Communiqués de presse

IBM ajoute des fonctionnalités de résilience des données enrichies par l'IA pour aider à lutter contre les ransomwares et autres menaces avec des solutions de stockage optimisées

Par Frédéric Levy, Storage Leader, IBM France, le 12 mars 2024 : Les cyberattaques constituent un risque existentiel, 89 % des organisations classant les ransomwares parmi les cinq principales menaces pour leur viabilité, selon un rapport de novembre 2023 de l'Enterprise Strategy Group de TechTarget, un cabinet d'analystes de premier plan[1]. Et ce n'est là qu'un des nombreux risques qui pèsent sur les données des entreprises - les menaces internes, l'exfiltration de données, les pannes matérielles et les catastrophes naturelles représentent également un danger important. De plus, comme l'indique le rapport IBM X-Force Threat Intelligence Index 2024 qui vient d'être publié, à mesure que le marché de l'IA générative s'établit, celle-ci devient une cible d'attaque de plus en plus attirante, ce qui inciterait les cybercriminels à investir encore davantage dans de nouveaux outils. Le rapport note que les entreprises devraient également reconnaître que leur infrastructure sous-jacente existante est une passerelle vers leurs modèles d'IA qui ne nécessite pas de nouvelles tactiques de la part des attaquants pour la cibler[2].

Pour aider les clients à contrer ces menaces grâce à une détection plus précoce et plus précise, nous annonçons de nouvelles versions améliorées par l'IA de la technologie IBM FlashCore Module disponible dans les nouveaux produits IBM Storage FlashSystem, ainsi qu'une nouvelle version du logiciel IBM Storage Defender pour aider les organisations à améliorer leur capacité à détecter les ransomwares et autres cyberattaques qui menacent leurs données et à y répondre.

La quatrième génération de la technologie FlashCore Module (FCM), récemment disponible, offre des capacités d'intelligence artificielle au sein de la famille IBM Storage FlashSystem. FCM fonctionne avec Storage Defender pour assurer la résilience des données de bout en bout dans les applications primaires et secondaires, avec des capteurs alimentés par l'IA conçus pour une notification plus précoce des cyber-menaces afin d'aider les entreprises à reprendre leur fonctionnement normal plus rapidement.

Détection précoce des menaces dans le flux de données

Les produits IBM FlashSystem existants analysent toutes les données entrantes jusqu'à une granularité au niveau bloc sans impact sur les performances au fur et à mesure qu'elles sont écrites, en utilisant un logiciel de détection de corruption des données en ligne et une IA basée sur le Cloud pour aider à identifier les anomalies qui pourraient indiquer le début d'une cyberattaque, permettant ainsi au système de détecter, de répondre et de restaurer rapidement avec des copies immuables. La nouvelle technologie mise en œuvre par FCM4 est conçue pour surveiller en permanence les statistiques recueillies à partir de chaque entrée/sortie, en utilisant des modèles de machine learning pour détecter les anomalies telles que les ransomwares en moins d'une minute[3].

« Les cybermenaces évoluent rapidement, ce qui fait de la détection précoce une étape critique lorsque nous aidons nos clients à répondre aux attaques », a déclaré **Daneyand "DJ" Singley, Executive Director chez MAPSYS**. *« Nous nous sommes tournés vers IBM FlashSystem et FCM3 pour aider nos clients à obtenir une récupération rapide, et avec la nouvelle technologie FCM4 dans les nouvelles baies FlashSystem, nous anticipons la capacité à prendre des mesures immédiates pour contrecarrer les attaques. »*

Les produits IBM FlashSystem mesurent déjà des paramètres tels que la compressibilité et le caractère aléatoire, ou entropie, des données, et transmettent ces informations au logiciel IBM Storage Insights afin qu'il puisse alerter les opérateurs lorsqu'une anomalie de l'application a été détectée, par exemple lorsqu'un ransomware commence à chiffrer les données d'une application. La technologie FCM4 des nouvelles baies FlashSystem est conçue pour capturer et résumer des statistiques détaillées sur chaque entrée/sortie en temps réel. FlashSystem utilise des modèles de machine learning pour distinguer les ransomwares et les logiciels malveillants du comportement normal, ce qui permet aux entreprises de prendre des mesures et de continuer à fonctionner en cas d'attaque.

