matière de bonnes pratiques. Les instructions détaillées, les impacts métier et les références font l'objet de différentes sections dans le rapport.
- Les partenaires peuvent générer des opportunités de mise à niveau ou de vente de services auprès de leurs clients, en se basant sur les résultats de ce rapport.
- **Produits cibles :** Deep Security 12.0 ou ultérieur, Trend Micro Cloud One™ – Workload Security

Rapport de conformité et de sécurité - Contenu

- Ce rapport indique le statut actuel des dispositifs protégés par Deep Security et livre des recommandations pour renforcer le niveau général de la sécurité des environnements de clients.
- Le rapport de conformité de Deep Security apporte aux clients les données suivantes :
  - Une synthèse technique globale, notamment sur les principaux systèmes d'exploitation utilisés et les versions de l'agent Deep Security.
  - Une synthèse du niveau de conformité de l'environnement Deep Security du client.
  - Un rapport détaillé avec un score d'utilisation et de conformité par module.
- Tous les paramètres sont issus du guide des bonnes pratiques pour Deep Security
- Le guide des bonnes pratiques de Deep Security propose différents paramètres pour différents environnements/scénarios (problématique de performances, de sécurité, etc.)

Contenu du rapport de conformité - Éléments de scoring (1/2)

1. État de l'anti-malware :

Description	Recommandation		
	Temps réel	Manuel	Programmé
État	On		

2. Paramètres de l'anti-malware :

Description	Recommandation		
	Temps réel	Manuel	Programmé
Protection contre les spyware et les grayware	True	True	True
Alerte si un évènement est mis en log lors du scan antimalware	True	True	True
Paramètres de scan : répertoires à analyser	All Directories	All Directories	All Directories
Paramètre de scan : fichiers à analyser	All Files	All Files	All Files
Analyse en temps réel	Read/Write	N/A	N/A
Analyse des fichiers compressés	True	True	True
Analyse des objets Microsoft Office embarqués	True	True	True

Contenu du rapport de conformité - Éléments de scoring (2/2)

2. Réputation web

Description	Recommandation
État	On

3. Contrôle applicatif

Description	Recommandation
État	On

4. Monitoring de l'intégrité

Description	Recommandation
État	ON/Temps-réel

5. Inspection des logs

Description	Recommandation
État	On

6. Pare-feu

Description	Recommandation
État	On

7. Prévention des intrusions

Description	Recommandation
État	Prevent/Detect

Contenu du rapport de conformité à la sécurité

Informations détaillées :

- Conformité des agents
- Détails sur l'agent Deep Security
- Conformité des modules de sécurité
- Version de l'agent Deep Security
- Ratio des ordinateurs managés
- Conformité des paramètres

