PRÉSENTATION DE LA SOLUTION

INFINIDAT

InfiniSafe® Cyber Detection

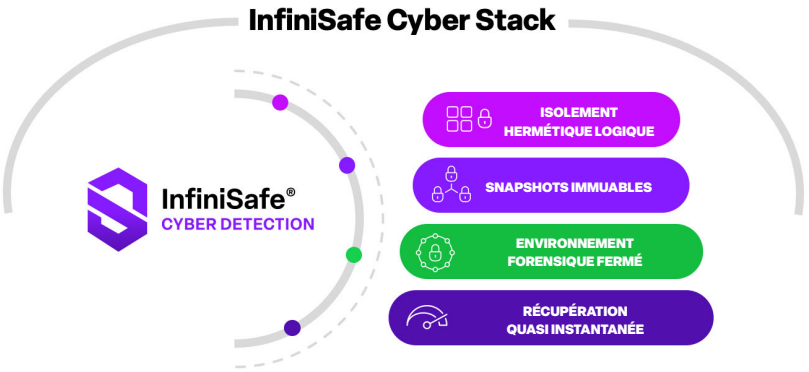
L'impact de la cybercriminalité devrait coûter aux entreprises 8 000 milliards de dollars par an[1] Toutes les 39 secondes, une nouvelle attaque se produit quelque part sur le web[2] Les coûts pour une entreprise comprennent la détérioration et la destruction des données, la perte de productivité, le vol de propriété intellectuelle, le vol de données personnelles et financières, le détournement de fonds, etc. Aux perturbations de l'activité après l'attaque s'ajoutent l'analyse forensique, la détection et la restauration des données et des systèmes piratés, ainsi que la perte de confiance et de réputation. La plupart des équipes de sécurité et informatiques pensent qu'elles subiront une cyberattaque, un jour ou l'autre. Vous sentez-vous prêt ?

La technologie InfiniSafe fournit une cyber stack multicouche pour la création d'environnements résilients de cyberstockage avec les plateformes InfiniBox® et InfiniBox™ SSA.

La nouvelle solution InfiniSafe Cyber Detection améliore les capacités de résilience et de réponse du cyberstockage d'Infinidat en permettant aux équipes de sécurité et informatiques de détecter les attaques de ransomware et de malware avec une précision avoisinant 99,5 %. Elle permet également la récupération quasi instantanée des données à partir de copies propres et « reconnues fiables » sur les plateformes InfiniBox et InfiniBox SSA.

InfiniSafe Cyber Detection ajoute un niveau de détection des données à la cyber stack InfiniSafe qui entoure les quatre couches principales de la pile et renforce la capacité d'InfiniSafe à détecter les cyberincidents. InfiniSafe Cyber Detection effectue une analyse approfondie des blocs, des fichiers et des bases de données en présentant les snapshots immuables des InfiniBox et InfiniBox SSA à de puissants moteurs d'analyse basés sur l'IA qui valident leur intégrité et, grâce à l'apprentissage automatique, identifient tout changement malveillant pouvant indiquer une cyberattaque.

Lorsqu'une attaque est détectée, InfiniSafe Cyber Detection fournit un rapport forensique pour diagnostiquer les données compromises et la nature de la compromission, et fournit des informations critiques sur l'origine des données compromises. Ensuite, grâce à la puissance de la technologie InfiniSafe, l'utilisateur peut rapidement reprendre ses activités normales, une fois qu'il a identifié une bonne copie connue des données.



La cyberdétection InfiniSafe utilise une combinaison de plus de 200 analyses basées sur le contenu complet qui inspectent le contenu des fichiers et des données, et pas seulement les métadonnées. De puissants algorithmes d'apprentissage automatique vous indiquent le type de variante utilisée pour corrompre les données avec une précision de 99,5 %, aidant les entreprises à protéger leur infrastructure et leur contenu critiques sans crouler sous les faux positifs. Vous pouvez ainsi vous concentrer sur les vrais problèmes et les résoudre rapidement.

Si la corruption des données est identifiée, InfiniSafe Cyber Detection fournit les outils forensiques nécessaires pour diagnostiquer, identifier et aider à récupérer les actifs affectés. InfiniSafe Cyber Detection signale les fichiers qui ont été impactés. Vos équipes dédiées à la sécurité et aux logiciels peuvent analyser les résultats forensiques afin d'éradiquer tous les problèmes, si nécessaire à l'aide de leurs propres outils. Les données compromises peuvent alors être facilement remplacées par leur dernière version reconnue fiable, ce qui garantit le retour à la normale des activités de l'entreprise avec un minimum de temps d'arrêt. InfiniSafe Cyber Detection est une option complémentaire à notre technologie principale InfiniSafe ; sa licence est basée sur un abonnement.

