DELL Technologies

Présentation

CyberSense® pour Dell PowerProtect Cyber Recovery

Outils d'analyse et de criminalistique alimentés par l'IA pour détecter et diagnostiquer les cyberattaques et y remédier de manière plus intelligente

L'AVANTAGE CYBERSENSE

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

- Analyse régulière des données de sauvegarde pour valider l'intégrité des données et alerter en cas de détection d'un comportement suspect.
- Analyse directe du contenu des images de sauvegarde de Dell Avamar, NetWorker, Commvault, NetBackup et PowerProtect Data Manager sans qu'il soit nécessaire de réhydrater les données.
- Il offre une analyse approfondie et complète de chaque scan de données pour détecter les attaques par ransomware, même les plus sophistiquées.
- Alertes personnalisées pour les règles YARA et les signatures de logiciels malveillants afin de détecter les comportements connus des ransomwares ou des acteurs malveillants internes.
- Facilite une restauration plus intelligente et plus rapide grâce à des rapports criminalistiques post-attaque qui permettent d'obtenir des informations détaillées sur la profondeur et l'étendue de l'attaque, ainsi qu'une liste des derniers jeux de sauvegardes fiables avant corruption.

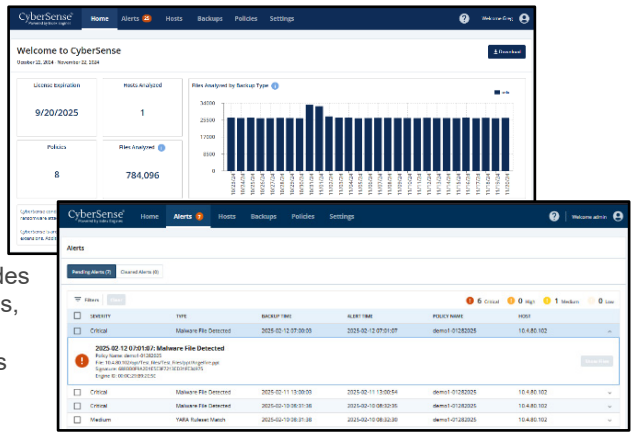
CyberSense se distingue des autres approches d'analytique des données et offre un plus haut degré de confiance quant à l'intégrité des données de sauvegarde et à la possibilité de les restaurer rapidement après une attaque.

Alors que la fréquence des cyberattaques ne cesse d'augmenter et que les cybercriminels deviennent de plus en plus résilients, les outils de sécurité conventionnels ne parviennent plus à protéger les données contre les cyberattaques.

CyberSense® intervient pour détecter avec une précision de 99,99 %* la corruption des données après une attaque, et facilite leur restauration intelligente et rapide. En tant que première ligne de restauration 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 et les documents stratégiques pour garantir que les données sont exemptes de toute corruption.

CyberSense analyse les sauvegardes de données dans un coffre-fort Cyber Recovery pour observer l'évolution des données au fil du temps. La solution utilise ensuite l'apprentissage automatique et l'IA pour détecter les signes de corruption indiquant une attaque par ransomware. Les données sont comparées à plus de 200 analyses basées sur le contenu pour détecter la corruption avec une confiance de 99,99 %*, 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 référentiels de fichiers, les systèmes de fichiers et les bases de données essentielles.

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 des restaurations rapides et organisées, contribuant à atténuer les interruptions d'activité et les pertes de données, et, ainsi, à réduire le coût de la cyberrestauration.

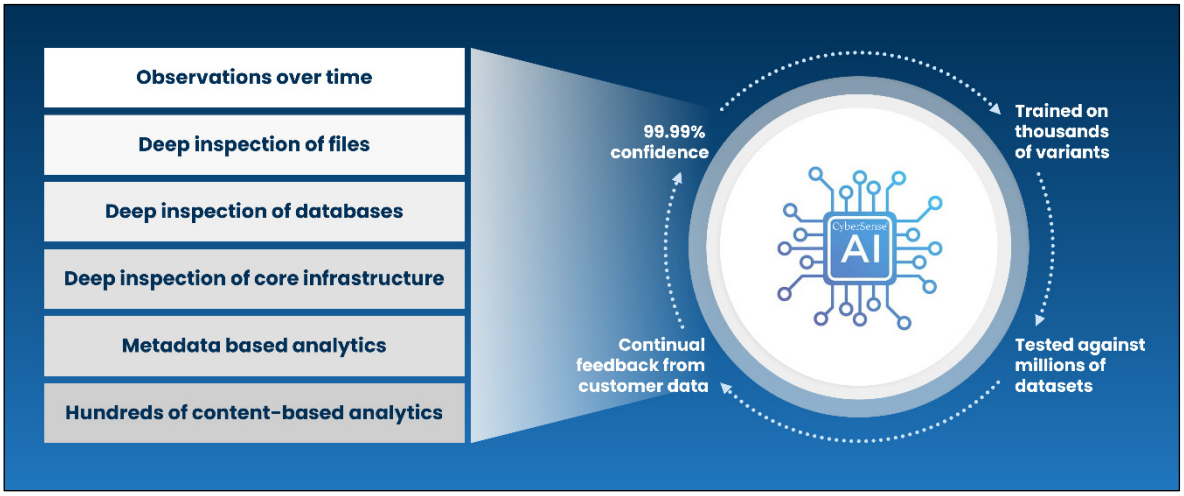


Le workflow Cyber Recovery

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. CyberSense suit méticuleusement les modifications apportées aux fichiers au fil du temps et permet d'identifier efficacement les données corrompues, même par les cybermenaces les plus sophistiquées.

Analyse complète du contenu

CyberSense est la seule solution du marché qui permet l'indexation et l'analyse de l'ensemble des données protégées. L'analyse de l'IA profonde de CyberSense porte sur l'ensemble des données et une décision probabiliste est générée avec une précision de 99,99 %* pour déterminer si les données sont intègres ou si elles ont été corrompues par un ransomware. 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.



Loin d'être un simple outil basé uniquement sur les métadonnées, CyberSense détecte la corruption des données à l'aide d'une analytique complète du contenu. La solution vérifie les fichiers et les bases de données pour détecter les modifications indiquant une attaque, y compris une corruption totale ou partielle des fichiers. L'analytique traditionnelle ignore ces menaces, ce qui entraîne un sentiment de confiance trompeur. Des alertes de seuil personnalisées peuvent être définies en fonction des modifications apportées aux fichiers, aux fichiers ajoutés ou aux fichiers supprimés. Des règles YARA personnalisées et des signatures de logiciels malveillants peuvent également être établies pour détecter les logiciels malveillants dans les sauvegardes, à la fois en amont et en aval.

Types de données pris en charge

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

Résumé

Entièrement intégré à Dell PowerProtect Cyber Recovery, CyberSense analyse les données de votre coffre-fort et détecte les indicateurs comportementaux 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, limitant ainsi les interruptions d'activité et les coûts importants qui vont de pair.

En savoir plus sur Dell PowerProtect Cyber Recovery

Contactez un expert Dell Technologies

En savoir plus sur CyberSense

Prenez part à la conversation avec #PowerProtect

* D'après le rapport ESG « Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption » réalisé à la demande d'Index Engines. Juin 2024