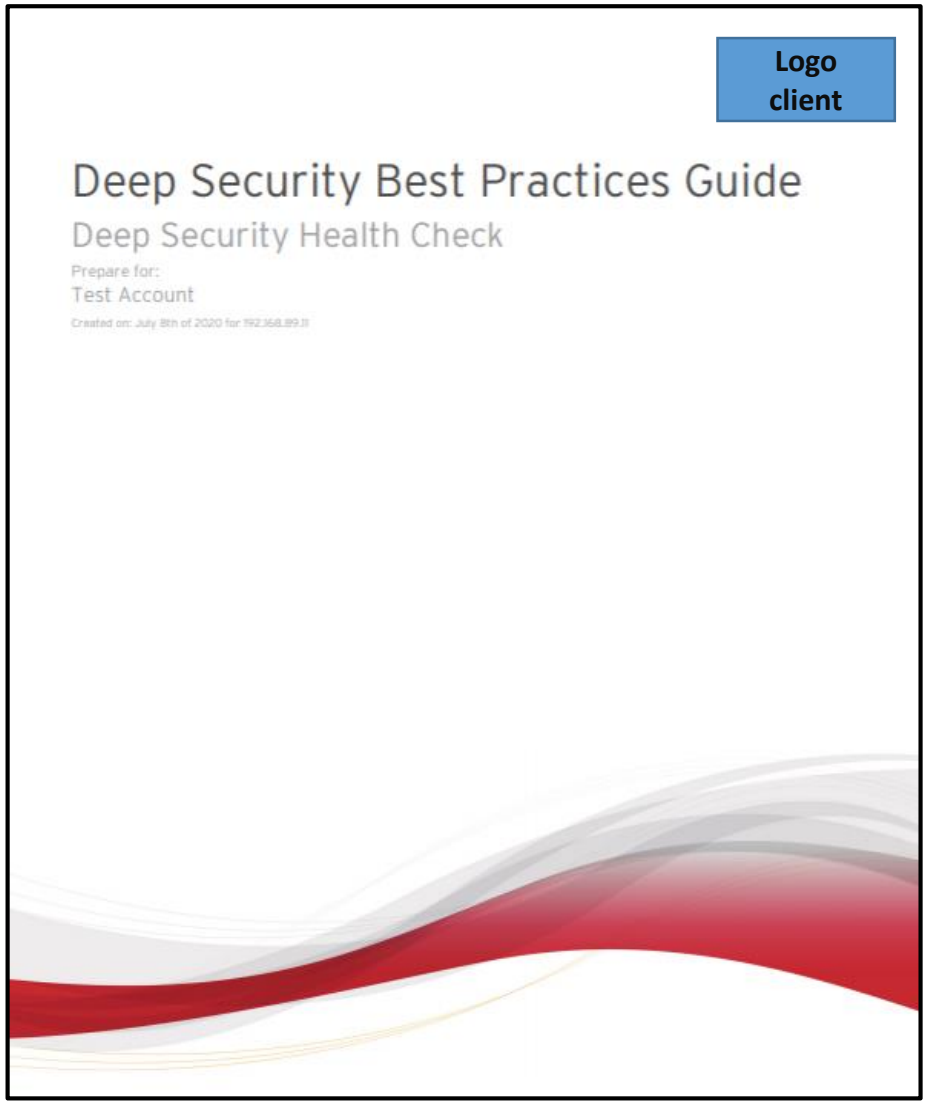
Computer Protected Mode Distribution

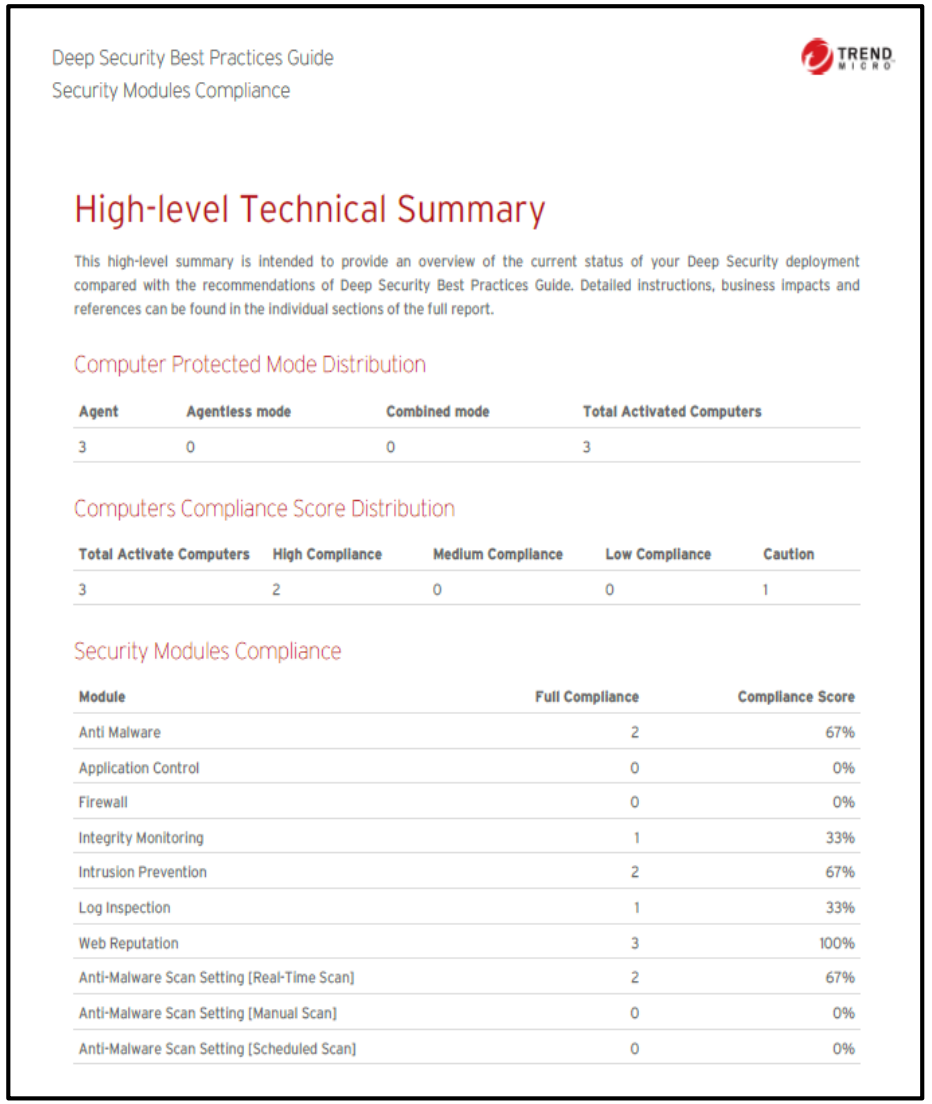
Agent	Agentless mode	Combined mode	Total Activated Computers
3	0	0	3

