PRÉSENTATION DE LA SOLUTION

Protégez-vous contre les attaques de ransomware avec Pure

Renforcez la protection de vos données avec Pure1, FlashArray, FlashBlade™ et les snapshots SafeMode.

Les attaques de ransomware restent l'une des préoccupations majeures des dirigeants d'entreprise et des responsables informatiques. Et pour cause, elles menacent gravement l'accès à l'élément vital de toute entreprise : ses données. Les conséquences peuvent en être catastrophiques : vous devrez soit payer les cybercriminels pour qu'ils décryptent vos données (ou pas), soit jongler entre les outils de décryptage, soit prier pour que l'une de vos sauvegardes fonctionne. Des millions de dollars sont dépensés chaque année pour protéger l'accès aux données… pourtant beaucoup d'entreprises sous-estiment encore la valeur stratégique d'une meilleure protection de leurs données.

Votre protection de données actuelle pourrait ne pas suffire

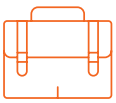
Les sauvegardes permettent de se prémunir contre des scénarios courants et de récupérer vos données critiques en cas de catastrophe naturelle provoquée par l'homme, de corruption des données ou de suppressions accidentelles. En revanche, les attaques de ransomware peuvent mettre sous tension plus que prévu les infrastructures de protection des données basées sur des architectures traditionnelles (par exemple sur disque ou sur bande).

Vos données et systèmes de sauvegarde peuvent être également compromis, nécessitant potentiellement la réinstallation et la reconfiguration de votre solution de sauvegarde avant même de pouvoir envisager la reprise des données.

Vous pensez certainement que le ransomware ne vise que des systèmes Windows et vous avez de ce fait stocké vos sauvegardes sur des serveurs Linux que vous considérez imprenables. Détrompez-vous : en 2019, une nouvelle famille de ransomwares appelés Lilocked (ou Lilu)[3] a vu le jour et commencé à cibler des serveurs Linux et les données qu'ils hébergent.

Risque financier

Les dépenses liées à l'attaque NotPetya ont contribué à une perte trimestrielle de 264 millions de dollars chez Maersk.[1]



Pertes de productivité

Le coût des temps d'arrêt est 23 fois plus élevé que le montant moyen des rançons exigées en 2018.[2]

[1] Forbes, août 2017.

[2] « A Look at Ransomware in 2019 » (Analyse des attaques de ransomware en 2019), Datto, octobre 2019.

[3] « Lilocked Ransomware Infects Thousands of Linux Servers to Encrypt Files » (Le ransomware Lilocked infecte des milliers de serveurs Linux et crypte leurs fichiers) SecurityIntelligence, septembre 2019.

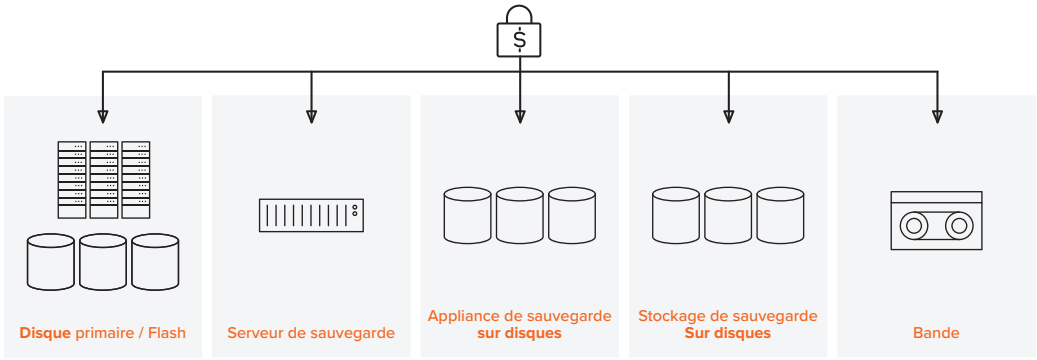
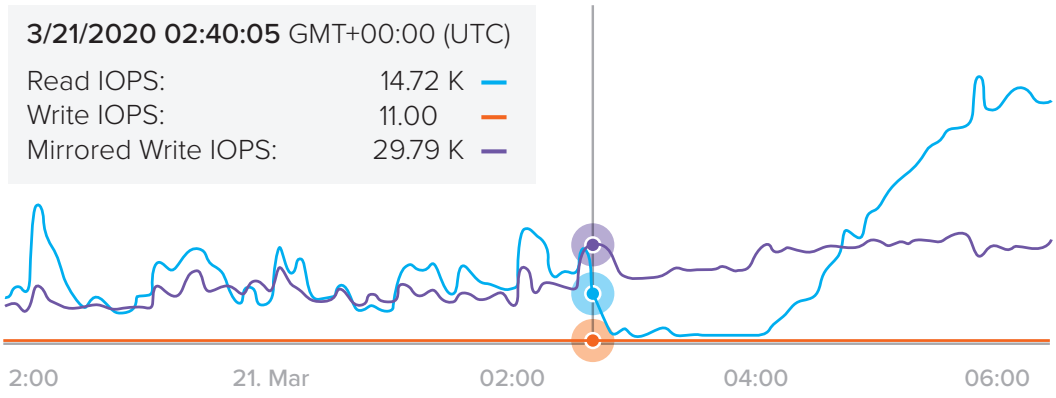


