Présentation de la solution

WithSecure™ Elements **Endpoint Detection and Response**

WithSecure™ Elements – Réduire les risques, simplifier les processes, gagner en efficacité

Sommaire

AVERTISSEMENT : Le présent document donne un aperçu détaillé des principaux composants de la solution de sécurité WithSecure™ Elements Endpoint Detection and Response. Certains détails ont été volontairement omis afin de prévenir les cyberattaques ciblées contre nos solutions.

WithSecure™ améliore constamment ses services. WithSecure™ se réserve le droit de modifier les caractéristiques ou les fonctionnalités de ses logiciels, conformément à ses pratiques en matière de cycle de vie des produits.

Dernière mise à jour : mai 2021

1. Résumé

Les cyberattaques ciblées sont souvent redoutables. Pour les entreprises, elles peuvent supposer un préjudice financier colossal, et ce, avant même que les pirates informatiques ne parviennent à exfiltrer des données. La seule étape de neutralisation d'une attaque peut prendre plus de deux mois et coûter près de deux millions de dollars.[1] Les attaques sans fichier ne sont généralement pas reconnues par les protections antivirus traditionnelles et les attaques ciblées peuvent passer inaperçues pendant des mois, voire des années.[2] Avec la solution WithSecure™ Elements Endpoint Detection and Response solution, vous pouvez obtenir une visibilité contextuelle sur votre sécurité, automatiser l'identification des cybermenaces et stopper les attaques avant qu'elles ne donnent lieu à des fuites d'informations sensibles, confidentielles ou protégées.

[1] Selon le rapport 2018 du Ponemon Institute sur le coût d'une violation de données, le nombre de jours nécessaires à l'identification d'une violation de données varie de 150 à 287 jours selon le secteur d'activité, et les activités de réponse à une violation de données coûtent, à elles seules, 1,76 million de dollars sur 69 jours en moyenne.

[2] Le rapport 2020 du Ponemon Institute sur le coût d'une violation de données indique que le temps moyen pour identifier et contenir une violation de données est de 280 jours.

Une cybersécurité résiliente et flexible, avec WithSecure™ Elements

Dans un monde où les entreprises doivent sans cesse se réinventer, la seule constante est le changement. WithSecure™ Elements propose une sécurité tout-en-un, capable de s'adapter en continu aux besoins des organisations et à l'évolution des cybermenaces. WithSecure™ Elements propose des modèles de licence flexibles et des technologies de sécurité à la carte, avec une gamme complète de composants : gestion des vulnérabilités, gestion des patchs, protection des endpoints, détection et réponse. La gestion de la sécurité se fait au moyen d'une console de gestion cloud centralisée et intégrée.

Via cette même console, les entreprises peuvent gérer la sécurité de leurs services de collaboration Microsoft 365. Elements est disponible sous forme de service auto-géré ou sous forme d'un service d'abonnement 100% managé, par l'intermédiaire de nos partenaires certifiés. Les clients peuvent facilement passer d'un service autogéré à un service entièrement managé : ainsi, les entreprises qui peinent à trouver des employés disposant des cybercompétences nécessaires peuvent rester protégées.

WithSecure™ Elements se compose de quatre solutions, toutes gérées via la même console, WithSecure™ Elements Security Center.

WithSecure™ Elements Endpoint Protection :

Cette solution cloud-native, alimentée par l'IA, peut être déployée en toute simplicité pour sécuriser tous vos endpoints et garder votre entreprise à l'abri des attaques. WithSecure™ Elements Endpoint Protection couvre les mobiles, les ordinateurs de bureau, les ordinateurs portables et les serveurs.

WithSecure™ Elements Endpoint Detection and Response :

Bénéficiez d'une visibilité totale sur les cybermenaces avancées avec notre solution EDR. Grâce à notre technologie unique Broad Context Detection, vous pouvez minimiser le bruit des alertes, et via la réponse automatisée, vous pouvez stopper efficacement les intrusions 24h/24. WithSecure™ Elements Endpoint Detection and Response protège les ordinateurs de bureau, les ordinateurs portables et les serveurs.

WithSecure™ Elements Vulnerability Management :

Identifiez et gérez les vulnérabilités critiques présentes sur votre réseau et sur vos actifs. En identifiant, en priorisant et en corrigeant les vulnérabilités, vous pouvez réduire votre surface d'attaque et minimiser les points d'entrée pour les pirates informatiques.

WithSecure™ Elements Collaboration Protection :

Cette solution complète les capacités natives de protection de la messagerie de Microsoft 365. Elle fournit une sécurité avancée visant à prévenir les attaques menées par le biais des e-mails et des liens URL. Grâce à l'intégration de cloud-to-cloud, cette solution est facile à déployer et à gérer.

