Brochure

Stoppez les **attaques ciblées**

WithSecure™ Elements Endpoint Detection and Response

Protégez votre entreprise et vos données contre les attaques avancées

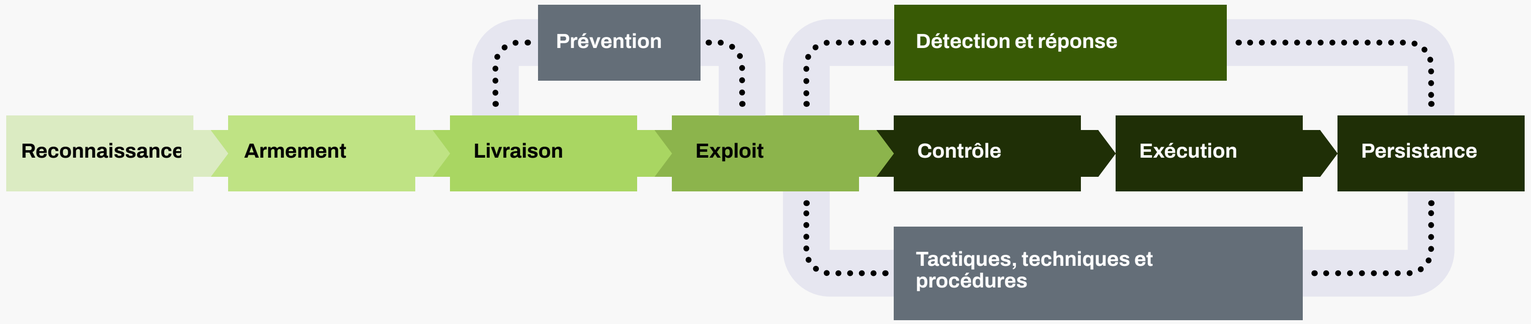
Face aux cybermenaces, la prévention est essentielle. Elle constitue la pierre angulaire de la cybersécurité. Pourtant, seule, elle n'est pas suffisante. Pour protéger votre entreprise et vos données contre les attaques ciblées, vous devez aller plus loin.

Pour lutter contre les cybermenaces en constante évolution et pour satisfaire aux réglementations (comme le RGPD), votre entreprise doit mettre en place des moyens de détection des intrusions.

WithSecure™ Elements Endpoint Detection and Response vous permet de réagir rapidement en cas de cyberattaque avancée. Cette solution a été conçue par notre équipe expérimentée de Threat Hunters.

Grâce au soutien des experts mondiaux de WithSecure, vos spécialistes IT peuvent assurer une réponse rapide et efficace en cas de cyberincident.

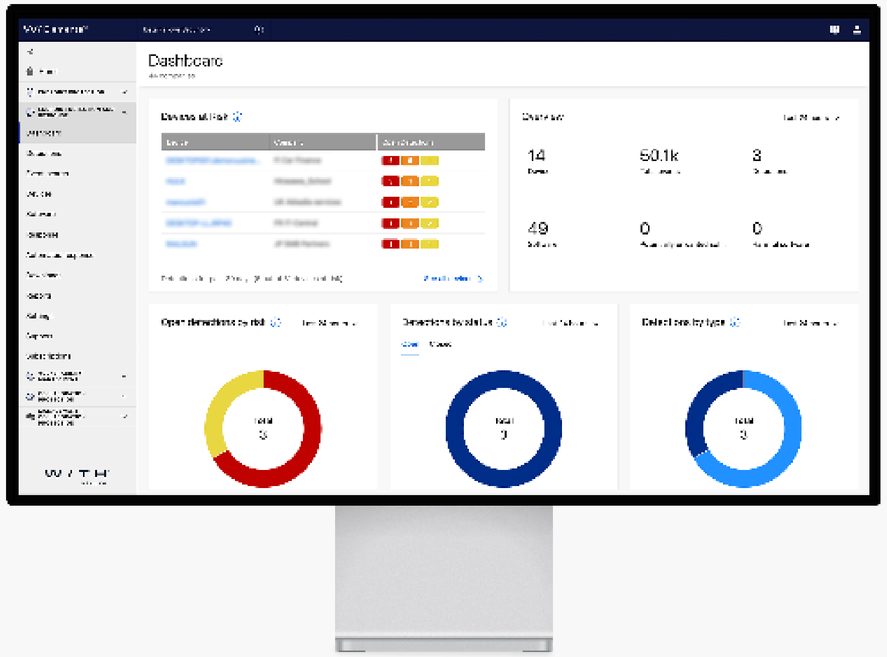
Vous pouvez aussi faire appel à un prestataire de services managés pour gérer ces opérations de détection et de réponse, afin de rester focalisé sur l'essentiel : votre activité.