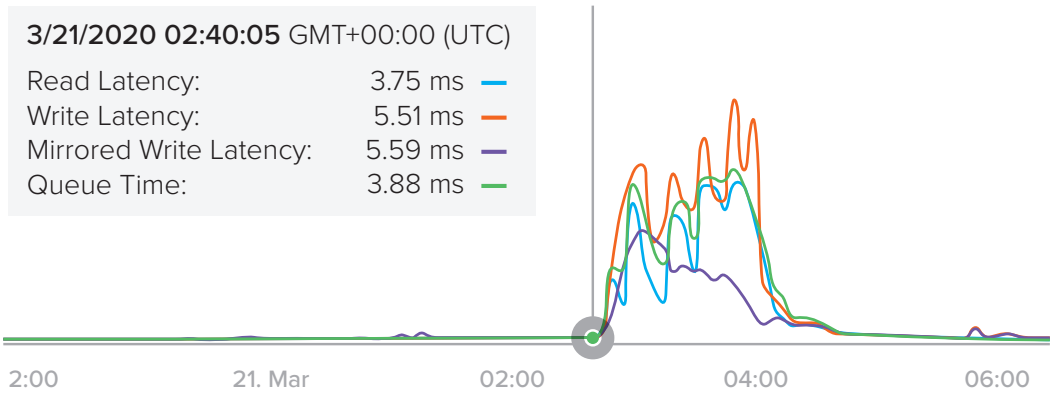
Figure 1 : Les attaques de ransomware peuvent compromettre les éléments clés de votre architecture de protection des données.

Détecter une activité anormale avec Pure1

Les ransomwares génèrent une charge de travail en I/O très supérieure à la normale qu'il est possible d'observer simplement avec la console Pure1 si vous stockez vos données sur une plateforme Pure Storage sur site ou dans le Cloud. Vous pouvez ainsi déterminer la date et l'heure de l'attaque, pour chaque VM, dans le but de restaurer les données à partir de vos derniers snapshots.

Le chiffrement des données par le ransomware a également pour conséquence une possible diminution du taux de réduction de données qu'il est également possible de détecter dans Pure1. Le volume de données chiffré par les ransomwares est très variable ; dans la plupart des cas observés, ce volume reste relativement faible par rapport à l'ensemble des données stockées.