Computers Compliance Score Distribution

Total Activate Computers	High Compliance	Medium Compliance	Low Compliance	Caution
3	2	0	0	1

Guide des bonnes pratiques - Exemple de rapport (1/3)





Deep Security Best Practices Guide
Security Modules Compliance

TREND MICRO

High-level Technical Summary

This high-level summary is intended to provide an overview of the current status of your Deep Security deployment compared with the recommendations of Deep Security Best Practices Guide. Detailed instructions, business impacts and references can be found in the individual sections of the full report.

Computer Protected Mode Distribution

Agent	Agentless mode	Combined mode	Total Activated Computers
3	0	0	3

Computers Compliance Score Distribution

Total Activate Computers	High Compliance	Medium Compliance	Low Compliance	Caution
3	2	0	0	1

Security Modules Compliance

Module	Full Compliance	Compliance Score
Anti Malware	2	67%
Application Control	0	0%
Firewall	0	0%
Integrity Monitoring	1	33%
Intrusion Prevention	2	67%
Log Inspection	1	33%
Web Reputation	3	100%
Anti-Malware Scan Setting [Real-Time Scan]	2	67%
Anti-Malware Scan Setting [Manual Scan]	0	0%
Anti-Malware Scan Setting [Scheduled Scan]	0	0%

Guide des bonnes pratiques - Exemple de rapport (2/3)

1. Report Overview

The primary objective of this report is to outline the current status of computers protected by Deep Security and suggest recommendations specifically targeted at increasing the overall security posture for your environment. This report provides the following information:

- An overview of the compliance level of Deep Security.
- A per-module breakdown of their use and compliance score
- A high-level technical overview, including the main Operating Systems in use, DS Agent Versions.

All results provided should be analysed in the context of the needs and particularities of the environment in question, as configuration checks may prove to be more or less critical for it's security and operational integrity.

Computer Compliance Distribution

The graph below shows the breakdown of all managed computers by their compliance score. Computers with High compliance have scores between 75-100% and are the expected standard. Medium and Low compliance have scores between 50-74% and 25-49%, respectively. Computers with scores between 0-24% are considered to be in a 'Caution' state. Appropriate measures should be taken to improve their scores.

High Compliance (2 Computers)
Medium Compliance (0 Computers)
Low Compliance (0 Computers)
Caution (1 Computers)

Deep Security Computers Details

Version	Managed ratio	Compliance
12.0.0.1090	100%	77%
12.0.0.1186	100%	4%
20.0.0.877	100%	85%

Deep Security Best Practices Guide
Security Modules Compliance

2. Environment modules overview

This section shows an overall score for each of the used modules, if a module is turned off, the score will be considered as zero.

