DOSSIER ESG

Renforcer votre cyber-résilience avec Veritas

Date : septembre 2021 **Auteurs :** Christophe Bertrand, Senior Analyst ; Monya Keane, Senior Research Analyst

RÉSUMÉ : Les départements IT sont constamment mis à l'épreuve par le risque des cyberattaques et l'impact sévère qui peut en résulter sur les activités de l'entreprise. L'établissement d'une stratégie robuste pour protéger, détecter et récupérer ses données lors de ces événements est crucial. Veritas peut vous y aider grâce à un ensemble de technologies différenciées et éprouvées qui devraient faire partie des ensembles d'outils de lutte contre les cybercriminels de tous les professionnels de l'informatique.

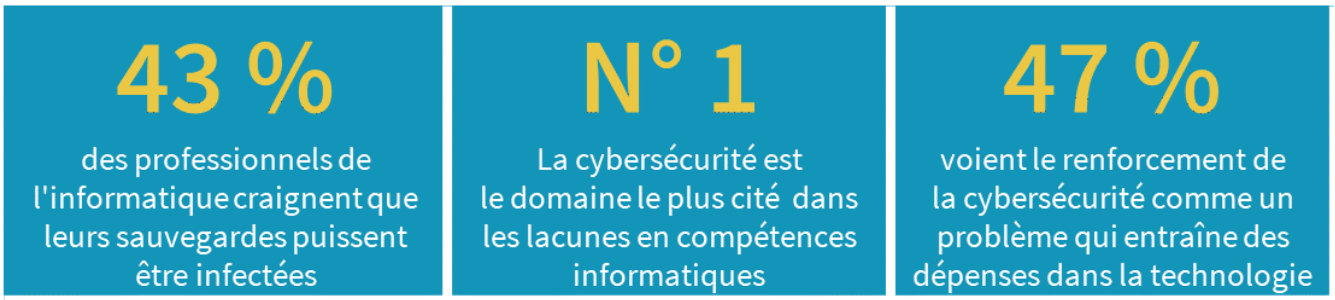
Aperçu du marché

Les recherches d'ESG confirment ce que les actualités nous ont déjà appris : la fréquence des attaques de ransomware est élevée. Cette année, 18 % des entreprises ont signalé avoir été victimes d'attaques quotidiennes et 24 % ont signalé être victimes d'une attaque par semaine.[1] La conséquence négative directe de ces attaques est l'interruption des activités. Les interruptions coûtent cher et ne touchent pas uniquement le service informatique mais toute l'entreprise. D'après l'étude menée par ESG, en moyenne, une application d'entreprise sur trois est critique. 15 % de ces applications sont tellement importantes qu'elles ne peuvent tolérer aucun temps d'arrêt et le temps d'arrêt tolérable estimé pour des applications critiques est uniquement de deux heures.[2]

Les environnements de production ne sont pas les seuls exposés à des risques : 43 % des professionnels de l'informatique interrogés par ESG indiquent être très inquiets à l'idée que les sauvegardes de leurs entreprises puissent être infectées ou compromises par une attaque de ransomware (voir la Figure 1).[3] Cette préoccupation mène à des actions : 47 % des personnes interrogées dans le cadre de l'étude d'ESG voient le renforcement de la cybersécurité de leur entreprise comme un enjeu qui entraîne des dépenses pour la technologie et 25 % se focalisent également sur l'investissement dans le renforcement des programmes de continuité des affaires et de reprise après incident.[4]

La situation est exacerbée par le manque important de certaines compétences qui touche tout le secteur informatique. Le manque d'expertise en cybersécurité en particulier a été signalé par 48 % des personnes interrogées et le manque de compétences en matière de protection des données par 24 % des personnes interrogées.[5]

Figure 1. Le paysage des cybermenaces actuel



Source : Enterprise Strategy Group

[1] Source : ESG Master Survey Results, *Tape's Place in an Increasingly Cloud-based IT Landscape*, janvier 2021.
[2] Source : ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, août 2020.
[3] Source : ESG Master Survey Results, *Tape's Place in an Increasingly Cloud-based IT Landscape*, janvier 2021.
[4] Source : ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, décembre 2020.
[5] Ibid.

Tirer parti du cadre de cybersécurité du NIST

Le NIST (National Institute of Standards and Technology) a publié le cadre de cybersécurité du NIST (voir la Figure 2) pour aider les entreprises à évaluer les menaces de cybersécurité auxquelles elles font face. Ce cadre indique comment les parties prenantes internes et externes peuvent gérer et réduire ces risques.