WithSecure™ Elements Endpoint Protection, Endpoint Detection and Response et Vulnerability Management sont regroupés dans un unique paquet logiciel mis à jour automatiquement : avec cette solution, vous économisez du temps et de l'argent pour le déploiement et la gestion logicielle.

Avantages des solutions intégrées

La solution modulaire WithSecure™ Elements s'adapte aux besoins de votre entreprise. Cette cyberprotection unifiée propose un modèle de licence plus simple et réduit votre travail de gestion de la sécurité. Vous gagnez en efficacité, sans faire de compromis sur votre sécurité. Notre console cloud, WithSecure™ Elements Security Center, offre une visibilité accrue avec une gestion et des analyses centralisées, sur l'ensemble des endpoints et des services cloud. Elle est entièrement gérée par l'un de nos partenaires certifiés ou autogérée avec une assistance WithSecure™ à la demande pour les dossiers les plus complexes. Le Security Center offre une visibilité unique sur votre statut de sécurité en intégrant la protection des endpoints, l'EDR, la gestion des vulnérabilités et la protection de Microsoft 365.

Toutes les solutions actives au niveau des endpoints (Elements Endpoint Protection, Endpoint Detection and Response et Vulnerability Management) utilisent un seul agent logiciel, que vous n'avez à déployer qu'une seule fois. Les solutions complémentaires peuvent ensuite être activées ultérieurement sans avoir à déployer de dispositif supplémentaire. WithSecure™ Elements Collaboration Protection est une solution cloud qui ne nécessite pas d'installations sur les endpoints de votre entreprise.

Outre les avantages en termes de déploiement et de gestion, les solutions WithSecure™ Elements sont conçues pour fonctionner ensemble, de manière intégrée, pour maximiser votre sécurité. Dotée de capacités XDR, la solution WithSecure™ Elements fournit une sécurité holistique, en brisant les cloisonnements qui existent traditionnellement entre des solutions déconnectées.

WithSecure™ Elements

	Endpoint Protection Standard	Endpoint Protection Premium	Detection and Response	Vulnerability Management	Microsoft 365 Protection
Anti-malware avancé et gestion des patchs	✓	✓			
Anti-ransomware avec DataGuard et Contrôle des applications		✓			
Protection avancée contre les menaces			✓		
Gestion et priorisation des vulnérabilités				✓	
Sécurisation avancée de la messagerie et des collaborations pour Microsoft 365					✓

Note : les fonctionnalités disponibles peuvent varier selon la plateforme d'exploitation.

Présentation de WithSecure™ Elements Endpoint Detection and Response

WithSecure™ Elements Endpoint Detection and Response est une solution de pointe de détection et de réponse opérant au niveau contextuel. Elle aide les entreprises à obtenir une visibilité immédiate sur leur environnement informatique et sur leur statut de sécurité. Elle protège les données sensibles en détectant rapidement les attaques et en y répondant grâce à des conseils d'experts. Grâce à sa deep intelligence bidirectionnelle et à son haut niveau d'automatisation, cette solution offre une protection contre les menaces avancées et prévient les violations de données. Elle détecte les incidents qui affectent le réseau grâce à des clients légers installés sur des hôtes monitorés. Ces clients recueillent des données sur les événements comportementaux tels que les accès aux fichiers, les processus lancés, les connexions réseau et les éléments inscrits dans le registre ou les logs système. Ces événements sont ensuite analysés plus en détail. En plus des détections en temps réel, des détections supplémentaires sont réalisées à partir des données historiques. Ces technologies de pointe ne sont qu'une partie de l'équation : les experts qui exploitent ces technologies jouent, eux aussi, un rôle-clé. Chez WithSecure™, nous associons technologie et expertise humaine pour proposer une solution de détection et de réponse de pointe.

Nos Threat Hunters et nos chercheurs comptent parmi les meilleurs experts du secteur. Ils se consacrent à leur travail pour proposer le meilleur de la cybersécurité.

Une détection peut être transférée aux experts WithSecure™ pour une analyse plus approfondie de la menace par nos experts en cybersécurité.

Cette solution est aussi proposée sous forme de service EDR managé par nos partenaires, pour fournir un service tout-en-un de détection et de réponse aux intrusions alliant technologies, renseignements sur les menaces et services partenaires. Avec les services EDR managés, les entreprises soulagent leurs propres équipes informatiques, qui ne sont alertées que lorsque des menaces réelles sont détectées.

