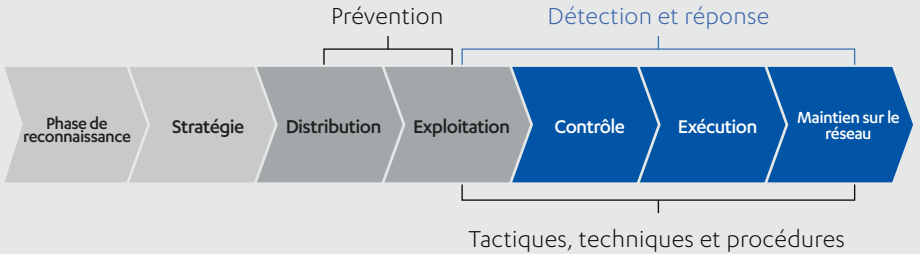
STOPPEZ LES ATTAQUES CIBLÉES

F-Secure Rapid Detection & Response

F-Secure

PROTÉGEZ VOTRE ENTREPRISE ET SES DONNÉES CONTRE LES ATTAQUES AVANCÉES

Contre les cyber menaces, la prévention est essentielle. Elle constitue la pierre angulaire de la cyber sécurité. Pourtant, seule, elle n'est pas suffisante. Pour protéger votre entreprise et ses données contre les tactiques, techniques et procédures (TTP) utilisées par les pirates informatiques lors d'attaques ciblées, vous devez aller plus loin.



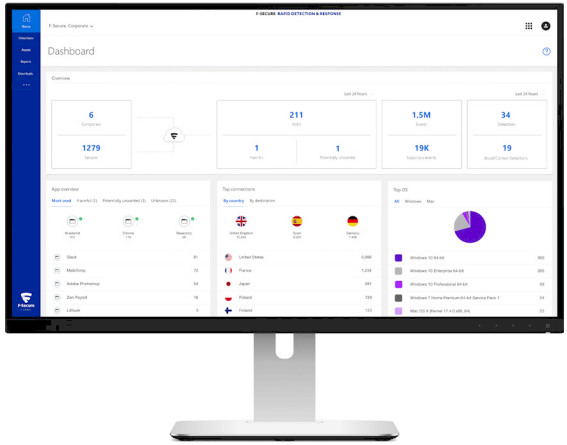
Pour satisfaire aux nouvelles réglementations (comme le RGPD), votre entreprise doit mettre en place des moyens de détection des intrusions. Elle doit être capable de réagir rapidement en cas de cyber attaque.

Créée par une équipe d'experts expérimentés en cyber menaces, la protection F-Secure Rapid Detection & Response vous protège contre ce type de menaces. Vos propres spécialistes informatiques peuvent réagir rapidement et efficacement aux cyber attaques avancées, avec le soutien des experts en cyber sécurité de F-Secure. Vous pouvez également laisser un fournisseur de services gérer les opérations de détection et de réponse pour votre entreprise. Vous pourrez alors compter sur des conseils d'experts en cas d'attaque et vous focaliser sur l'essentiel : votre activité.

APERÇU

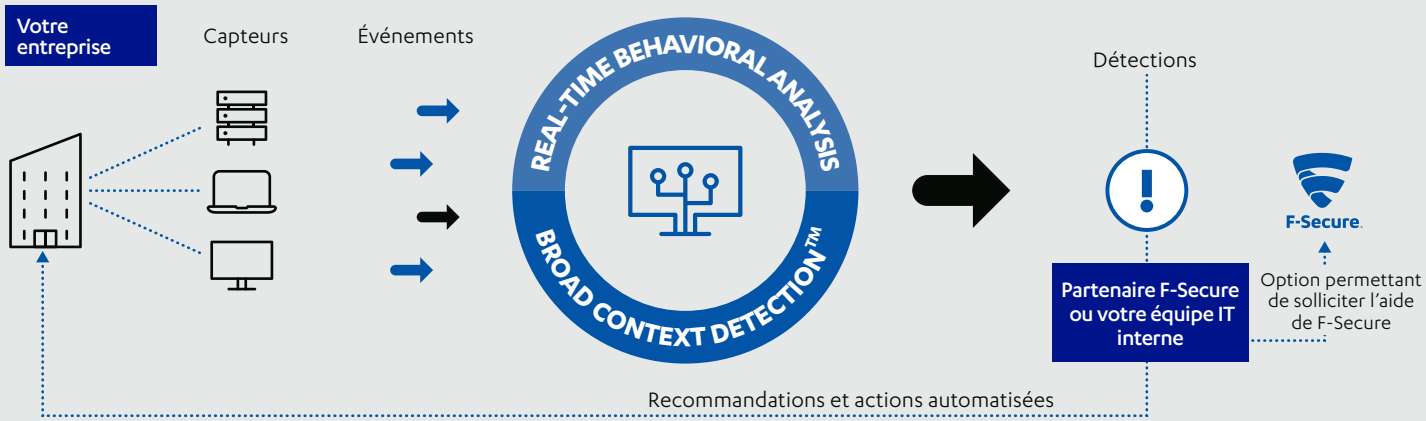
STOPPEZ LES ATTAQUES CIBLÉES AVEC L'AIDE DE NOS EXPERTS ET GRÂCE À L'AUTOMATISATION