2.1 Modules overview

Anti Malware (2/3)

Compliance Score

The Deep Security anti-malware module provides agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware. To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code.

Note: Portions of the threat database are hosted on Trend Micro servers or stored locally as patterns. Deep Security Agents periodically download anti-malware patterns and updates to ensure protection against the latest threats.

A newly installed Deep Security Agent cannot provide anti-malware protection until it has contacted an update server to download anti-malware patterns and updates. Ensure that your Deep Security Agents can communicate with a Deep Security Relay or the Trend Micro Update Server after installation.
The anti-malware module eliminates threats while minimizing the impact on system performance. The anti-malware module can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

Application Control (0/3)

Compliance Score

Application control continuously monitors for software changes on your protected servers. Based on your policy configuration, application control either prevents unauthorized software from running until it is explicitly allowed (whitelisted), or allows unauthorized software until it is explicitly blocked (blacklisted). Which option you choose depends on the level of control you want over your environment.

Warning: Application control continuously monitors your server and logs an event whenever a software change occurs. It is not intended for environments with self-changing software or that normally creates executables, such as some web or mail servers.unauthorized applications.

Firewall (0/3)

The firewall module provides bidirectional stateful inspection of incoming and outgoing traffic. Firewall rules define what actions to take on individual packets in that traffic. Packets can be filtered by IP and MAC address, port and packet flag across all IP-based protocols and

Guide des bonnes pratiques - Exemple de rapport (3/3)

frame types. The firewall module can also help prevent denial of service attacks and detect and prevent reconnaissance scans.

0%
Compliance Score

Integrity Monitoring (1/3)

The integrity monitoring module scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files on Deep Security Agents. Using a baseline secure state as a reference, the integrity monitoring module performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes.

33%
Compliance Score

Intrusion Prevention (2/3)

The Intrusion Prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

67%
Compliance Score

When patches are not available for known vulnerabilities in applications or operating systems, Intrusion Prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed.

Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, Intrusion Prevention can also be used as a lightweight web application firewall (WAF).

Log Inspection (1/3)

The log inspection protection module helps you identify important events that might be buried in your operating system and application logs. These events can be sent to a security information and event management (SIEM) system or centralized logging server for correlation, reporting, and archiving. All events are also securely collected in the Deep Security Manager.

The log inspection module lets you:

* Meet PCI DSS log monitoring requirements.
* Detect suspicious behavior.
* Collect events across heterogeneous environments containing different operating systems and diverse applications.
* View events such as error and informational events (disk full, service start, service shutdown, etc.).
* Create and maintain audit trails of administrator activity (administrator login or logout, account lockout, policy change, etc.).

Deep Security Best Practices Guide
Security Modules Compliance

The log inspection feature in Deep Security enables real-time analysis of third party log files. The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with intrusion prevention and integrity monitoring, log inspection content is delivered in the form of rules included in a security update. These rules provide a high level means of selecting the applications and logs to be analyzed.

33%
Compliance Score

Web Reputation (3/3)

The web reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the security level being enforced, Deep Security will either block or allow access to the URL.

100%
Compliance Score

Note: The web reputation module does not block HTTPS traffic.

Anti-Malware Scan Setting [Real-Time Scan] (2/3)

Real-time scans continuously monitor for malware. Every time a file is received, opened, downloaded, copied, or modified, a real-time scan occurs. (In comparison, manual and scheduled scans only detect malware at specific times, when you run them.) If Deep Security detects no security risk, the file remains in its location and users can proceed to access the file. If Deep Security detects a security risk, it displays a notification message, showing the name of the infected file and the specific security risk.

67%
Compliance Score

Anti-Malware Scan Setting [Manual Scan] (0/3)

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the computer. The time it takes to complete scanning depends on the number of files to scan and the computer's hardware resources.

0%
Compliance Score

Anti-Malware Scan Setting [Scheduled Scan] (0/3)

Scheduled scans run automatically on the configured date and time. Use scheduled scan to automate routine scans and improve scan management efficiency.

