Tripwire Enterprise 8.7

Détecter. Réagir. Prévenir.

Tripwire® Enterprise est une suite de gestion de la configuration de sécurité offrant des solutions totalement intégrées pour la gestion des politiques, de l'intégrité des fichiers et de leur restauration. Les entreprises peuvent utiliser ces solutions ensemble pour bénéficier d'une solution exhaustive de gestion de la configuration de bout en bout, ou utiliser les solutions de contrôle de l'intégrité des fichiers ou de gestion des politiques indépendamment pour aborder les défis urgents actuels en matière de sécurité et de conformité, tout en établissant une base solide qui les positionne pour être prêtes pour l'avenir.

La gamme permet aux équipes de sécurité, de conformité et opérationnelles d'atteindre rapidement un niveau de sécurité de base à l'échelle de leur infrastructure en réduisant le champ d'attaque, en augmentant l'intégrité du système et en assurant une conformité continue. De plus, étant donné que Tripwire Enterprise s'intègre aux applications en vue d'automatiser le flux de travail à l'aide de solutions supplémentaires de sécurité des terminaux comme les solutions de SIEM (gestion des informations et des événements de sécurité) et les outils de gestion du changement, les entreprises peuvent élargir leur vision en matière de sécurité et gagner en efficacité.

Tripwire possède plus de 20 ans de métier dans le domaine de la sécurité et conformité industrielle, grâce à une technologie spécifique de détection rapide et en temps réel des cybermenaces et de protection contre les attaques futures.

Tripwire a protégé et mis en conformité plus de la moitié des entreprises du Fortune 500 et la plupart des réseaux les plus sensibles dans le monde, grâce à ses fonctionnalités répondant aux nombreuses exigences de conformité et de politique de sécurité.

En tant que solution clé de sécurité et de conformité, Tripwire Enterprise applique une stratégie de détection, de réaction et de prévention grâce à sa capacité à:

- **Détecter** les cybermenaces et les possibles violations en mettant en évidence les indicateurs potentiels de risques.
- **Réagir** aux déviations à l'aide d'alertes en faible ou grand volume et donner des directives sur les mesures à prendre pour revenir à un état stable de sécurité.
- **Prévenir en s'adaptant et priorisant les menaces et changements déviants** pour maintenir une vision renforcée, objective, globale de son positionnement en matière de sécurité à travers les périphériques et systèmes.

Comment ca marche : Contrôles intégrés

Tripwire Enterprise fournit cinq fonctionnalités et capacités intégrées qui fonctionnent ensemble pour créer une solution de gestion de la chaîne logistique (SCM):

- **Tripwire File Integrity Manager** est la première et la meilleure solution de contrôle de l'intégrité des fichiers. Elle parcourt des environnements hétérogènes pour détecter les menaces et fournir un aperçu instantané des vulnérabilités de la configuration, tout en améliorant l'efficience opérationnelle en évitant les dérives en matière de configuration et les changements non autorisés. Le contrôle de l'intégrité des fichiers de Tripwire peut être utilisé de façon autonome pour fournir des renseignements granulaires sur les

terminaux offrant un aperçu rapide de son positionnement en matière de sécurité et de conformité. Lorsqu'elle est utilisée en combinaison avec Tripwire Policy Manager, elle fournit une évaluation de la configuration déclenchée par le changement et d'autres systèmes de réponse configurables. Cela transforme une évaluation « passive » de la configuration en une solution défensive dynamique, continue et en temps réel qui détecte immédiatement les écarts par rapport aux standards de sécurité attendus en matière de configuration sécurisée et aux directives de protection renforcée.

» **Tripwire Policy Manager** établit et assure une évaluation continue de la configuration avec agent ou sans agent de conformité pour plus de 1 000 combinaisons de plateformes et de politiques, de normes, de règlements et de directives de fournisseurs concernant la sécurité et la conformité. Le Policy Manager permet aussi une gestion personnalisée et complète des politiques de sécurité, des dérogations et des exceptions, des options de correction automatisées, et la notation des politiques en ordre de priorité en fonction de seuils, de pondérations et de niveaux de gravité. Il fait tout cela tout en fournissant aux auditeurs des preuves de conformité et en rendant l'état des politiques hautement visible et applicable pour les équipes de conformité.

» **Remediation Manager** fonctionne avec Tripwire Policy Manager pour fournir des directives intégrées aux équipes de sécurité et de conformité dans le but de corriger les configurations de sécurité mal alignées ou à la dérive, tout en conservant la gestion, les approbations et les autorisations en fonction des rôles. Cela aide les équipes opérationnelles à connaître plus facilement et efficacement ce qui a échoué et configurer les systèmes à un état prêt pour la production - et une fois qu'ils sont en production, à les conserver dans cet état.