La prévention complique la vie des pirates informatiques

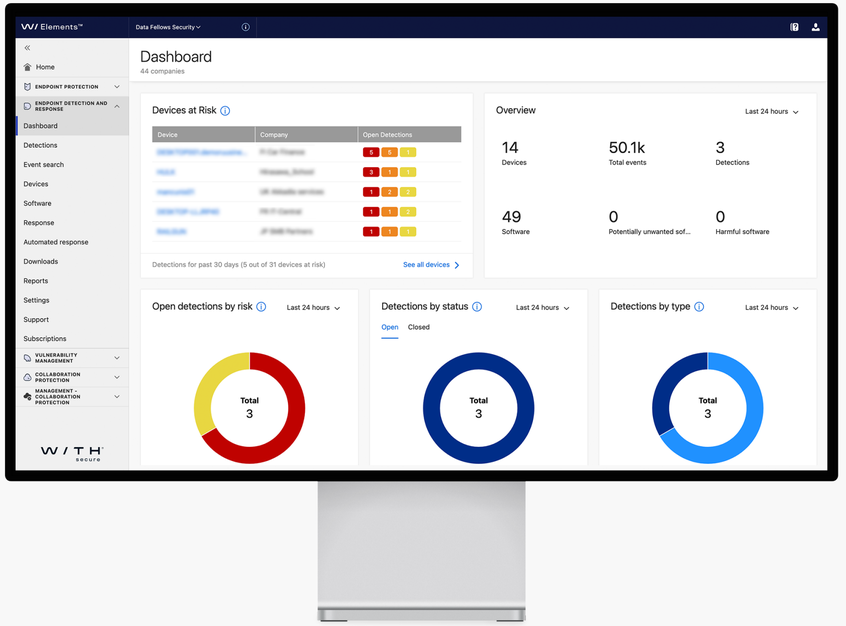
Les hackers les plus expérimentés disposent de compétences qui leur permettront, tôt ou tard, d'accéder à votre réseau. Pour autant, il n'est pas nécessaire de leur dérouler le tapis rouge. En misant sur la prévention, vous pourrez leur compliquer la tâche et il leur sera plus difficile d'atteindre leur objectif. Ils devront fournir des efforts plus importants et réaliser des investissements supplémentaires.... Tout cela aura un effet dissuasif.

WithSecure™ Elements Endpoint Detection and Response, solution post-intrusion pour la détection des cyberattaques avancées, ne vous dispense pas d'une solution efficace de protection des endpoints, dont le rôle est de bloquer les cybermenaces courantes comme les ransomwares.

2. Fonctionnalités-clés

Avec la solution WithSecure™ Elements Endpoint Detection, vous détectez les cybermenaces avancées et les attaques ciblées sans fichier avant qu'elles ne donnent lieu à des violations de données. Vous pouvez les analyser et y répondre rapidement grâce à nos technologies de pointe.

Voici certains des principaux atouts de cette solution, en termes de visibilité, de détection et de réponse :



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

- Améliorez la visibilité sur la sécurité de votre environnement informatique, grâce à l'inventaire des applications et des endpoints
- Repérez facilement les utilisations abusives en recueillant et corrélant les événements comportementaux, au-delà des simples malwares
- Répondez plus rapidement aux attaques ciblées, en vous basant sur les alertes contextualisées et la criticité de l'hôte

Protégez votre entreprise et ses données sensibles en détectant rapidement les intrusions informatiques

- Détectez et stoppez rapidement les cyberattaques ciblées, afin de minimiser leur impact sur votre activité et sur votre image
- Anticipez les intrusions et mettez en place des capacités avancées de détection et de réponse en seulement quelques jours
- Identifiez les menaces ou signes d'attaque affectant les endpoints et toujours actifs dans la mémoire lorsque la fonctionnalité EDR est activée
- Vous satisferez aux réglementations PCI, HIPAA, ainsi qu'au RGPD qui exige que les violations de données soient signalées dans les 72 heures

Répondez rapidement aux intrusions, grâce à l'automatisation et aux consignes de nos experts, ou exploitez les données de l'incident pour vos propres investigations SOC

- L'automatisation et les renseignements sur les menaces intégrés aident votre équipe à se focaliser uniquement sur les attaques réelles
- Recevez des conseils pour répondre aux alertes, avec la possibilité d'automatiser les mesures de réponse 24h/24 (les fonctions d'automatisation seront introduites dans le cadre d'une mise à jour)
- Surmontez vos lacunes (compétences, ressources) en externalisant le monitoring des menaces avancées auprès d'un prestataire certifié, soutenu par nos experts
- Pour les clients ou partenaires disposant de capacités de Threat Hunting, WithSecure™ Elements for Endpoint Detection and Response peut fournir l'intégralité des données brutes sur les incidents via le service supplémentaire de Recherche d'événements pour le Threat Hunting