0%
Compliance Score

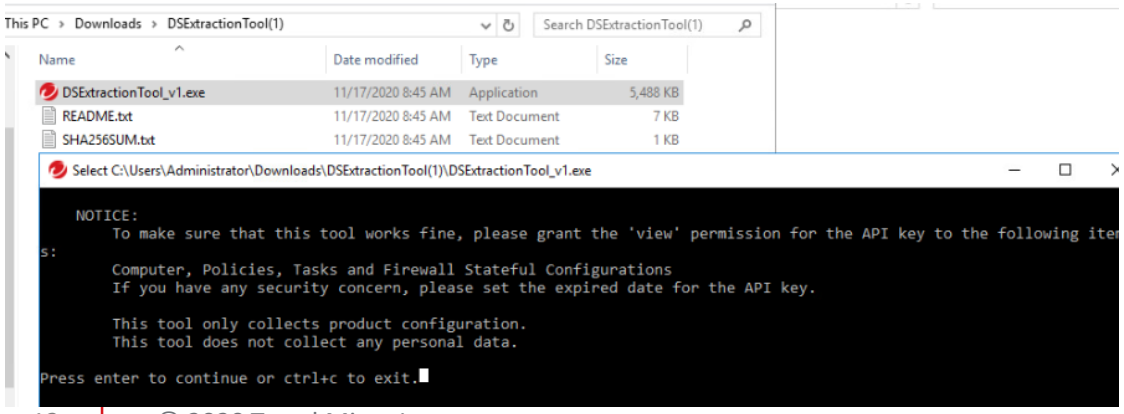
Étapes recommandées (utilisation en interne)

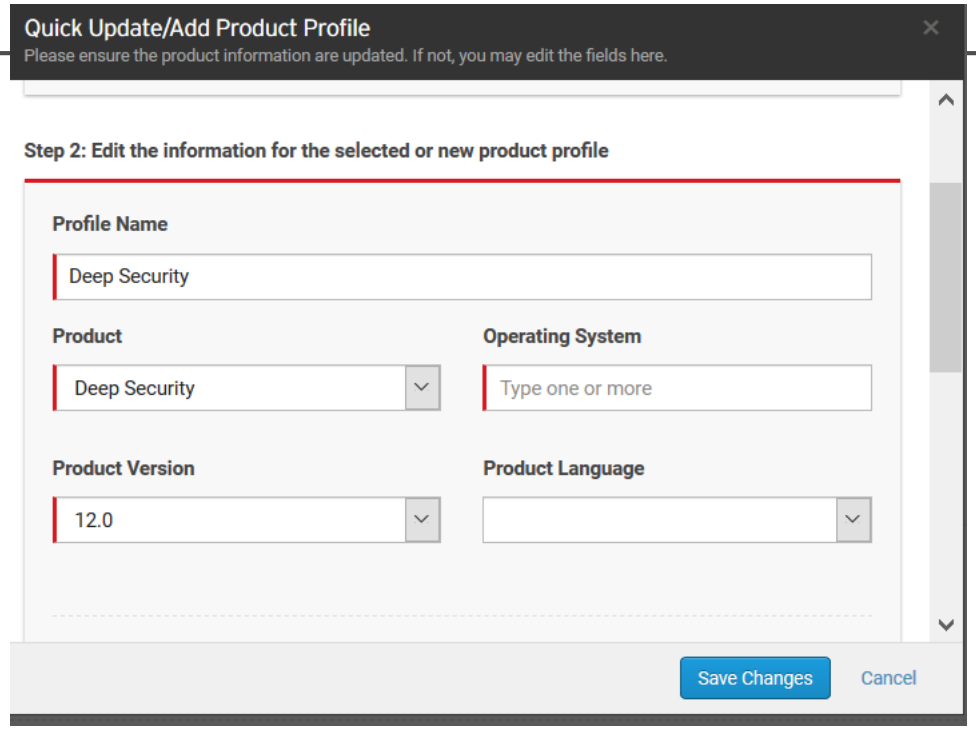
- Utilisez la présentation « Guide des bonnes pratiques - Présentation Client » pour informer vos clients
- Concluez un accord avec le client si celui-ci souhaite réaliser une évaluation.
- Téléchargez l'outil d'extraction.
- Connectez-vous au portail partenaire et soumettez une demande pour un rapport de conformité. Consultez la base de connaissances How to Generate a Deep Security Best Practice Guide Report pour comprendre la démarche, étape par étape, pour soumettre une demande.
- Le rapport de conformité sera généré par Trend Micro suite à la demande. Le statut de la demande est accessible via MySupport -> Support Requests. Une fois le rapport généré, vous recevez un email vous indiquant qu'il est disponible en téléchargement. Le rapport PDF est disponible à partir de Support Requests -> File Attachments.
- Présentez les résultats du rapport à vos clients pour définir un plan d'actions.