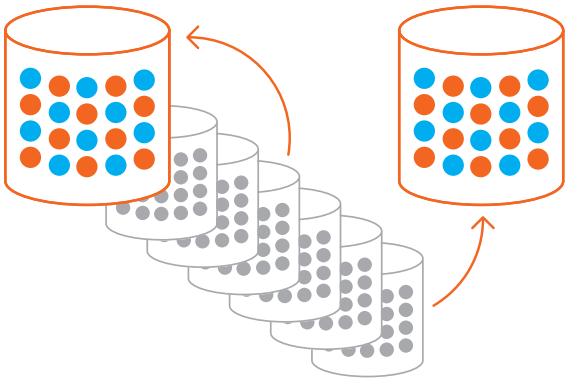


Gagnez en agilité et en rapidité avec les snaps FlashArray

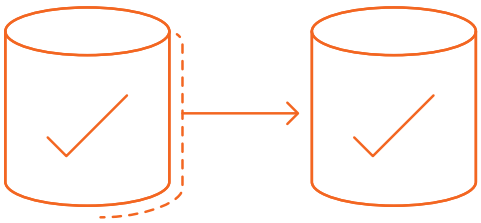
Les snapshots immuables FlashArray sont un bon moyen pour remonter le temps et tester la cohérence des données avant de revenir à l'état juste avant l'attaque portant sur les serveurs incriminés. Totalement indolores pour la production, n'occasionnant pas de dégradation de performance des volumes de données en production dans la durée, ne nécessitant pas d'opération de réservation d'espace au niveau du volume ou méta-volume, et utilisables immédiatement sous forme de copie instantanée sans consommer d'espace supplémentaire grâce à la déduplication, ces jeux de données sont montés sur des serveurs hors-ligne pour tester la cohérence des données.

Pour faire face aux ransomwares il est recommandé de faire au moins **1 à 2 snaps quotidiens** et de les **conserver de 7 à 14 jours**.

Restorer n'importe quel cliché vers n'importe quel volume



100% metadata



Instant snaps & clones

Renforcez la protection de vos données avec les snapshots SafeMode

Les snapshots SafeMode est une fonctionnalité intégrée aux baies FlashBlade™. Elle vous permet de créer des snapshots en lecture seule de vos données sauvegardées et de leurs catalogues de données associés, une fois vos sauvegardes intégrales réalisées. Vous pouvez récupérer les données directement depuis ces snapshots, ce qui vous permet de vous prémunir contre les attaques de ransomware et même contre les administrateurs peu scrupuleux. En outre FlashBlade fournit les avantages suivants :

- **Protection accrue –** Les ransomwares ne peuvent pas éradiquer (supprimer), modifier ou crypter les snapshots SafeMode. En outre, seule une personne désignée dans votre entreprise peut travailler directement avec le support technique Pure afin de configurer la fonctionnalité, modifier la politique ou supprimer manuellement les snapshots.
- **Intégration des sauvegardes –** Utilisation du même processus de snapshot quels que soient le produit de sauvegarde ou les outils natifs utilisés pour gérer les processus de protection des données.
- **Flexibilité –** La cadence de création et de suppression des snapshots est personnalisable.
- **Restauration rapide –** Exploitation d'une architecture massivement parallèle et de performances élastiques qui s'adaptent aux données pour accélérer la sauvegarde et, par là même, la reprise.
- **Protection des investissements –** FlashBlade inclut les snapshots SafeMode sans frais supplémentaires. Votre abonnement ou votre contrat de support et maintenance couvrent les améliorations.

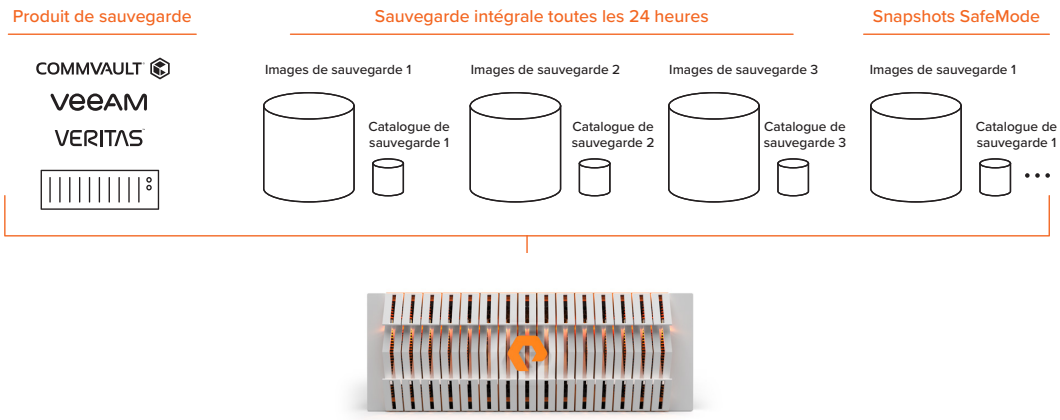


Figure 2 : Les opérations quotidiennes créent des snapshots en lecture seule des images de sauvegarde et du catalogue de métadonnées.

Ressources complémentaires

En savoir plus sur les snapshots SafeMode.

PS1030-01 11/2019