Présentation

Stoppez les attaques ciblées avec l'aide de nos experts

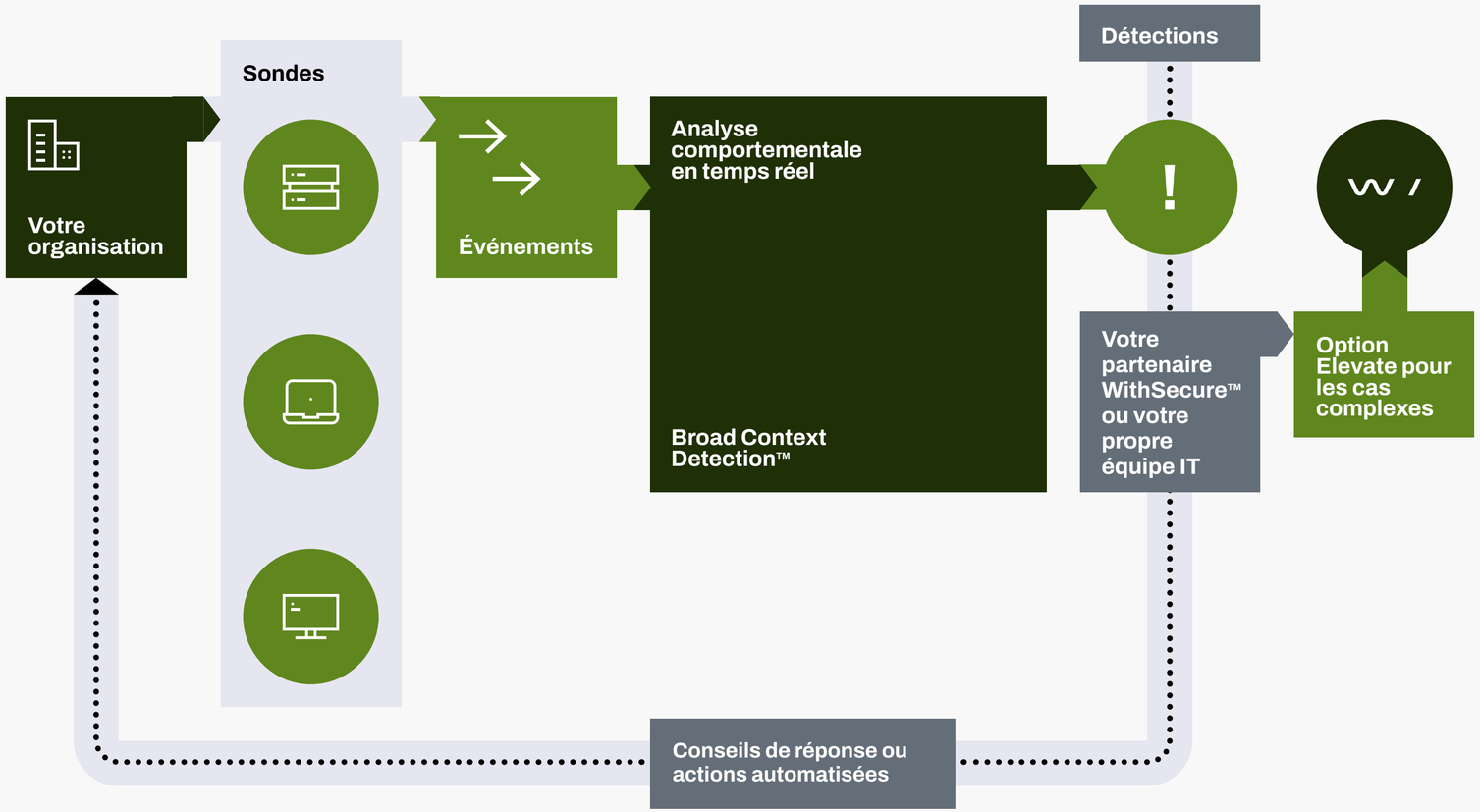
Pour détecter les attaques sophistiquées, vous devez mobiliser les technologies les plus avancées en matière d'analyse et de machine learning.



Le service EDR (Endpoint Detection & Response) de WithSecure, 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 chaque attaque. Grâce à notre outil Broad Context Detection™, à l'automatisation intégrée et à l'expertise de spécialistes, vous serez en mesure de stopper les cyberincidents et d'apporter les mesures correctives qui s'imposent.