» **Les fonctionnalités d'enquête et d'approfondissement des causes profondes** donnent aux équipes de sécurité et opérationnelles la capacité d'enquêter rapidement et efficacement pour déterminer les causes profondes. Les systèmes changent inévitablement à mesure que les entreprises révisent et changent leur personnel, leurs processus et leurs technologies. Tripwire Enterprise peut fournir des comparaisons côte à côte approfondies, granulaires, des bases de référence et des comparaisons historiques pour informer rapidement les équipes d'investigation de ce qui a changé, quand, qui en est la cause et à quelle fréquence, avec de l'information sur le « comment ».

» **La plateforme Tripwire Axon®** permet une collecte de données flexible et une communication résiliente à l'échelle d'une vaste gamme d'appareils, d'espace cloud et de biens virtualisés. La plateforme Tripwire Axon aborde les défis liés à la collecte en utilisant un agent extensible et économique en ressources, des techniques de messagerie désynchronisées et des définitions de messages neutres en ce qui concerne le produit et la plateforme. L'agent de Tripwire Axon est optimisé pour une utilisation minimale des ressources globales du système et de la bande passante du réseau. Les codes binaires d'Agent sont mis en place dans C++ pour minimiser l'empreinte et maximiser le rendement.

Fonctionnalités de pointe en matière de sécurité et conformité industrielle.

Tripwire ajoute continuellement de nouvelles capacités à Tripwire Enterprise pour répondre aux défis changeants en matière de sécurité et de conformité. Tripwire Enterprise possède maintenant de nouvelles fonctionnalités pour contrôler les actifs dans le cloud, protéger les engins industriels et détecter des preuves de comportement nuisibles dans votre environnement à l'aide du protocole MITRE ATT&CK.

» **Cloud Management Assessor** Cloud Management Assessor de Tripwire aide les utilisateurs de Tripwire Enterprise à déterminer le niveau de sécurité du déploiement de leurs Amazon Web Services (AWS), de Microsoft Azure et Google Cloud Platform en recueillant, en analysant et en cotant les données de configuration des comptes en fonction des meilleures pratiques (comme la version 1.1.0 de la Center for Internet Security AWS Foundations Benchmark, ou base de référence des fondements des services AWS du centre pour la sécurité sur Internet).

De plus, Cloud Management Assessor peut évaluer automatiquement vos cases S3 des services AWS et votre stockage sur Azure pour déterminer s'ils sont exposés à un accès anonyme, et signaler les objets qui ont été récemment exposés.

» **Tripwire Data Collector** Tripwire Data Collector élargit les capacités de base de Tripwire Enterprise pour la détection du changement et la conformité de base dans l'environnement industriel. Les environnements de technologie opérationnelle de surveillance comportent leur ensemble unique de défis. L'architecture sans agent du Tripwire Data Collector a été conçue au complet pour évaluer les configurations, la sécurité et l'état, y compris les micrologiciels, la révision du matériel, les versions de logiciels, les niveaux de retouche et bien plus.

Le Tripwire Data Collector est en mesure de communiquer avec les appareils à l'aide de différents protocoles industriels, comme Modbus TCP, Ethernet/IP CIP et SNMP. Pour les appareils qui ne peuvent pas être

Tripwire s'est appuyé sur son outil original de détection des intrusions basé sur l'hôte, qui pouvait simplement détecter les changements apportés aux fichiers et aux dossiers, et l'a amélioré pour en faire une solution solide de contrôle de l'intégrité des fichiers, en mesure de surveiller en détail l'intégrité du système : fichiers, répertoires, registres, paramètres de configuration, DLL, ports, services, protocoles, etc. De plus, les intégrations additionnelles offrent des renseignements granulaires sur les terminaux permettant la détection des menaces et la conformité aux politiques et audits. Il a fallu des années pour améliorer la capacité de Tripwire à détecter et juger les changements avec priorisation et intégration des risques en matière de politiques et sécurité, pour permettre des alertes à valeur élevée et à faible volume - aidant les plus grandes entreprises à gérer l'intégrité, la sécurité et la conformité de la configuration de leurs systèmes.

liés, les informations de configuration peuvent être recueillies à l'aide d'intégrations avec le FactoryTalk AssetCentre de Rockwell Automation, MDT AutoSave et KEPServerEX de Kepware. Les données de configuration peuvent aussi être recueillies à l'aide de l'extracteur Web, qui peut aller chercher des données de configuration à partir de pages Web.