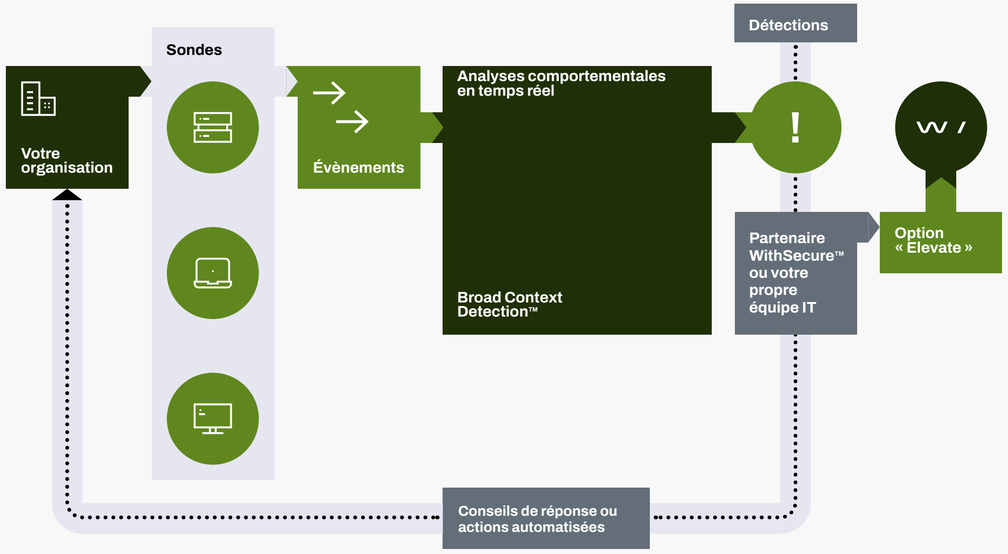
Une solution adaptée à vos compétences et à vos ressources en cybersécurité

Vous pouvez choisir la formule la plus adaptée à vos compétences et ressources :

1. **Service entièrement managé par les partenaires WithSecure™** : cette option est la meilleure pour les entreprises qui souhaitent être protégées contre les menaces ciblées avancées tout en appliquant une stratégie d'externalisation de leur cybersécurité.
2. **Service géré en interne avec l'assistance de WithSecure™ en cas d'incident :** cette option est parfaite pour les entreprises dont les compétences en matière de cybersécurité sont limitées. Les dossiers les plus complexes peuvent être transmis à WithSecure™ en utilisant la fonction intégrée WithSecure™ Elevate.
3. **Gestion interne :** cette option convient aux entreprises qui disposent d'un service informatique possédant un niveau élevé de compétences en cybersécurité. Le flux de réponse aux incidents de base couvre la détection des incidents via les Broad Context Detections et la réponse à ces menaces.
4. **Gestion interne avec capacités complètes de Threat Hunting :** cette option convient aux entreprises qui disposent de leur propre centre d'opérations de sécurité (SOC) et peuvent effectuer un Threat Hunting avancé dans le cadre de leurs investigations.

3. Présentation de la solution

La solution WithSecure™ Elements Endpoint Detection and Response repose sur le déploiement facile de clients au niveau des hôtes, avec un portail de gestion cloud et, en option, des services managés fournis par des partenaires certifiés.
Cette solution offre des fonctionnalités de détection des menaces avancées et des attaques ciblées, ainsi que de Broad Context Detections permettant de cerner précisément le risque et de mieux définir la réponse. Le déploiement prévoit l'installation de clients de monitoring et de réponse sur les endpoints de l'entreprise.



Le schéma ci-dessus décrit, dans les grandes lignes, le fonctionnement de la solution WithSecure™ Elements Endpoint Detection and Response :

1. **Des sondes de surveillance légères,** conçues pour être déployées sur vos appareils, monitorent les activités initiées par les pirates informatiques et transmettent en temps réel ces événements à notre cloud.
2. **L'analyse des données comportementales en temps réel** permet de repérer et de surveiller les processus et autres comportements ayant déclenché les événements.
3. **La technologie Broad Context Detection™** affine encore davantage les données en contextualisant les événements, en identifiant rapidement les attaques réelles, et en les priorisant selon le niveau de risque, la criticité de l'hôte et le profil des menaces en circulation.
4. **Lorsqu'une détection est confirmée**, notre solution guide vos équipes IT et sécurité, pour les aider à contenir la menace et à la neutraliser.

3.1 Elements Security Center, le portail de gestion

La solution Elements Endpoint Detection and Response facilite le déploiement, la gestion et le monitoring des menaces avancées sur vos endpoints, depuis une seule console web intuitive. Vous disposez d'une visibilité contextuelle immédiate sur votre environnement informatique et sur l'état de sécurité de votre réseau, que vos employés soient au bureau ou à l'extérieur (déplacements, télétravail...).

Ce portail de gestion a été conçu pour simplifier et accélérer la gestion de la sécurité pour les environnements complexes et multi-sites. Vous trouverez ci-dessous quelques exemples illustrant comment cette solution réduit considérablement le temps et les ressources nécessaires à la surveillance et à la gestion avancées des menaces.