> « **79 %** des organisations déclarent que **la préparation aux ransomwares** figure parmi les cinq **priorités professionnelles** de leur équipe de direction et/ou de leur conseil d'administration »
>
> Rapport de recherche du Enterprise Strategy Group, The Long Road Ahead to Ransomware Prepareness, juin 2022

Détection

Analyse et détection par apprentissage automatique

Analyse forensique

Des rapports forensiques pour diagnostiquer et identifier l'impact de l'attaque

Récupération

Rapports sur la dernière version reconnue fiable des fichiers pour rationaliser la récupération

Si une corruption de données est identifiée, InfiniSafe Cyber Detection fournit les outils forensiques nécessaires pour diagnostiquer, identifier et aider à récupérer les actifs affectés. InfiniSafe Cyber Detection signale les fichiers qui ont été impactés. Vos équipes dédiées à la sécurité et aux logiciels peuvent analyser les résultats forensiques afin d'éradiquer tous les problèmes, si nécessaire à l'aide de leurs propres outils. Les données compromises peuvent alors être facilement remplacées par leur dernière version reconnue fiable, ce qui garantit le retour à la normale des activités de l'entreprise avec un minimum de temps d'arrêt. InfiniSafe Cyber Detection est une option complémentaire à notre technologie principale InfiniSafe ; sa licence est basée sur un abonnement. {InfiniSafe Cyber Detection est un produit post-attaque qui se concentre sur la résilience des données dans la cyber-pile InfiniSafe et ne remplace pas les meilleures pratiques de prévention des ransomwares et des malwares, ni les produits traditionnels de gestion des menaces sur les serveurs, applications et réseaux dans la stratégie globale de cyber-sécurité.

Detection

InfiniSafe Cyber Detection utilise l'analyse du contenu intégral de toutes les données protégées. Cette connaissance approfondie est le seul moyen de s'assurer que vos données sont intègres et que les cybercriminels ne contournent pas vos outils d'analyse de données, ne dissimulent pas leurs traces et ne corrompent pas secrètement vos données.

À l'instar de notre apprentissage automatique par cache neuronal, InfiniSafe Cyber Detection est doté d'un apprentissage automatique puissant et déterministe. Plus de 200 analyses combinées, soit 20 fois plus que les concurrents, avec des observations de données qui deviennent plus intelligentes au fil du temps avec davantage d'observations. L'apprentissage automatique est entraîné sur des milliers de ransomwares, de malwares et de chevaux de Troie afin de trouver des modèles de comportement inhabituels et de distinguer l'activité de l'utilisateur de celle du ransomware, tout en minimisant les faux positifs et les faux négatifs.cyber stack.

Analyse forensique

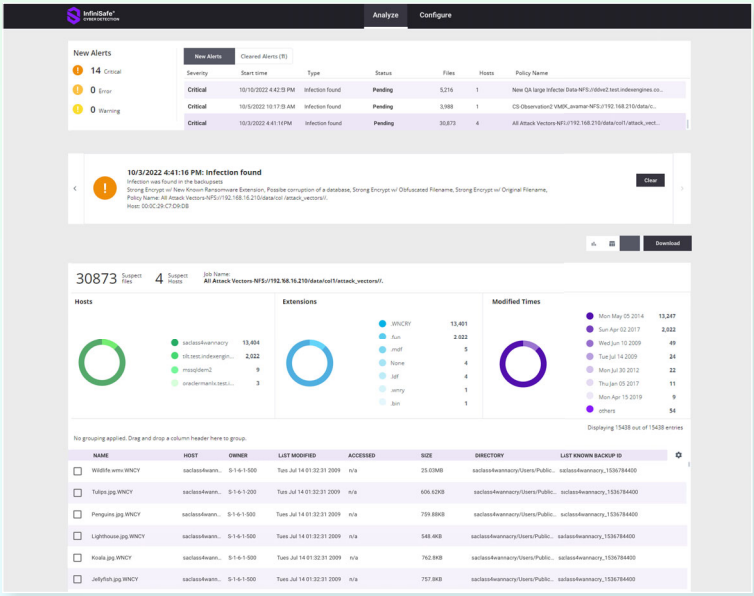
Lorsque des données sont corrompues, InfiniSafe Cyber Detection génère une liste des fichiers corrompus. Les fichiers corrompus sont marqués, puis les rapports forensiques sont créés pour diagnostiquer et identifier l'impact de l'attaque et fournir les informations nécessaires pour faciliter la récupération.