» **Protocole MITRE ATT&CK**
Élaboré par la société MITRE, le protocole ATT&CK est un modèle de cybersécurité utile illustrant comment les adversaires se comportent et expliquant les tactiques que vous devriez utiliser pour atténuer le risque et améliorer la sécurité. À l'aide du contenu des politiques du protocole ATT&CK, vous pouvez détecter et signaler les comportements nuisibles dans votre environnement - en ajoutant un niveau supplémentaire de protection à votre stratégie de sécurité.

Prêt à aller plus loin?

Pour en savoir davantage sur les fonctionnalités, les rapports, les politiques disponibles, l'assistance et bien plus, visitez tripwire.com pour consulter les fiches produits suivantes :

- » Tripwire Enterprise Report Catalog
- » Tripwire Enterprise Policy Manager
- » Tripwire Connect
- » Tripwire Enterprise Remediation Manager
- » Tripwire Enterprise Agent Platform Support
- » Tripwire Axon
- » Tripwire Axon Agent Platform Support

Fonctionnalités et avantages

Plateforme mise à jour de collecte et de transmission de données	Tripwire Enterprise offre des services pointe en matière de gestion de la sécurité, du contrôle de l'intégrité, de la configuration et de la conformité grâce à sa solution Tripwire Axon, une plateforme de collecte et de transmission de données aux terminaux, enfichable, extensible et à rendement élevé. Les utilisateurs bénéficient d'une visibilité et d'une cyber-résilience sans précédent tout en réduisant les fardeaux opérationnels et en améliorant la réactivité.
Soutien pour les environnements hybrides	Tripwire Enterprise peut surveiller la sécurité et la conformité des environnements en local et dans le cloud. Les clients peuvent réduire leurs coûts et obtenir une meilleure visibilité en utilisant une seule solution pour les deux environnements.
Point de contrôle unique pour toutes les configurations	Tripwire Enterprise offre un contrôle centralisé des configurations à l'échelle de toute l'infrastructure physique et virtuelle, y compris les serveurs et les appareils, les applications et de nombreuses plateformes et systèmes d'exploitation.
Intégration avancée à l'aide d'API REST	Les API REST mises à jour permettent à la valeur de Tripwire Enterprise d'être intégrée à d'autres applications. Les API REST permettent la commande et le contrôle programmable d'applications comme Tripwire Enterprise et l'extraction des renseignements recueillis. Les API d'administration permettent l'automatisation de tâches comme l'activation de la surveillance en temps réel ou les politiques d'exécution.
Surveillance du réseau de TO	À l'aide du Tripwire Data Collector avec Tripwire Enterprise, les utilisateurs peuvent surveiller les changements et la conformité de leur réseau industriel, ce qui permet un environnement plus sécurisé sans compromettre la disponibilité.
Fonctionnalité "vision des ressources"	La visualisation des ressources vous permet de classifier les biens à l'aide d'étiquettes pertinentes pour votre entreprise, comme le risque, la priorité, l'emplacement géographique, les politiques réglementaires et d'autres. Les fonctionnalités de visualisation des actifs de Tripwire Enterprise permettent désormais le provisionnement des ressources à l'aide d'un fichier d'étiquetage des ressources, une portée plus grande pour un grand nombre de ressources et un étiquetage de ressources importées Tripwire IP360, ce qui fournit une vue plus exacte du risque à l'échelle de toute l'entreprise.
Outils du flux de travail pour la gestion des configurations défaillantes	Le Remediation Manager fournit des outils de flux de travail basés sur le rôle qui permettent aux utilisateurs d'approuver, de refuser, de reporter ou d'exécuter la correction des configurations défaillantes.
Intégration aux systèmes de gestion du changement	Étant donné que Tripwire Enterprise s'intègre aux solutions de pointe de gestion du changement (CMS), à mesure que des changements ont lieu, Tripwire Enterprise rapproche automatiquement les changements détectés des billets de changement et des demandes de changement.
Préparation plus rapide et plus facile aux audits	Tripwire Enterprise réduit grandement le temps et l'effort requis pour la préparation aux audits en fournissant des bases de référence continues et exhaustives pour l'infrastructure informatique ainsi que la détection du changement en temps réel et des renseignements intégrés pour déterminer l'incidence des changements.
Soutien pour le maintien d'un état sécurisé et conforme	Tripwire Enterprise combine l'évaluation de la configuration et la surveillance de l'intégrité des fichiers pour détecter, analyser et signaler les changements à mesure qu'ils ont lieu et pour maintenir la conformité continue des configurations. Cet accès immédiat à l'information sur le changement permet à l'équipe informatique de régler les problèmes avant qu'ils n'entraînent des violations importantes des données, des problèmes lors des audits ou des pannes à long terme.
Processus automatisés de conformité de la TI	Tripwire Enterprise automatise la conformité avec les organismes régissant les règlements et les normes de l'industrie, comme PCI, NERC, SOX, FISMA, DISA et bien d'autres.