Au sein de ce cadre, les recommandations sont organisées en 5 fonctions, puis sous-divisées en 23 catégories. Dans chaque catégorie, le cadre définit un certain nombre de sous-catégories (108 au total) sur les conséquences sur la cybersécurité et les contrôles de sécurité.

Figure 2. Le cadre du NIST

Source : NIST.gov

Protection, détection et récupération à l'aide de l'approche Veritas

Ces derniers mois, Veritas a utilisé le cadre du NIST pour identifier les domaines dans lesquels ses solutions peuvent être intégrées dans le contexte de la stratégie de cyber-résilience d'une entreprise. À partir de ces conclusions, Veritas a défini trois piliers : la protection, la détection et la récupération. Veritas a confiance en sa capacité à aider de manière significative les entreprises dans ces trois domaines.

Protection

Les entreprises ont besoin d'un logiciel de protection véritablement complet. Si une des parties d'un environnement est accidentellement exposée à une attaque de ransowmare, cela signifie que vous n'avez pas correctement protégé l'ensemble de votre environnement. La récupération sera plus difficile, voire impossible. Aujourd'hui, beaucoup de cybercriminels ne se concentrent pas seulement sur la capture des données, mais s'attaquent également à l'infrastructure elle-même, par exemple en surchargeant les environnements de machines virtuelles ou en ciblant des composants spécifiques du réseau de l'entreprise.

Immutabilité

Cette tendance fait de l'immutabilité un élément vital. Les données qui sont immuables ne peuvent pas être modifiées ou corrompues par un ransomware une fois stockées. Cela constitue une couche de protection importante. Veritas fournit une immutabilité native sur ses appliances Flex mais ne s'arrête pas là. Les appliances Flex comprennent également une horloge indépendante et inviolable qui empêche les attaquants d'accélérer artificiellement l'expiration des images (qui est une technique bien connue utilisée par les auteurs de ransomwares).

Veritas travaille avec des fournisseurs de logiciels tiers, notamment Data Domain de Dell et NEC HYDRAstor, pour proposer une interface via la technologie de plug-in OST. Via l'API, la solution Veritas est capable d'indiquer au matériel qui reçoit les données pendant combien de temps il doit les conserver. Veritas a créé deux modes de déploiement. Il s'agit des modes suivants :

- Mode de conformité : c'est un mode verrouillé. Peu importe les informations d'identification dont vous disposez, pendant la durée prédéterminée de conservation des données immuables, elles resteront immuables et ineffaçables. En d'autres termes, personne ne peut ni les chiffrer, ni les supprimer.
- Mode entreprise : ce mode permet aux administrateurs IT de faire expirer des images en cas de préoccupation en matière de gestion de la capacité de stockage (ce qui peut devenir un véritable défi avec les données immuables). Tout comme les dispositifs de protection de certaines armes nucléaires nécessitent deux personnes autorisées pour toute activation, le Mode entreprise nécessite les informations de connexion de deux administrateurs pour renforcer la sécurité.

Veuillez noter que ces deux modes de déploiement concernent les appliances de stockage Veritas Flex immuables et non les capacités OST.

Sauvegarde sans faille

Pour faire simple, la sauvegarde sans faille consiste en la création d'un système, de données ou d'un réseau qui ne possèdent pas d'autres interfaces connectées par câble ou sans fil à des réseaux externes. Pendant de nombreuses années, Veritas a pris en charge la sauvegarde sans faille sur bande via des solutions de centres de sauvegarde et de cartouches éjectables. Cette méthodologie a depuis longtemps fait ses preuves. Mais aujourd'hui, beaucoup d'entreprises souhaitent une résilience similaire sous une forme numérique. Veritas a configuré sa fonctionnalité de réplication d'image automatique pour reproduire beaucoup d'avantages de la sauvegarde sans faille traditionnelle sur bande.

Un serveur de sauvegarde primaire de NetBackup écrit de façon unidirectionnelle sur un second serveur NetBackup. Les données dédupliquées et chiffrées sont conservées dans ce second serveur de sauvegarde. Le réseau des services sortants est complètement séparé du serveur unidirectionnel, ce qui recrée la fonctionnalité de la sauvegarde sans faille.

Les informations de connexion peuvent également être différentes sur ce serveur. De ce fait, même si un environnement de production primaire complet est compromis, cela ne signifie pas forcément que le second environnement sera également affecté.

