Présentation de solution

CyberSense® pour PowerProtect Cyber Recovery

Outils d'apprentissage automatique, d'analytique et d'investigation basés sur l'IA pour détecter et diagnostiquer les menaces, puis effectuer une restauration après une cyberattaque

L'AVANTAGE CYBERSENSE

CyberSense® est entièrement intégré à la solution de coffre-fort PowerProtect Cyber Recovery de Dell.

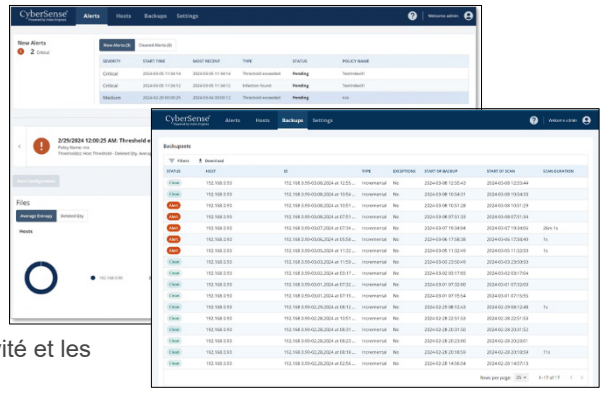
- Cette intégration permet une approche automatisée, avec une analyse régulière des données de sauvegarde afin de valider leur intégrité et de signaler toute détection d'un comportement suspect.
- La capacité de CyberSense à analyser directement le contenu des images de sauvegarde, dont celles de Dell NetWorker, Avamar, PowerProtect Data Manager et bien d'autres, permet l'analyse de contenus sans avoir à réhydrater les données.
- CyberSense est la seule solution à fournir une analytique basée sur le contenu complète à chaque analyse des données afin de détecter les attaques par rançongiciel les plus sophistiquées, qui échappent facilement à la vigilance des outils d'analyse moins optimisés, car ceux-ci n'inspectent que les métadonnées.
- Lors d'une attaque, CyberSense fournit des rapports d'analyse postérieure approfondie permettant de déterminer l'ampleur de l'attaque, puis il fournit une liste des derniers jeux de sauvegardes fiables antérieurs à la corruption afin de faciliter le processus de récupération.

CyberSense se distingue des autres approches d'analytique des données et offre un plus haut niveau de confiance quant à l'intégrité des données de sauvegarde et à la possibilité de les récupérer rapidement après une attaque.

Lorsque les outils de sécurité conventionnels échouent à protéger les données contre les cyberattaques, **CyberSense®** intervient après l'attaque pour détecter les données corrompues avec une précision de 99,5 % et faciliter une restauration intelligente et rapide. À la fois dernière ligne de défense et première ligne de récupération pour des milliers d'organisations dans le monde entier, CyberSense garantit l'intégrité des ressources de données, couvrant l'infrastructure principale, les bases de données de production et les documents stratégiques pour garantir que les données sont exemptes de toute corruption malveillante.

CyberSense examine les sauvegardes de données pour en observer l'évolution au fil du temps, puis utilise l'apprentissage automatique basé sur l'IA pour détecter les signes de corruption indiquant une attaque par rançongiciel. L'apprentissage automatique évalue ensuite plus de 200 analyses basées sur le contenu pour détecter la corruption avec une confiance de 99,5 % afin de vous aider à protéger votre infrastructure et votre contenu stratégiques. CyberSense détecte les suppressions massives, le chiffrement et d'autres modifications suspectes résultant d'attaques sophistiquées dans l'infrastructure principale (y compris Active Directory, DNS, etc.), les fichiers utilisateur et les bases de données de production stratégiques. En cas de détection d'un signe de corruption, une alerte est générée dans le tableau de bord avec des informations supplémentaires qui détaillent l'ampleur et l'impact de l'attaque.

En cas de comportement suspect, CyberSense fournit des rapports d'investigation post-cyberattaque afin de diagnostiquer le degré d'impact. Si une corruption de données est détectée, l'outil compile une liste des derniers jeux de données de sauvegarde certifiés fiables afin de permettre une restauration rapide et organisée, contribuant à minimiser les interruptions d'activité et les pertes de données.