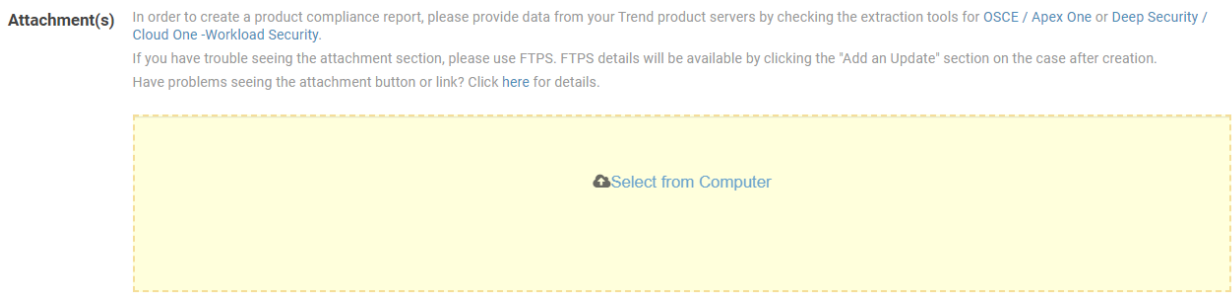
Soumettre une demande de rapport BPG via le portail partenaires (1/2)

Base de connaissances : How to Generate a Deep Security Best Practice Guide Report pour comprendre la démarche, étape par étape, pour soumettre une demande.

1. Connectez-vous au portail partenaires et créez votre demande de support.
2. Renseignez les informations du client.
3. Choisissez “Add a new profile” et inscrivez le nom.
   - Sélectionnez Deep Security en tant que Produit.
4. Téléchargez l’outil d’extraction et exécutez-le sur votre serveur.
5. Exécutez DSExtractionTool_v1.exe et lisez le fichier README.txt. Suivez les instructions à l’écran.



