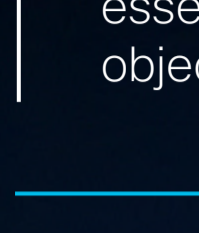


# Plus de visibilité pour mieux se protéger

Les protocoles de sécurité réactifs sont obsolètes. La proactivité est la clé pour prendre le contrôle de vos opérations de sécurité et protéger votre entreprise.



## La force du leadership en matière de sécurité



Les cyberattaques coûtent de plus en plus cher

**4,45 M\$**

C'est le coût moyen d'une attaque par ransomware, sans compter le prix de la rançon<sup>1</sup>

Des capacités de détection des menaces et de réponse efficaces sont essentielles pour assurer la continuité des opérations et atteindre les objectifs de croissance de l'entreprise.



Tout le monde est concerné

**83 %** des entreprises ont subi plus d'une violation de données<sup>1</sup>

Le volume, la fréquence et la complexité des attaques sont en hausse et les équipes du SOC sont de plus en plus sollicitées.



Les alertes sont de plus en plus nombreuses

**37 %** des professionnels de l'IT et de la sécurité disent que leur environnement est devenu plus difficile à protéger, car le volume et la complexité des alertes augmentent<sup>2</sup>

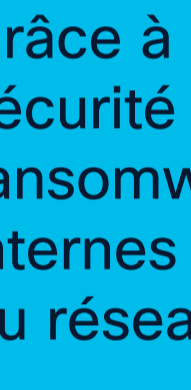
Le trop grand nombre de sources de détection et la complexité des enquêtes suscitent une lassitude vis-à-vis des alertes et entraînent une augmentation du taux de roulement des analystes.

Les outils de sécurité actuels ont du mal à détecter et analyser les menaces sophistiquées développées par des groupes de hackers comme BlackTech, Volt Typhoon ou Wizard Spyder.

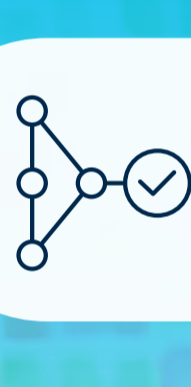


## Améliorez l'expérience du SOC pour renforcer la sécurité de votre entreprise.

Les responsables de la sécurité et leurs équipes veulent être plus efficaces, offrir de meilleures expériences et améliorer leur ROI.



**Plus d'efficacité** : détectez et contrez des menaces sophistiquées comme les ransomwares grâce à la corrélation des données téléométriques et en associant l'intuition humaine et l'IA.



**De meilleures expériences** : gagnez en visibilité, répondez plus rapidement et soulagez vos équipes d'analystes grâce à une vue unifiée et à davantage d'automatisation



**Un meilleur ROI** : exploitez pleinement vos ressources de sécurité grâce aux réponses automatisées et aux enquêtes techniques guidées, et améliorez la productivité du SOC.

- Technologie de détection et de réponse étendues (XDR)
- Sécurité endpoint
- Détection et réponse réseau (NDR)
- Sécurisation des e-mails
- Sécurité du cloud



## Cisco Breach Protection est à vos côtés pour :

- Détecter les menaces plus tôt** → **Minimiser votre exposition**
- Hiérarchiser les incidents selon l'impact potentiel** → **Minimiser les risques pour l'entreprise**
- Mener des enquêtes techniques rapidement** → **Comprendre pleinement les cyberattaques**
- Accélérer les délais de réponse** → **Neutraliser les attaques avant qu'elles vous impactent**



## Plus de visibilité pour mieux se protéger.

Nous analysons plusieurs milliards de demandes d'authentification, les attaques par phishing, les pages web frauduleuses et nous suivons tous les processus de connexion depuis les endpoints pour que rien n'échappe à votre équipe de sécurité. Elle peut neutraliser les menaces, comme les ransomwares, avant qu'elles impactent votre entreprise.

Grâce à notre solution optimisée par Cisco Security Cloud, les utilisateurs bénéficient d'une plateforme de visibilité complète pour bloquer les attaques sophistiquées plus efficacement.

Cisco Breach Protection renforce votre sécurité grâce à :

**500**  
spécialistes en recherche de menaces  
**TALOS**

**IA**  
Des algorithmes optimisés par l'IA

**550 Mds**  
d'événements liés à la sécurité observés chaque jour

Neutralisez les menaces plus efficacement que personne en associant l'intuition humaine à l'IA et à l'automatisation.

Détectez et contrez les menaces comme jamais.

[Découvrez Cisco Breach Protection](#)