Le workflow Cyber Recovery

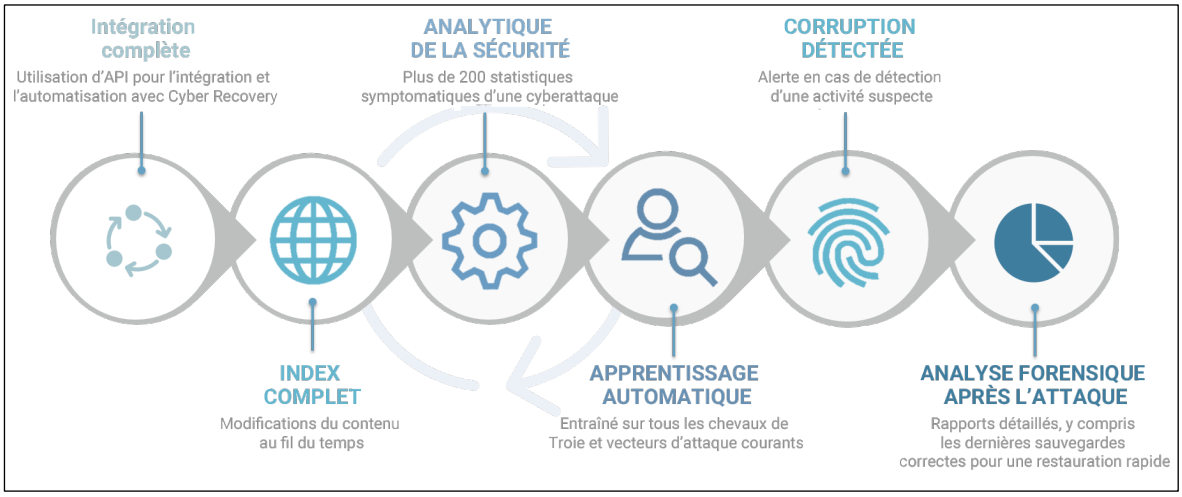
CyberSense s'intègre de manière transparente à Dell PowerProtect Cyber Recovery, et surveille activement les fichiers et les bases de données dont il analyse l'intégrité pour détecter toute corruption due aux rançongiciels. Une fois les données répliquées dans le coffre-fort Cyber Recovery et soumises au verrouillage de rétention, CyberSense lance automatiquement une analyse complète des données de sauvegarde et enregistre des captures instantanées des fichiers, des bases de données et de l'infrastructure principale. Ces observations permettent à CyberSense de suivre méticuleusement les modifications apportées aux fichiers au fil du temps et d'identifier efficacement les données corrompues, même par les cybermenaces les plus sophistiquées.

L'analyse CyberSense fonctionne directement sur les données de l'image de sauvegarde, ce qui permet de contourner le logiciel de sauvegarde d'origine et l'étape de réhydratation des données. Grâce à l'analytique avancée, CyberSense identifie le chiffrement et la corruption de fichiers ou de pages de base de données, identifie les extensions de logiciels malveillants connues, détecte les créations ou suppressions massives de fichiers, et bien plus encore.

CyberSense s'appuie sur des algorithmes d'apprentissage automatique basés sur l'IA, entraînés à faire face aux derniers chevaux de Troie et rançongiciels, pour prendre des décisions déterministes concernant les corruptions de données indicatrices d'une cyberattaque. En cas d'attaque, une alerte critique s'affiche rapidement dans le tableau de bord Cyber Recovery. De plus, CyberSense propose des rapports d'investigation post-attaque, pour faciliter le diagnostic et la récupération rapides après une attaque par rançongiciel, afin de minimiser la perte de données.

Analyse complète du contenu

CyberSense est la seule offre sur le marché qui fournit une analytique basée sur le contenu complète pour l'ensemble des données protégées. Cette fonctionnalité distingue CyberSense des autres solutions qui adoptent une vue moins granulaire des données et dont les fonctions analytiques recherchent les signes évidents de corruption au niveau des métadonnées. La corruption au niveau des métadonnées, comme un changement de l'extension de fichier en chiffrée ou une modification radicale de sa taille, n'est pas difficile à détecter. Ces types d'attaques ne sont pas représentatives des méthodes les plus sophistiquées aujourd'hui utilisées par les cybercriminels.



CyberSense va plus loin que ces solutions limitées aux métadonnées, car il se base sur l'analytique complète du contenu pour détecter la corruption des données. Il effectue un audit des fichiers et des bases de données pour détecter même les attaques qui ciblent exclusivement le contenu ou la structure des fichiers, ou celles qui opèrent un chiffrement partiel à l'intérieur d'un document ou d'une page de base de données. Ces attaques ne peuvent pas être détectées par des outils qui n'analysent pas l'intérieur du fichier pour comparer son évolution au fil du temps. Sans une analytique basée sur l'ensemble du contenu, le nombre important de faux négatifs générés viendra fausser votre perception de l'intégrité et de la sécurité de vos données. De plus, CyberSense permet de créer des alertes basées sur des seuils personnalisés en fonction de la quantité ou de la proportion de fichiers ou d'extensions modifiés, créés ou supprimés, et de l'entropie sur un hôte.

Types de données pris en charge

CyberSense génère ses analyses à partir d'un large éventail de types de données, qui inclut l'infrastructure de base (DNS, LDAP, Active Directory, etc.), les fichiers non structurés (documents, contrats, propriété intellectuelle…) et les bases de données (dont Oracle, DB2, SQL, PostgreSQL, Epic Caché, entre autres).

Synthèse

Entièrement intégré à Dell PowerProtect Cyber Recovery, CyberSense audite vos données et détecte les indicateurs de danger et de corruption. CyberSense vous permet de déterminer proactivement le degré d'impact d'une cyberattaque en cours, afin de faciliter la mise en œuvre d'un plan de diagnostic et de restauration rapides, et de limiter les interruptions d'activité et les coûts importants qui vont de pair.

En savoir plus sur Dell PowerProtect Cyber Recovery	Contacter un expert Dell Technologies	En savoir plus sur CyberSense	Prenez part à la conversation avec #PowerProtect