« Les organisations doivent adopter une approche de « défense en profondeur » contre les ransomwares et autres cyberattaques, d'autant plus que les logiciels malveillants deviennent de plus en plus sophistiqués », a déclaré **Dave Pearson, Research VP, Infrastructure, IDC**. *« L'infrastructure de stockage est une autre couche où la cyber-résilience peut être améliorée, et IBM a construit son nouveau FlashCore Module 4 avec des fonctionnalités basées sur l'IA conçues pour accélérer la détection des ransomwares, réduire la propagation et l'impact et accélérer la récupération. »*

Identifier plus intelligemment les menaces dans l'ensemble des applications

Le logiciel IBM Storage Defender offre une résilience des données de bout en bout dans les environnements informatiques hybrides multi-cloud modernes qui incluent des machines virtuelles (VM), des bases de données, des applications, des systèmes de fichiers, des charges de travail SaaS et des conteneurs. La nouvelle version d'IBM Storage Defender étend ses capacités de détection des menaces pour aider à renforcer la fiabilité des copies comme base de référence pour les équipes afin de commencer la récupération après les cyberattaques. De plus, IBM Storage Defender comprend des capteurs alimentés par l'IA et développés par IBM Research, qui sont conçus pour détecter rapidement les ransomwares et autres menaces avancées avec une grande précision. Defender envoie des alertes de haute pertinence aux outils de sécurité afin de réduire le rayon d'action des failles de sécurité et d'aider les entreprises à se remettre des attaques.

Nous avons ajouté à IBM Storage Defender des fonctionnalités de gestion des applications et de l'inventaire du stockage, conçues pour aider les entreprises à évaluer l'étendue de leurs applications et de leurs données. Cela peut les aider à intégrer leurs actifs dans un plan de continuité des activités pour restaurer au plus vite les services les plus critiques après une cyberattaque. Defender permet également d'orchestrer et d'automatiser la récupération des applications VMware.

L'attrait de Defender réside en partie dans la facilité avec laquelle il s'intègre à d'autres solutions IBM Storage et IBM Security, notamment IBM QRadar, IBM Guardium, IBM FlashSystem, IBM Storage Scale,IBM Storage Ceph et IBM Fusion. Au-delà des solutions IBM, Defender s'intègre à Cohesity et s'intégrera à d'autres plateformes de données tierces afin d'assurer la résilience des données de bout en bout dans l'ensemble des données de l'entreprise.

Mieux ensemble

Individuellement, FlashSystem et Defender disposent de fonctionnalités qui peuvent aider les entreprises à accroître la résilience de leurs données, mais ils sont encore plus performants ensemble. Par exemple, les administrateurs de stockage peuvent désormais créer des groupes de protection qui incluent des volumes spécifiques et qui sont automatiquement sauvegardés conformément aux politiques définies par l'utilisateur. Les copies immuables des données peuvent désormais être restaurées ou récupérées vers plusieurs emplacements cibles, y compris différents emplacements lors de la récupération après une cyberattaque. De plus, les copies immuables peuvent être répliquées vers un autre cluster IBM Storage Defender pour une couche de protection supplémentaire.

Nous avons également mis au point des paramètres qui permettent aux administrateurs d'automatiser la création d'instantanés immuables Safeguarded Copy, des copies ponctuelles cyber-résilientes de données qui ne peuvent pas être modifiées ou

supprimées par des erreurs d'utilisateur, des actions malveillantes ou des cyber-attaques. L'isolation de ces copies de sauvegarde des données de production est conçue pour permettre aux organisations de récupérer les données plus rapidement après une perte de données.

De nouveaux rapports montrent que les acteurs malveillants déploient désormais des cyberattaques basées sur l'IA, et nous devons combattre le feu par le feu. Notre nouveau matériel FlashCore Module et notre logiciel Storage Defender s'appuient tous deux sur les capacités d'IA d'IBM pour les aider à mieux relever ce défi. Le portefeuille de produits IBM contribue non seulement à fournir une résilience complète des données aux clients, y compris à de nombreuses organisations financières et de soins de santé parmi les plus importantes au monde, afin de les aider à éviter les menaces en premier lieu, mais aussi à accélérer le processus de récupération dans le cas où les attaquants ont réussi à s'infiltrer.

Pour découvrir IBM FlashSystem lors d'une démonstration virtuelle : https://www.ibm.com/fr-fr/flashsystem/resources/demo

Pour en savoir plus sur IBM Storage Defender https://www.ibm.com/fr-fr/products/storage-defender

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com

---

[1] *2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation, published by Enterprise Strategy Group / TechTarget, November 2023*

***[2]** Rapport IBM : L'identité numérique fait l'objet d'attaques, ce qui ralentit le temps de récupération des entreprises suite à des violations, publié par IBM Security, Février 2024*

[3] ***Disclaimer:*** *Internal experimentation by IBM Research has demonstrated detection of ransomware within 1 minute of the ransomware starting its encryption process. This experiment was done on a FlashSystem 5200 with 6 FCMs with the 4.1 firmware load. The 5200 had 8.6.3 GA level software loaded. The host connected to the 5200 was running Linux with XFS Filesystem. In this particular case, the IBM ransomware simulator called WannaLaugh was used. Underlying system must be compatible with FCM4.1 and version 8.6.3 GA level software loaded in order to receive results obtained.*