Comment détecter une attaque sophistiquée ? En recourant aux technologies d'analyse les plus avancées et au machine learning pour protéger votre entreprise contre les cyber menaces et les intrusions informatiques.



Le service EDR (Endpoint Detection & Response) de F-Secure, leader du secteur, vous donne la visibilité contextuelle dont vous avez besoin pour détecter rapidement les attaques ciblées et intervenir efficacement. Nos processus automatisés vous permettent de neutraliser rapidement les éventuelles intrusions, avec l'aide de nos experts. Lorsqu'un vol de données se produit, il vous faut plus qu'une simple alerte. Afin de planifier la meilleure réponse possible, vous devez comprendre les spécificités de l'attaque. Grâce à l'association de notre technologie Broad Context Detection™, de fournisseurs de services certifiés et de l'automatisation intégrée, vous serez en mesure de mettre fin aux vols de données et d'apporter les mesures correctives qui s'imposent.

FONCTIONNEMENT



La technologie et l'expertise de pointe de F-Secure à votre service

1. Des capteurs de surveillance légers, déployés sur vos endpoints, surveillent les événements comportementaux générés par les utilisateurs. Ils les transmettent ensuite en temps réel à nos outils d'analyse des données comportementales et aux mécanismes de Broad Context Detection™ afin de distinguer les comportements malveillants des comportements normaux et habituels.
2. La contextualisation élargie et les informations descriptives de l'attaque permettent de confirmer facilement une détection. Cette confirmation est réalisée soit par le partenaire F-Secure, soit par votre propre équipe informatique qui a la possibilité de passer la main à F-Secure pour les cas les plus délicats.
3. Lorsqu'une détection est confirmée, notre solution fournit des conseils et recommandations, afin de vous aider à contenir la menace et à la neutraliser.

CHERCHER UNE AIGUILLE DANS UNE BOTTE DE FOIN – UN EXEMPLE CONCRET

Détecter les cyber menaces avancées en repérant les événements individuels mineurs générés par les hackers revient à trouver une aiguille dans une botte de foin.

Au sein d'une installation client de 325 nœuds, nos capteurs ont collecté environ 500 millions d'événements sur une période d'un mois. L'analyse des données brutes au sein de nos systèmes back-end a permis de les filtrer : nous avons ainsi obtenu 225 000 événements suspects.

Suite à une analyse plus poussée menée avec notre outil Broad Context Detection™, ce nombre a été réduit à seulement 24 évènements. Après une vérification plus poussée, 7 événements ont été confirmés comme étant des menaces réelles.

Vos équipes de sécurité informatiques peuvent se concentrer sur des détections précises, et donc réagir plus rapidement et plus efficacement en cas de cyber attaque avérée.

500 MILLIONS
d'évènements
collectés, chaque mois, par 325 capteurs

225 000
événements suspects
après analyse comportementale en temps réel des événements

24
détections
après contextualisation de ces évènements

7
Menaces réelles
après confirmation qu'il s'agit bien de menaces réelles

AVANTAGES

VISIBILITÉ

Obtenez une visibilité immédiate sur votre environnement informatique et sur l'état de protection de vos systèmes

- Meilleure visibilité sur votre niveau de sécurité grâce à l'inventaire des applications et des endpoints.
- Identification des activités suspectes via la collecte et la corrélation des événements comportementaux, pour détecter plus que les simples malware standards.
- Alertes, avec contextualisation et informations sur la criticité des ressources, pour des interventions plus efficaces.