Soutien aux entreprises

Tripwire Enterprise peut fonctionner avec ou sans agent, et fonctionne avec :

- **Tous les systèmes d'exploitation majeurs :** Windows, Red Hat, CentOS, Ubuntu, SUSE et Debian
- **Beaucoup de systèmes d'exploitation propres aux fournisseurs :** AIX, Solaris, HP-UX, etc.
- **Services de répertoires :** Active Directory, LDAP, etc.
- **Appareils connectés au réseau :** Pare-feu, configuration IPS et IDS, routeurs, etc.
- **Bases de données :** Oracle, MS SQL, DB2 et PostgreSQL

Soutien large et approfondi du département informatique

Bien que le département informatique doivent surveiller des serveurs essentiels ou la totalité de l'infrastructure - y compris les environnements clouds et virtualisés, les applications et engins industriels - Tripwire Enterprise permet d'évaluer, de valider et d'appliquer les politiques et de détecter tous les changements, peu importe leur source.

Tripwire Enterprise assure l'ensemble des services suivants

Applications	Tripwire Enterprise offre des fonctionnalités de gestion des politiques de conformité et de contrôle de l'intégrité des fichiers pour faire en sorte que les applications supportées soient configurées correctement pour assurer la sécurité, la conformité, ainsi qu'une performance et disponibilité optimale.
Services de répertoire	Tripwire Enterprise fournit un service indépendant de gestion des politiques de conformité pour les objets et les attributs du répertoire du serveur conformes au protocole LDAP, comme le schéma du protocole LDAP, les paramètres de mots de passe, les autorisations aux utilisateurs, les ressources du réseau, les mises à jour de groupe et les politiques de sécurité.
Bases de données	Tripwire Enterprise travaille en collaboration avecles éléments des systèmes de fichiers de Tripwire pour aider les entreprises à maintenir leurs serveurs de bases de données Oracle, Microsoft et IBM dans un état constant de sécurité et de haute performance.
Systèmes de fichiers et ordinateurs de bureau	Tripwire Enterprise évalue la configuration des serveurs physiques et virtuels et des systèmes de fichiers des ordinateurs de bureau, y compris les paramètres de sécurité, les paramètres de configuration et les autorisations.
Appareils en point de vente	Tripwire Enterprise sécurise les appareils en point de vente contre les cybermenaces, gère les politiques de sécurité et de conformité pour ces appareils, et fournit des opérations informatiques, tels que des alertes, des notifications et des directives de réponse lorsque l'on soupçonne que des indicateurs de potentielles violations ou d'anomalies existent sur ces appareils.
Environnements virtualisés	Tripwire Enterprise travaille dans des environnements virtualisés, c.-à-d. des clouds privés, publics et hybrides. La console de Tripwire Enterprise peut fonctionner à titre de machine virtuelle, et ses agents peuvent surveiller tout type de terminal virtualisé supporté. Cela comprend la protection contre les cybermenaces dans des environnements virtualisés/cloud, le contrôle de l'intégrité des systèmes, l'application de politiques de sécurité et de conformité, les tableaux de bord, la production de rapports et les alertes et notifications en temps réel.
VMware	Tripwire Enterprise offre une vue globale de l'infrastructure virtuelle de VMware, permettant le contrôle continu de la configuration des environnements virtuels.
Appareils sur le réseau	Tripwire Enterprise évalue les paramètres de configuration de la gamme la plus vaste d'appareils connectés au réseau industriel, y compris tout appareil fonctionnant avec un système d'exploitation conforme à POSIX.

Tripwire est le leader la mise en place d'une base de protection solide en matière de cybersécurité. En partenariat avec des sociétés du Fortune 500, des entreprises industrielles et des agences gouvernementales, Tripwire protège l'intégrité des systèmes essentiels, incluant les environnements physiques, virtuels, clouds et DevOps.Notre gamme primée de produits offre des contrôles fondamentaux de sécurité de qualité supérieure tels que la détection et l'analyse des ressources, la gestion de la configuration sécurisée, la gestion de la vulnérabilité et la gestion des journaux. En tant que précurseur du contrôle de l'intégrité des fichiers (FIM), l'expertise de Tripwire repose sur plus de 20 années d'innovation aidant les entreprises à découvrir, minimiser et surveiller leur champ d'attaque.

Apprenez-en plus sur le site tripwire.com, obtenez des informations concernant la sécurité, découvrez les tendances et des idées sur tripwire.com/blog, ou connectez avec nous sur LinkedIn, Twitter et Facebook.

TEDS870aFR 1806