- Cette solution est compatible avec n'importe quelle solution de protection des endpoints. Elle fonctionne aussi de manière intégrée avec les autres solutions WithSecure via une infrastructure de gestion commune et un client unique.
- Les entreprises deviennent capables de repérer et de gérer à la fois les malwares et les cybermenaces avancées.
- L'affichage des détections fournit une contextualisation élargie des attaques ciblées via une chronologie présentant tous les hôtes touchés, les événements connexes et les actions préconisées.
- En intégrant la gestion des endpoints et des outils système au sein d'un portail de sécurité unique, vous bénéficiez d'une rationalisation accrue, qui se traduit par d'importants gains de temps.
- Comme il s'agit d'un service cloud géré par WithSecure™, aucun serveur matériel ou logiciel n'est nécessaire. Pas d'installation de serveur, pas de maintenance : vous avez uniquement besoin d'un navigateur et d'une connexion internet.

Le portail Elements Security Center prend en charge les dernières versions des navigateurs suivants : Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome et Safari. Il est disponible en français et dans plusieurs langues (anglais, allemand, finnois, italien, japonais, polonais, portugais, espagnol (Amérique latine), suédois, etc.).

La version managée par les partenaires comprend des fonctionnalités spécialement conçues pour aider les prestataires de services : rapports destinés aux clients finaux, tableau de bord offrant une vue d'ensemble sur toutes les sociétés managées, et tableau de bord spécifique à chacune de ces organisations.

3.2 Clients endpoints

Les clients endpoints sont des outils de monitoring légers et discrets conçus pour détecter les anomalies, notamment les événements inédits et encore non-répertoriés, ou bien les séquences d'événements résultant très probablement d'activités malveillantes. Ces clients sont déployés sur tous les ordinateurs Windows et MacOS de l'entreprise requérant une surveillance afin de recueillir des données comportementales. Ils sont conçus pour fonctionner avec n'importe quelle solution de protection des endpoints et s'intègrent parfaitement aux solutions de WithSecure via une infrastructure de gestion cloud et un client unique.

Le tableau ci-dessous décrit les systèmes d'exploitation pris en charge et les fonctionnalités disponibles sur chaque système d'exploitation.

WithSecure™ Elements

	Postes de travail Windows	Serveurs Windows	Mac os	Linux
Système d'exploitation	7 / 8 / 10	2019 / 2016 / 2012 /2011 / 2008 R2	10.12 ou ult.	
Client unique avec WithSecure™	Oui	Oui	Oui	Oui
Événements comportementaux	Oui	Oui	Oui	Oui
Visibilité sur les applications	Oui	Oui	Non*	Non*
Isolation des hôtes à distance	Oui	Oui	Oui	Oui

* Cette fonctionnalité n'est pas encore disponible.
** Disponible avec WithSecure™ Business Suite par le biais d'actions manuelles.
Plus d'informations sur la configuration requise et le déploiement du client dans le guide utilisateur disponible à l'adresse suivante : https://www.withsecure.com/userguides/business/edr/latest/fr/deploiement-latest-fr

3.3 Visibilité sur les applications

En disposant d'une visibilité étendue sur votre environnement informatique et sur vos services cloud, vous réduisez votre degré d'exposition aux menaces avancées et aux fuites de données. Cette visibilité vous permet de répertorier toutes les applications actives s'exécutant sur les endpoints du réseau de votre entreprise, pour identifier facilement les applications indésirables, inconnues ou nuisibles.

Vous pouvez notamment identifier les applications potentiellement indésirables (Potentially Unwanted Applications - PUA) et les applications indésirables (Unwanted Applications - UA). Les « applications potentiellement indésirables » présentent des comportements que vous pouvez juger gênants ou inopportuns. Les « applications indésirables » présentent des comportements ayant un impact plus grave sur votre appareil ou vos données.

Les applications identifiées comme « potentiellement indésirables » (PUA) peuvent :

- affecter votre vie privée ou votre productivité : par exemple, en exposant des informations personnelles ou en effectuant des actions non-autorisées
- peser anormalement sur les performances de votre appareil : par exemple, en utilisant une quantité excessive de stockage ou de mémoire
- compromettre la sécurité de votre appareil ou de vos données : par exemple, en vous exposant à des contenus inattendus ou à des applications non souhaitées

L'impact sur votre appareil ou vos données peut varier, de léger à grave. Ces applications ne sont toutefois pas suffisamment nocives pour être classées comme malwares.