Fonctionnement



La technologie de pointe et les experts WithSecure, à votre service

1. Des sondes légères, déployées sur les endpoints, monitorent les événements comportementaux générés par les utilisateurs, et les transmettent en continu à l'analyse comportementale en temps réel et à notre Broad Context Detection™, pour distinguer les comportements-utilisateurs malveillants des comportements-utilisateurs normaux.
2. Des alertes contextualisées sont générées, avec des scores de risque, pour permettre à votre équipe - ou au partenaire WithSecure™ qui vous accompagne - de confirmer facilement les détections. Il est possible d'automatiser les réponses ou encore de transmettre directement les cas les plus complexes à WithSecure™.
3. Lorsqu'une détection est confirmée, notre solution fournit des conseils et recommandations, pour aider à contenir la menace et à la neutraliser.

Fonctionnement

Chercher une aiguille dans une botte de foin – Un exemple concret

Détecter les cybermenaces avancées en se basant sur les événements isolés déclenchés par les pirates informatiques 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 grâce à 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.

Avec WithSecure™, vos équipes de sécurité informatiques peuvent se concentrer sur des détections précises, et donc réagir plus rapidement et plus efficacement en cas de cyberattaque avérée.

500 millions
d'événements collectées chaque mois par 325 sondes

225 000
événements suspects après analyse comportementale en temps réel

24
détections après contextualisation élargie de ces évènements

7
menaces confirmées comme étant des 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 statut de sécurité grâce à l’inventaire des applications et des appareils.
- Identification des activités suspectes via la collecte et la corrélation des événements comportementaux, pour détecter plus que les simples malwares standards.
- Alertes, avec contextualisation et informations sur la criticité des actifs concernés, pour des interventions plus efficaces.

Détection

Protégez vos données commerciales et sensibles en détectant rapidement les intrusions

- Détectez et stoppez rapidement les cyberattaques 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 RPGD, qui exigent que les violations de données soient signalées dans les 72 heures.

Réponse

Assurez une réponse rapide aux attaques grâce à des mesures automatisées et à des recommandations d'experts

- L’automatisation et les renseignements sur les menaces intégrées aident votre équipe à se concentrer uniquement sur les attaques réelles.
- Les alertes comprennent des conseils d’intervention. Il est possible d’automatiser la réponse aux cyberattaques, pour des interventions 24h/24.
- Surmontez vos lacunes (compétences, ressources) et répondez aux attaques avec l'aide d'un prestataire certifié par WithSecure™

Fonctionnalités

Sondes

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

• Des capteurs déployés sur tous les ordinateurs et les serveurs de votre entreprise.
• Client unique et infrastructure de gestion intégrée avec les solutions de protection des endpoints WithSecure.
• Ces sondes recueillent des données comportementales à partir des appareils Windows, Mac et linux, sans compromettre la vie privée des utilisateurs.

Réponse guidée

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

- Interventions guidées pas à pas et actions à distance pour stopper les attaques.
- Des prestataires de services certifiés pour vous guider et vous assister dans vos actions.
- Et pour les cas les plus complexes, bénéficiez des analyses et des recommandations des experts WithSecure via la fonction « Elevate à WithSecure ».

Broad Context Detection™

La technologie de détection propriétaire de WithSecure™ permet d'évaluer plus facilement 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 cybermenaces les plus courantes.

Réponse automatisée

Pour réduire l'impact des attaques ciblées en contenant les cybermenaces, 24 heures sur 24.

- Mesures de réponse automatisées en fonction de la criticité et des niveaux de risque, et plan prédéfini.
- Les informations fournies sur la criticité et les niveaux de risque permettent la priorisation des mesures de réponse
- Les cyberattaques sont rapidement contenues, même si votre équipe n'est disponible que durant les heures de bureau.