Alertes organisées par niveau de gravité

Nouveaux détails sur la suspicion de corruption

Graphiques dynamiques personnalisables permettant d'approfondir les détails de l'attaque

Liste des fichiers corrompus pouvant être téléchargée

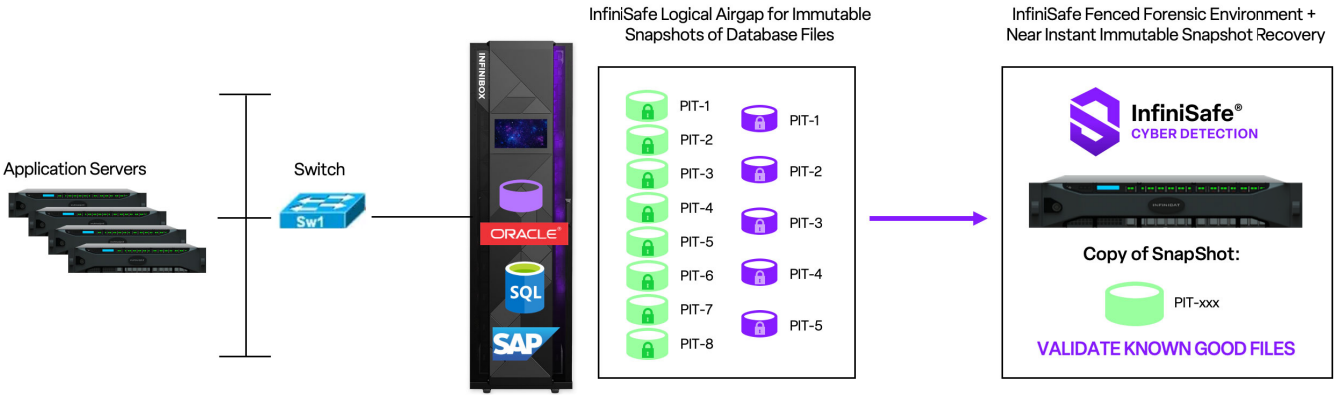


Le tableau de bord post-attaque : une expérience utilisateur améliorée, davantage d'insights sur les données, un flux de travail post-attaque intuitif.

Récupération

Enfin, InfiniSafe Cyber Detection signale la dernière copie reconnue fiable d'un fichier ou d'une sauvegarde lorsque la copie de sauvegarde se trouve sur une InfiniBox ou une InfiniBox SSA. La solution détermine où se trouvent les données corrompues, où se situe la dernière version reconnue fiable des données et quels sont les snapshots ou les jeux de sauvegarde dans lesquels se trouvaient les données, afin de rationaliser le processus de récupération.

Cas d'utilisation : Cyberdétection des blocs, des fichiers et des bases de données



Les entreprises qui utilisent l'InfiniBox ou l'InfiniBox SSA dans des applications de bases de données critiques savent, lorsqu'elles utilisent la technologie de cyber stack InfiniSafe avec Cyber Detection, qu'elles peuvent prendre des snapshots fréquents et immuables pour valider leur intégrité et, grâce à l'apprentissage automatique, identifier tout changement indiquant une cyberattaque. InfiniSafe Cyber Detection détermine tous les problèmes et signale les copies reconnues fiables des données pour une récupération quasi instantanée avec InfiniSafe.

Matrice de cyberdétection

Les entreprises utilisant plusieurs InfiniBox ou InfiniBox SSA peuvent répliquer les données vers une matrice de cyberdétection désignée, dans un environnement forensique fermé, en utilisant les outils de réplication natifs d'Infinidat. La matrice de cyberdétection analyse tous les fichiers de données, marque tous les fichiers corrompus et crée un rapport forensique. Cette configuration fournit aux entreprises les informations nécessaires pour détecter une cyberattaque.

Les ransomwares malveillants et les logiciels malveillants continuent de perturber les services et les entreprises critiques, qu'il s'agisse des pipelines d'énergie, d'écoles ou d'hôpitaux. Les pertes économiques totales dues aux ransomwares et aux attaques de logiciels malveillants continuent d'augmenter. La mise en œuvre d'une stratégie de cyberdétection efficace peut atténuer l'exposition de votre entreprise et assurer une récupération rapide.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

france@infinidat.com

INFINIDAT