DÉTECTION

Protégez vos données commerciales et sensibles en détectant rapidement les intrus

- Détectez et stoppez rapidement les cyber attaques ciblées, afin de minimiser leur impact sur votre activité et sur votre image.
- Configurez la solution en quelques heures, pour faire face immédiatement à d'éventuelles intrusions.
- Avec cette solution, vous répondrez aux exigences réglementaires PCI, HIPAA et RGPD, qui exigent que les violations de données soient signalées dans les 72 heures.

RÉPONSE

Réagissez rapidement en cas d'intrusion, avec l'aide de nos experts et grâce à l'automatisation

- L'automatisation et les renseignements sur les menaces intégrés aident votre équipe à se focaliser uniquement sur les attaques réelles.
- Les alertes comprennent des conseils de réponse avec, en option, la possibilité d'automatiser la réponse 24h/24.
- Surmontez vos lacunes (compétences, ressources) et répondez aux attaques grâce à un fournisseur de service certifié par F-Secure.

Capteurs

Des outils de surveillance légers et discrets, conçus pour fonctionner avec n'importe quelle solution EPP.

- Capteurs déployés sur tous les postes de travail pertinents de votre entreprise.
- Infrastructure de gestion intégrée et client unique avec les solutions de protection des postes de travail F-Secure.
- Ces capteurs recueillent des données comportementales à partir des périphériques, sans compromettre la vie privée des utilisateurs

Broad Context Detection™

La technologie de détection propriétaire de F-Secure permet de mieux évaluer l'ampleur d'une attaque ciblée.

- Analyse en temps réel du comportement, de la réputation et du Big Data grâce au machine learning.
- Contextualisation automatique des détections, visualisables chronologiquement.
- Affichage des niveaux de risque, de la criticité de l'hôte affecté et des cyber menaces les plus courantes.

Visibilité des applications

Visibilité inédite sur votre environnement informatique et votre statut de sécurité.

- Identification des applications indésirables et des destinations étrangères des services cloud.
- Utilisation des données de réputation de F-Secure pour identifier les applications potentiellement dangereuses.
- Restriction des applications et services cloud potentiellement nuisibles, avant même que des violations de données ne se produisent.

Réponse guidée

Pour faire face aux cyber attaques les plus avancées, avec vos ressources existantes.

- Fonctionnalité d'actions à distance pour mieux stopper les attaques.
- Des prestataires de services certifiés pour vous guider et vous assister dans vos actions.
- Pour les situations délicates, « Elevate to F-Secure » : bénéficiez des analyses et des recommandations des experts de F-Secure.

Réponse automatisée

Pour réduire l'impact des attaques ciblées en contenant les cyber menaces, 24h/24.

- Mesures de réponse automatisées en fonction de la criticité et des niveaux de risque, basée sur un calendrier prédéfini.
- Les informations fournies sur la criticité et les niveaux de risque améliorent la priorisation des mesures de réponse.
- Les cyber attaques sont rapidement contenues, 24h/24, même si votre équipe n'est disponible que durant les heures de bureau.

VISIONNER LA VIDÉO SUR

f-secure.com/RDR

F-Secure dispose d'une visibilité inégalée sur les cyber attaques réelles. Nous comblons le fossé entre détection et réponse aux cyber attaques. Pour ce faire, nous misons sur l'expertise inégalée de centaines consultants techniques – les meilleurs du secteur –, sur les millions d'appareils exécutant nos logiciels primés et sur des innovations permanentes en matière d'intelligence artificielle. Banques, compagnies aériennes et multinationales nous font confiance pour combattre les cyber menaces les plus redoutables. Avec notre réseau de partenaires de distribution et nos plus de 200 fournisseurs de services, nous veillons à ce que chacun puisse compter sur une cyber sécurité de haut-niveau.

Fondée en 1988, F-Secure est une entreprise du NASDAQ OMX Helsinki Ltd.

f-secure.com/fr_FR/ | twitter.com/fsecurefrance | linkedin.com/fsecure

F-Secure