Collecte de données d'événements pour détecter et contenir les menaces

WithSecure™ Elements Endpoint Detection and Response collecte des données depuis de nombreux endpoints pour aider à détecter et à contenir les menaces sur votre environnement. Ces données sont recueillies de trois manières différentes :

1. **Broad Context Detection™.** Cette méthode d'identification automatisée des menaces est conçue pour repérer les menaces réelles à partir d'un grand volume de données d'événements comportementaux collectées à partir des endpoints de l'entreprise. Par ailleurs, avec la fonction intégrée WithSecure™ Elevate, vous pouvez demander conseil à nos experts en cybersécurité pour résoudre les cas les plus complexes
2. **Event Search**. Cette fonction intégrée vous permet d'afficher, de rechercher et de consulter les données d'événements collectées sur vos endpoints et liées à des Broad Context Detections.
3. **Event Search for Threat Hunting**. Cette fonction avancée permet d'explorer et d'interagir avec toutes les données d'événements brutes collectées à partir des endpoints. Grâce aux capacités de filtrage sophistiquées, les experts en cybersécurité de votre SOC peuvent mener un Threat Hunting proactif, pour détecter et stopper les menaces cachées les plus avancées. Event Search for Threat Hunting est un composant optionnel de WithSecure™ Elements Endpoint Detection and Response.

3.4 Analyse comportementale

Cette fonctionnalité centrale permet de déceler les menaces avancées au milieu des quantités massives de données comportementales. Il s'agit de repérer des événements (ou séquences d'événements) inédits, suspects, et très probablement malveillants.

WithSecure™ recourt à l'analyse comportementale en temps réel, à l'analyse de la réputation et l'analyse big data - via le machine learning - pour recueillir plusieurs événements suspects pouvant être corrélés entre eux. L'analyse comportementale s'appuie sur l'intelligence artificielle pour détecter les activités malveillantes dissimulées. Elle recherche de petits événements isolés, exécutés dans le cadre des tactiques, techniques et procédures utilisées par les pirates informatiques. L'analyse comportementale vise à identifier automatiquement le profil de l'hôte. Ce profil est ensuite utilisé pour l'évaluation du niveau de risque.

L'intelligence artificielle intègre des capacités de machine learning destinées à améliorer continuellement les détections et à réduire les faux positifs. L'analyse comportementale illustre bien la manière dont WithSecure™ allie sciences des données et expertise humaine. WithSecure™ a baptisé cette approche « Man and Machine ».

3.5 Broad Context Detection™

Notre approche exclusive Broad Context Detection™ est conçue pour réduire au maximum le nombre de détections indiquant un potentiel piratage, et ainsi éviter les faux positifs. Les Broad Context Detections™ signalent les intrusions possibles en alertant les administrateurs lorsque des indicateurs évoquent des tactiques, techniques et procédures (TTP) utilisées dans les attaques ciblées. Il peut s'agir par exemple des actions suspectes suivantes :

- Activité anormale de programmes standard
- Tentative d'exécution de processus à partir de fichiers exécutables non-standard
- Exécution inattendue de scripts
- Exécution inattendue d'outils système à partir de processus standard

À chaque détection est associée un niveau de risque. Broad Context Detection™ fournit des informations sur l'hôte affecté et sur les cybermenaces en circulation. Un seul événement n'indique pas nécessairement une attaque. Toutefois, plusieurs détections relevées dans un court laps de temps pourront donner lieu à une alerte plus sérieuse et déclencher une Broad Context Detection™, pour signaler un cyberincident éventuel. Grâce à cette approche, les équipes informatiques disposent d'une liste relativement réduite de détections confirmées, chacune étant associée à un niveau de priorité propre et à des préconisations adaptées. Ainsi, non seulement vos équipes savent sur quoi se concentrer en premier lieu, mais elles savent aussi comment réagir rapidement et de manière décisive. Pour plus d'informations sur Broad Context Detection™, consultez notre livre blanc sur la détection des attaques avancées.

3.6 Gestion des incidents

Notre solution dispose d'une fonction intégrée de gestion des incidents permettant de visualiser et de gérer les Broad Context Detections. Chaque nouvelle détection déclenche une alerte par e-mail, et cet e-mail renvoie au portail : l'utilisateur accède ainsi directement aux détails de la détection et peut prendre les mesures qui s'imposent. Chaque Broad Context Detection est associée à un score de risque. Ce score est automatiquement calculé, sur la base des niveaux de criticité et de confiance. Les Broad Context Detections non-critiques présentant un faible niveau de risque sont répertoriées à titre préventif, car certaines attaques à évolution lente peuvent parfois déboucher sur des incidents plus graves, au niveau de risque plus élevé. La gestion des incidents consiste à attribuer un statut à chaque Broad Context Detection : « in progress », « monitoring », « closed as confirmed », « closed as false positive », ou « closed as unconfirmed ». Le marquage d'un faux positif dans Broad Context Detection™ fermera automatiquement toutes les futures détections correspondant au même type de détections. Elles seront alors traitées comme « faux positifs automatiques ».

3.7 Consignes de réponse

Après une détection confirmée, les consignes intégrées à la solution vous aident à prendre les mesures nécessaires pour contenir la menace et y répondre. Plusieurs actions sont recommandées, comme l'information aux utilisateurs et l'isolement des hôtes.