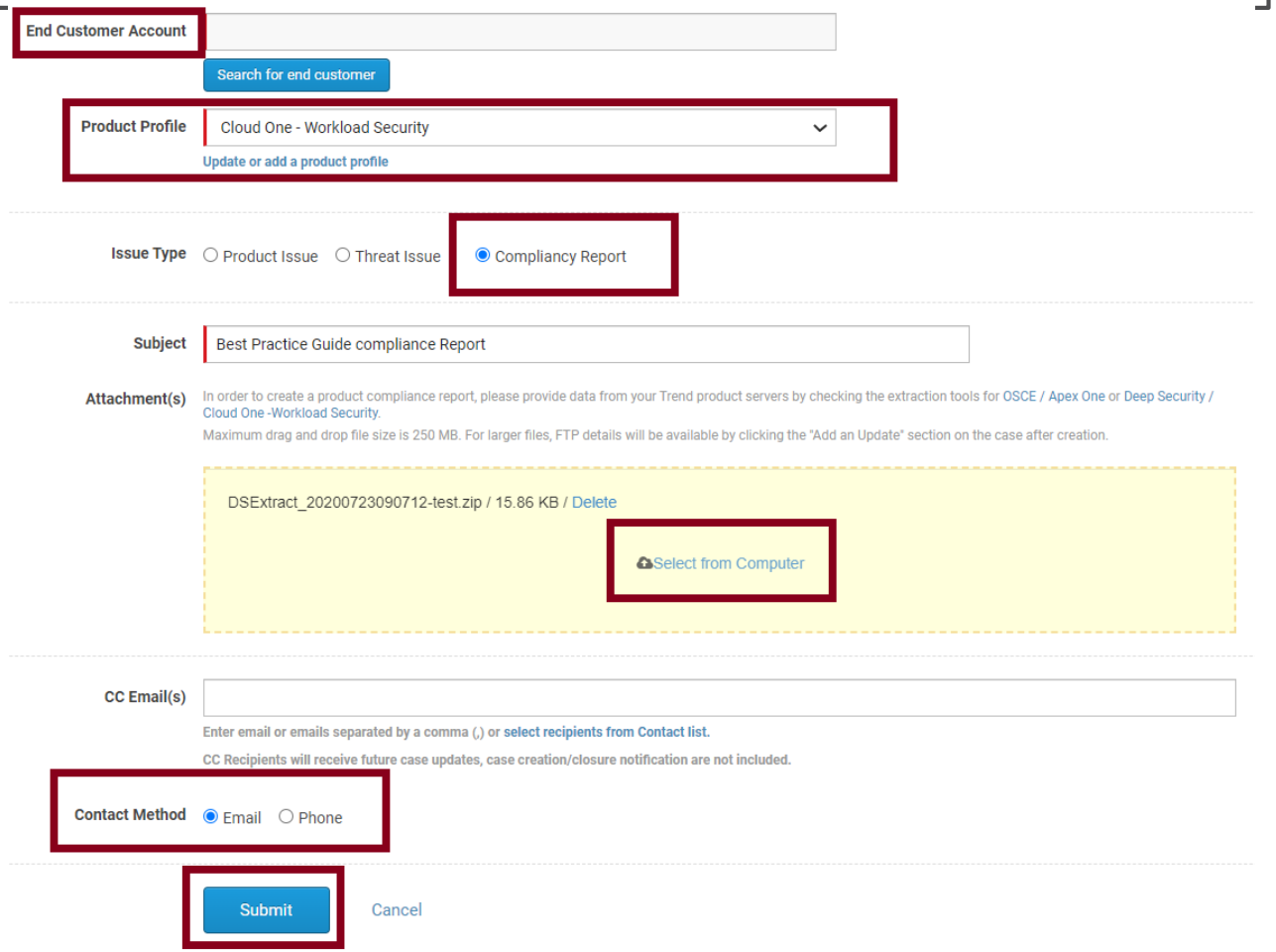




Soumettre une demande de rapport BPG via le portail partenaires (2/2)

Base de connaissances : How to Generate a Deep Security Best Practice Guide Report pour comprendre la démarche, étape par étape, pour soumettre une demande. .

7. L'analyse de conformité du serveur Deep Security est réalisés en quelques minutes et donne lieu à un répertoire compressé.
8. Téléchargez ce fichier de résultat dans la zone indiquée.
9. Indiquez l'email sur lequel vous souhaitez recevoir le rapport.
10. Cliquez sur soumettre.
11. Le message de confirmation d'envoi apparaît et vous informe de la création de la demande, ainsi que l'identifiant de la demande.
12. Une fois le rapport généré, vous recevez un email vous indiquant sa disponibilité en téléchargement.



Solutions/opportunités recommandées pour échanger avec les clients

- Mise à niveau vers la version la plus récente
- Mise à niveau vers Trend Micro Cloud One™ – Workload Security
- Migration vers une suite qui dispose de fonctionnalités supplémentaires
- Services Professionnels (support lors de la mise à niveau)
- Add-on Trend Micro™ XDR
- Service Trend Micro™ Managed XDR

Ressources de support

- Support par email : partnersupport@trendmicro.com
- Fiche solution Customer Success Service
- Base de connaissances : les étapes pour soumettre une demande de rapport de conformité et de sécurité via le portail partenaires
  - Generate a Best Practice Guide Report for Deep Security


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