Et les données sont écrites au format de données d'images pour NetBackup, ce qui signifie que ces données sont en réalité *inertes*. Si des fichiers chiffrés par des ransomwares arrivent jusqu'à vos images de sauvegarde, ils ne peuvent pas infecter le reste du système. Ils restent simplement sur place, comme des images inertes figées dans le temps et incapables d'infecter le reste de votre environnement. Et toutes les images sont isolées les unes des autres, ce qui renforce encore davantage cette approche.

Cloud et S3

NetBackup peut être déployé dans un environnement cloud. NetBackup v9.1 peut utiliser S3 comme cible de stockage. Il ne dépose pas simplement ses données sur ce support, il communique avec la cible pour définir combien de temps conserver une image particulière. Nul besoin de réhydrater les données, ni de faire intervenir un tiers. Les données se dirigent directement vers le compartiment d'objet S3 et restent dédupliquées à cet emplacement. Cela constitue une façon remarquablement efficace de tirer parti des cibles de stockage immuables sur le cloud pour la protection contre les ransomwares.

Détection

Veritas s'assure que les entreprises bénéficient d'une visibilité complète sur leur environnement. Tout élément (comme les charges de travail ou le matériel) inconnu des équipes informatiques constitue un risque. Il est dangereux de ne pas disposer d'une vision vraiment complète.

Veritas NetBackup IT Analytics

Veritas NetBackup IT Analytics crée des rapports sur les éléments informatiques, le stockage, les serveurs physiques, les MV et les serveurs cloud dans l'intégralité d'un environnement. Il crée également des rapports sur zones de l'environnement qui peuvent être protégées par d'autres produits de fournisseurs de sauvegarde, pas uniquement Veritas mais aussi Dell EMC, Rucrik, Cohesity, Veeam, Commvault, etc.

Veritas NetBackup IT Analytics effectue également des détections d'anomalies tout aussi étendues. Il propose des modèles prédéfinis pour la détection d'anomalies de ransomware et des capacités d'automatisation qui facilitent sont utilisation par les administrateurs qui ne sont pas forcément spécialisés en cybersécurité. Lorsque vous travaillez avec des centaines ou des milliers de machines virtuelles, vous avez besoin d'une solution comme celle-ci.

Veritas NetBackup effectue des détections d'anomalies dans les sauvegardes pour déterminer si une opération prend trop de temps, si la sauvegarde a un volume étrangement élevé ou si le ratio de déduplication est différent de celui attendu. Ces anomalies peuvent signaler des infections et elles déclenchent un rapport à un administrateur qui peut y accéder et corriger le problème lorsque c'est nécessaire. Au fil du temps, l'IA permet d'améliorer la détection d'anomalies et la différenciation de faux positifs par rapport aux réelles menaces grâce à l'apprentissage.

Les autres capacités de NetBackup liées à la réduction des risques de phishing comprennent un contrôle d'accès basé sur les rôles, la segmentation de l'environnement, et une authentification à plusieurs facteurs pour éviter qu'une attaque de phishing ne devienne une réelle menace. Veritas prend en charge le SAML (Security Assertion Markup Language) pour l'authentification à plusieurs facteurs, ce qui étend l'authentification à plusieurs facteurs à l'environnement NetBackup.

Veritas s'assure également que les communications ne puissent pas être détournées. Une étape d'autorisation de certificat doit avoir lieu entre les clients et les serveurs de sauvegarde. Du côté de l'utilisateur final, NetBackup offre un contrôle très granulaire et un accès basé sur les rôles.

Pour les ransomwares qui ciblent les données de sauvegarde, toute exfiltration de ces données est facilitée grâce au chiffrement des données en transit ou au repos. NetBackup prend en charge de nombreux services de chiffrement.

Veritas Data Insight

Pour les systèmes de fichiers, la solution Veritas Data Insight fournit des capacités de création de rapports prêtes à l'emploi avec des modèles prédéfinis conçus pour trouver des extensions de fichiers de ransomwares connues. Elle permet également une vision très granulaire des activités utilisateur. Le plus souvent, les ransomwares s'infiltrent dans une entreprise par le biais d'une attaque de phishing. Veritas Data Insight suit l'utilisation des fichiers par utilisateur et par groupe. Il reconnaît :

- Les opérations de lecture inhabituelles, qui indiquent des attaques d'exfiltration.
- Les opérations d'écriture inhabituelles qui pourraient être des attaques de chiffrement.
- Toute activité inhabituelle d'accès aux fichiers par un utilisateur.