Cette solution peut fournir des conseils pratiques pour répondre à un large éventail de menaces avancées. Grâce à ces recommandations, même les membres les moins qualifiés des équipes IT et sécurité peuvent plus facilement prendre les mesures qui s'imposent pour contenir les menaces et y répondre.

Voici plusieurs exemples d'activités déclenchant une détection

Cette liste n'est pas limitée aux seules attaques connues : de nouvelles données de détection sont sans cesse analysées et de nouvelles attaques sont identifiées par Broad Context Detection™ et par les Threat Hunters de WithSecure.

- **Attaque ciblée** visant un hôte
- **Mouvement latéral** impliquant un mouvement entre différents hôtes
- **Spoofing** de données dans le cadre d'une attaque
- **Persistance** (exemple : processus sur le même hôte)
- **Escalade des privilèges** (exemple : force brute des privilèges administrateurs)
- **Accès à des identifiants** donnant le contrôle sur un ordinateur/un réseau ciblé
- **Exfiltration** des informations présentes sur l'ordinateur/le réseau cible
- **Exécution anormale d'un processus** (exemple : paramètres suspects)
- **Accès anormal aux fichiers** (exemple : accès à plusieurs types de documents et à des fichiers système, sans accès racine)
- **Tentatives de falsification des données clients** (exemple : pour modifier les paramètres du client ou le désactiver)
- **Tentatives d'injection** vers un autre processus (exemple : en mode noyau ou vers une autre application)
- **Connexion à un hôte distant** depuis le réseau de commandes et de contrôle
- **Script PowerShell** chargé depuis un emplacement inhabituel
- **Modification - par PowerShell - d'un script PowerShell,** évoquant des manœuvres de persistance
- **Utilisation anormale de DLL** avec PowerShell à partir d'un processus ayant chargé le module
- **Connexion et exécution à distance** potentiellement utilisées pour un mouvement latéral

3.8 Fonction « Elevate to WithSecure™ »

WithSecure™ propose en option un service d'analyse des menaces pour les cas de détection nécessitant une analyse plus poussée et une assistance de la part des experts en cybersécurité de WithSecure.

« Elevate to WithSecure™ » est un service premium devant être souscrit à l'avance, pour un nombre prédéterminé de cas à analyser. Les demandes « Elevate to WithSecure » sont réalisées par le biais de la solution. Elles permettent aux analystes WithSecure™ d'accéder à l'ensemble des métadonnées collectées auprès des clients pour une détection spécifique.

Les analystes de WithSecure™ traitent la demande dans un délai de 2 heures et commencent alors à caractériser l'incident en recueillant des indices supplémentaires. Ils peuvent ainsi confirmer l'existence d'une menace et, éventuellement, mener une enquête.

- **Threat Validation** livre des informations complémentaires sur les détections Broad Context Detection™ découvertes au cours des 7 derniers jours. Cette fonctionnalité fournit un résumé et une description rédigés par un expert. Elle réunit toutes les données pouvant aider à déterminer si des mesures de réponse sont nécessaires.
- **Threat Investigation** fournit une enquête très détaillée sur une Broad Context Detection™, en s'appuyant sur toutes les données récentes et historiques. Cette option comprend également des conseils pratiques de réponse formulés par nos experts en cybersécurité, ainsi qu'un rapport complet sur le type d'attaque détecté.

« Elevate to WithSecure™ » repose sur l'analyse des preuves techniques telles que les méthodes, les technologies, les itinéraires réseau, l'origine du trafic et les chronologies. Toutefois, l'équipe WithSecure™ ne fournit que des recommandations via la solution. Les services professionnels complémentaires de réponse aux incidents doivent être souscrits séparément. Si le client suspecte un acte de cybercriminalité, nous lui recommandons de contacter les autorités compétentes et de fournir le rapport Threat Investigation sur la menace.

3.9 Actions automatisées

Des actions de réponse automatisées peuvent être mises en place pour réduire l'impact des cyberattaques ciblées. Les attaques sont alors contenues - même en dehors des heures de bureau - pour les cas où les niveaux de risque sont jugés suffisamment élevés. Cette fonctionnalité d'automatisation répond aux besoins des équipes de monitoring n'étant actives que durant les heures classiques de bureau. La première action de réponse automatisée peut ainsi intervenir sans délai, même pendant la nuit ou le week-end.

3.10 Actions de réponse avancées

Les actions de réponse avancées peuvent être utilisées pour réduire l'impact des cyberattaques ciblées et recueillir davantage d'informations. Ces actions de réponse peuvent être définies pour plusieurs endpoints à la fois, de manière à optimiser l'efficacité de la réponse à l'incident. Les endpoints déconnectés exécutent ces actions dès leur mise en ligne.

Les actions de réponse disponibles pour WithSecure™ Endpoint Detection and Response sont les suivantes :

- l'isolement du réseau pour le endpoint concerné (cette réponse peut être automatisée)
- la recherche des malwares et d'autres contenus malveillants sur le endpoint
- la récupération de différents types de données, logs, listes de processus et tâches
- la suppression et l'isolement des fichiers, dossiers, données de registre, processus et services.

