Les 5 principales raisons pour lesquelles votre entreprise devrait être protégée par une solution EDR dès maintenant

Acronis

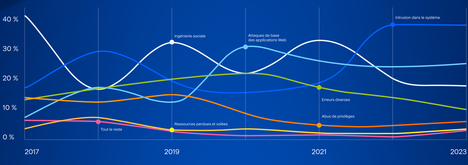
01.
L'augmentation des risques numériques exigent une approche axée sur la prévention

Le coût moyen d'une compromission des données a atteint un record historique en 2023 de 4,45 millions de dollars. Cela représente une augmentation de 2,3 % par rapport à

Source : Cost of Data Breach Report, 2023, Ponemon Institute et IBM Security.

02.
Assurer la défense contre les attaques avancées

Les attaques sont de plus en plus sophistiquées et vous avez besoin de contrôles de sécurité plus avancés, tels que l'EDR, pour être protégé.



Source: Verizon Data Breach Investigation Report (DBIR)

03.
Accélérer la réponse aux incidents et enrichir l'analyse

51 % des organisations prévoient d'accroître leurs investissements en sécurité à la suite d'une violation. Les principaux domaines identifiés pour des compromission. Supplémentaires compreniant la planification et les tests de réponse aux incidents (IR), la formation des employés et les technologies de détection et de réponse aux menaces.

Types de placement les plus courants parmi ceux qui augmentent leurs investissements en sécurité à la suite d'une compromission

Source: Cost of Data Breach Report, 2023, Ponemon Institute et IBM Security.

04.
Assurer la conformité aux exigences réglementaires existantes et imminentes

Chaque entreprise de catégorie A doit mettre en œuvre, à moins que le CISO n'ait approuvé par écrit l'utilisation de contrôles compensatoires raisonnablement équivalents ou plus sécurisés : (1) une solution de détection et de réponse des terminaux pour surveiller les activités anormales, y compris, mais sans s'y limiter, les mouvements latéraux.

Source: NY State DFS

Les 3 facteurs ayant le plus d'impact sur le coût des compromissions parmi 27 facteurs.

Source: Cost of Data Breach Report, 2023, Ponemon Institute et IBM Security.

05.
Exigences en matière d'assurance cybersécurité

Source: Federal Trade Comission https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

Les bonnes pratiques comprennent

- Cryptage des données sensibles
- Évaluation des vulnérabilités et gestion des correctifs
- EDR
- Sauvegarde et plan de reprise d'activité après sinistre par programmation
- Stratégies d'authentification (authentification multifacteur) et d'autorisation (gestion des privilèges minimaux) strictes
- Antimalware comportemental
- Formation de sensibilisation à la sécurité
- Plan d'intervention en cas d'incident

Faites l'expérience de la cyberprotection holistique qui assure la résilience de votre entreprise

Acheter | Essayer maintenant