Lorsqu'une activité inhabituelle est détectée, il la signale comme une attaque préliminaire potentielle. Vous pouvez ensuite éliminer l'attaque avant qu'elle ne se produise en tirant parti de cette vue granulaire de l'activité des utilisateurs.

Récupération

Vous avez besoin *d'options* de récupération. Parfois, ce qui est chiffré est un serveur en particulier qui possède une base de données en fonctionnement. Il peut également s'agir d'un système de fichiers ou d'un ensemble de fichiers particuliers. Mais peut-être que des serveurs situés ailleurs dans votre environnement se trouvent dans une batterie de serveurs de MV ou sur AWS ou Azure et peuvent, en théorie, exécuter la charge de travail.

Restauration granulaire

Veritas offre une restauration très rapide et granulaire, une restauration Bare Metal de serveurs physiques et une restauration des MV sur site, des MV sur le cloud et des conteneurs Kubernetes.

Cette récupération s'étend jusqu'aux systèmes ciblés individuellement. Si le serveur lui-même est chiffré, NetBackup peut effectuer une restauration complète Bare Metal de l'intégralité du serveur. La solution peut également effectuer une restauration rapide par lots. Grâce à la récupération instantanée, plutôt que d'effectuer des restaurations complètes, Veritas propose une façon d'associer la nouvelle protection des données continue incluse dans la dernière version de son logiciel phare grâce à la fonction de récupération. Elle envoie de petites quantités de données, mais permet de faire fonctionner de nouveau toute la MV rapidement.

Cloud

Veritas possède des capacités robustes et efficaces d'écriture et de stockage des données depuis un état dédupliqué vers un stockage S3 immuable. Pour tirer parti de ces données stockées de façon efficace, Veritas est capable de mettre en place un datacenter à la demande sur le cloud : les données secondaires ou tertiaires peuvent désormais être au cœur d'un datacenter qui n'existait pas auparavant.

Ces capacités permettent d'économiser de l'argent pour les opérations normales : vous n'utilisez le datacenter que lorsque c'est nécessaire. Mais elles permettent également de remplacer l'intégralité du datacenter si nécessaire. L'équipe informatique peut mettre en place cet environnement en tant qu'environnement EC2 dans le cloud créé depuis les données dédupliquées. Il en résulte un datacenter séparé disponible et entièrement fonctionnel, sans les charges liées au calcul permanent.

Orchestration et test

Tout se fait d'une manière orchestrée via une exécution en un clic. Des dizaines de serveurs et différentes parties de la pile peuvent être restaurés dans un ordre spécifique. Vous pouvez exécuter votre stratégie de résilience d'un simple clic.

Vous pouvez également la tester sans affecter votre activité. Pour connaître l'efficacité d'une stratégie, les tests sont indispensables. Mais il est difficile de réaliser des tests lorsque ceux-ci bloquent votre environnement de production. Veritas veut s'assurer que vous testez souvent et sans difficulté vos capacités de récupération en cas d'attaque de ransomware.

Conclusion

Les ransomwares et les cyber-risques ne sont pas près de disparaître et ils sont de plus en plus dangereux. Construire une infrastructure résiliente qui alimente une posture proactive sera la clé pour remporter ce combat. Tirer parti du cadre du NIST, comme l'a fait Veritas, est une excellente façon d'aborder le problème.

Veritas offre également une solution différenciée. Sa sauvegarde numérique sans faille avec la technologie AIR (Auto Image Replication), sa capacité à envoyer des données dédupliquées de façon native directement vers les objets S3, son moteur NetBackup d'IA/de ML, ses capacités de création de rapports globaux, d'analyses et d'alertes, ses options de récupération granulaires et l'orchestration avancée reflètent combien Veritas a travaillé pour mettre au point sa solution afin de protéger ses clients et prospects et leur permettre de rester en sécurité face aux pirates.

Veritas permet de créer de la valeur en offrant des solutions qui couvrent les trois piliers de sa méthodologie : protection, détection et récupération. Elle fournit une technologie qui a fait ses preuves et qui fonctionnera dans une grande variété d'environnements de façon évolutive.

Enterprise Strategy Group est un cabinet d'analyses, de recherches, de validation et de stratégie, qui alimente la communauté IT mondiale en renseignements commerciaux et en analyses exploitables.

www.esg-global.com contact@esg-global.com 508.482.0188