En utilisant ces actions de réponse, un administrateur réseau peut efficacement stopper une violation de données avant qu'elle ne cause d'autres dommages à l'entreprise. Veuillez noter que les actions de réponse avancées ne sont pas disponibles lorsqu'elles sont utilisées avec les produits WithSecure™ Business Suite.

3.11 Event Search

Cette fonction intégrée vous permet d'afficher, de rechercher et d'explorer les données d'événements collectées depuis les endpoints concernés par des Broad Context Detections. Event Search permet de filtrer et de rechercher des événements en fonction de l'heure, du endpoint ou du réseau concerné.

3.12 Event Search for Threat Hunting

Cette fonction avancée permet d'explorer et de manipuler toutes les données brutes d'événements collectées à partir des endpoints. Grâce au filtrage sophistiqué proposé, les experts en cybersécurité du SOC peuvent effectuer des recherches proactives, pour détecter et stopper les menaces cachées les plus sophistiquées. Cette fonctionnalité inclut un panel beaucoup plus large d'événements (en plus de ceux liés aux Broad Context Detections) et la quantité de données est également beaucoup plus importante. De ce fait, cette fonctionnalité est proposée en composant optionnel pour WithSecure™ Elements Endpoint Detection and Response.

4. Sécurité des données

4.1 Protection des données et confidentialité

Les données d'événements comportementaux collectées à partir des endpoints sont stockées sur le territoire de l'Union européenne (en Irlande) sur une année roulante, durant toute la période de la relation client. Ces données sont supprimées dans les deux mois suivant la fin du contrat.

Cette solution n'a pas vocation à surveiller les activités non-liées à la sécurité. Elle ne réalise pas de profilage des activités, intérêts ou interactions des employés. La collecte de données n'est axée ni sur les employés en tant qu'individus, ni sur les documents commerciaux, ni sur les contenus des e-mails. Pour plus de détails, n'hésitez pas à consulter la politique de confidentialité propre à cette solution. WithSecure™ est basé en Finlande : nous respectons les législations strictes de la Finlande et de l'Union européenne en matière de sécurité et de protection de la vie privée. Nous sommes respectueux du cadre européen de protection de la vie privée et nous comprenons les attentes de nos clients en la matière.

WithSecure™ opère conformément à la transposition finlandaise de la directive européenne sur la protection des données. La solution WithSecure™ Elements Endpoint Detection and Response a été conçue dans le respect du RGPD (Règlement Général sur la Protection des Données de l'Union européenne). Pour plus d'informations sur la conformité de WithSecure au RGPD, rendez-vous à l'adresse : https://www.withsecure.com/GDPR/.

4.2 Mesures de sécurité des données

En tant qu'entreprise de sécurité, nous prenons très au sérieux la sécurité de nos data centers et utilisons à cette fin plusieurs dizaines de mesures de sécurité, telles que :

- **La sécurité dès la conception** : nos systèmes sont conçus d'emblée pour être sécurisés. Nous intégrons le respect de la vie privée et la sécurité dans le développement de nos technologies et de nos systèmes, depuis les premières étapes de la conceptualisation jusqu'à l'exploitation.
- **Des contrôles d'accès rigoureux** : seul un petit groupe d'employés de WithSecure™ sujets à des contrôles approfondis a accès aux données de nos clients. Leurs droits et niveaux d'accès dépendent de leur poste. Le concept de privilège minimum est appliqué : les employés n'ont accès qu'aux informations dont ils ont besoin pour mener à bien leur mission.
- **Une sécurité opérationnelle renforcée** : la sécurité opérationnelle fait partie intégrante de notre quotidien. Elle couvre notamment la gestion des vulnérabilités, la prévention des malwares et la gestion des incidents, pour tous les événements susceptibles d'affecter la confidentialité, l'intégrité ou la disponibilité des systèmes ou des données.

4.3 Data centers

Notre solution Endpoint Detection and Response utilise les data centers d'Amazon Web Services (AWS) afin de maintenir une disponibilité optimale et la meilleure résistance possible aux éventuelles pannes. Ces data centers proposent également les meilleurs temps de réponse et la meilleure évolutivité. AWS indique que chacun de ses data centers est conforme aux directives de niveau 3+.

Pour plus d'informations sur les data centers AWS, rendez-vous sur le site : https://aws.amazon.com/compliance/. Les données d'événements comportementaux collectées à partir des endpoints sont stockées sur AWS en Europe (Irlande). La conservation des données sur un an est comprise dans l'abonnement Elements Endpoint Detection and Response. Nous n'appliquons aucun frais supplémentaires de stockage des données en fonction de la quantité de données collectées.

Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnements 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. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

WITH secure