Visibilité sur les applications

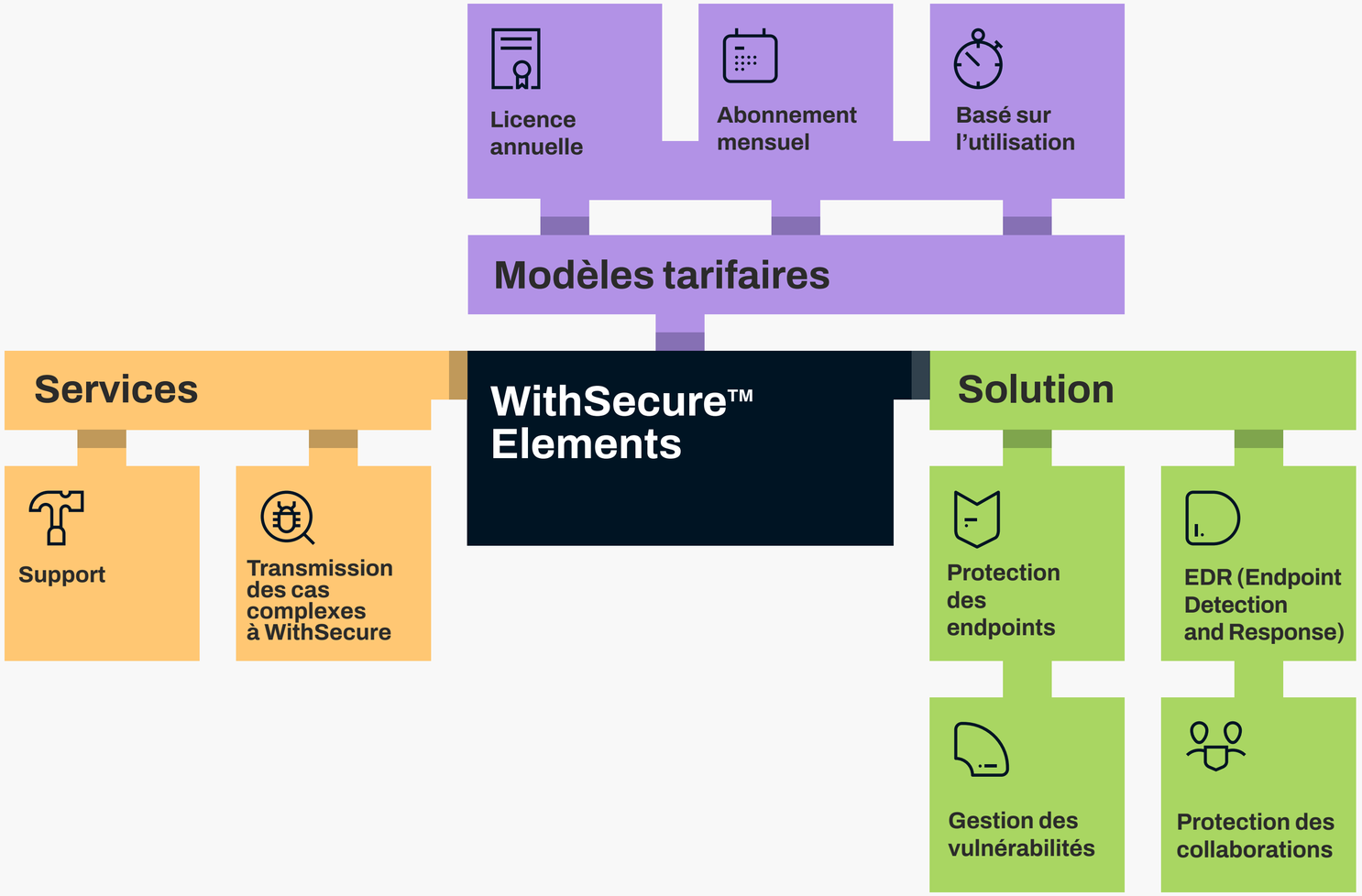
Visibilité inédite sur votre environnement informatique et votre statut de sécurité.

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

WithSecure™ Elements - Réduire les cyber-risques, gagner en efficacité

WithSecure™ Elements Endpoint Detection and Response est disponible en version standalone ou en tant que composant de la plateforme modulaire de cybersécurité WithSecure™ Elements.

Essayer dès maintenant



Qui sommes-nous ?

WithSecure™ est le partenaire de référence en matière de cybersécurité. Les fournisseurs de services informatiques, les MSSP et les entreprises - ainsi que de grandes institutions financières, des industriels et des milliers de fournisseurs en communications et technologies de pointe - nous font confiance. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir leur continuité opérationnelle. Notre protection basée sur l'IA sécurise les endpoints et protège les collaborations cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Nos consultants, quant à eux, proposent leurs conseils aux entreprises et challengers technologiques qui souhaitent renforcer la résilience. Depuis plus de 30 ans, nous élaborons une offre de pointe, pour nous développer au côté de nos partenaires, grâce à des modèles commerciaux flexibles.

WithSecure™ fait partie de F-Secure Corporation, fondée en 1988 et cotée au NASDAQ OMX Helsinki Ltd.

W / T H™
secure