Présentation de la solution

WithSecure™ Elements Endpoint Protection

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

Sommaire

Janvier 2023

AVERTISSEMENT : Le présent document donne un aperçu détaillé des principaux composants de la solution de sécurité WithSecure™ Elements Endpoint Protection. 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.

Résumé

WithSecure™ Elements Endpoint Protection offre aux entreprises tout ce dont elles ont besoin pour la protection des endpoints. Cette solution protège les postes de travail, ordinateurs portables, mobiles et serveurs contre les cybermenaces – comme les attaques par ransomware – et assure une prévention proactive contre les violations de données. Elle prend également en charge la gestion des patchs pour lutter efficacement contre l'exploitation des vulnérabilités logicielles. Elements Endpoint Protection surpasse la concurrence et obtient continuellement les meilleures notes aux évaluations du secteur.

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 interface, les entreprises peuvent gérer la sécurité de leurs services de collaboration Microsoft 365. Cette solution 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 auto-géré 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. Cette solution a été récompensée à de nombreuses reprises par l'AV-TEST Best Protection.

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 cibler les incidents. 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 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. L'intégration de cloud-to-cloud rend cette solution 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 Elements, 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. Vous gagnez en efficacité, sans faire de compromis sur votre sécurité. La 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 bien auto-gérée 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 non-souscrites peuvent donc être activées ultérieurement sans avoir à déployer de dispositif supplémentaire. WithSecure™ Elements Collaboration Protection est une solution cloud qui ne nécessite pas d'installation 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, WithSecure™ Elements fournit une sécurité holistique et brise les cloisonnements qui existent traditionnellement entre des solutions déconnectées.

WithSecure™ Elements Endpoint Protection répond aux besoins des entreprises qui recherchent :

- Une couverture des endpoints de niveau supérieur et des services plus complets que ceux proposés par les solutions concurrentes, avec un coût total de possession (TCP) beaucoup plus attractif.
- Un excellent niveau de protection nécessitant un minimum de ressources, avec la possibilité d'externaliser complètement la gestion de la solution auprès d'un prestataire de services certifié.
- Un moyen simple et modulable d'assurer la protection de plusieurs sites géographiquement dispersés depuis un emplacement centralisé.
- Une solution permettant d'investir moins de temps et de ressources dans la maintenance des environnements de serveurs locaux.

Elements Endpoint Protection intègre la protection des endpoints, avec plusieurs outils de sécurité à valeur ajoutée, pour fournir :

- Une protection plus étendue que celle offerte par la plupart des solutions de sécurisation des endpoints.
- Une gestion unifiée et rationalisée via le cloud, pour économiser du temps et de l'argent en matière de gestion et de maintenance, avec un coût total de possession minimisé.

Cette solution est conçue sous la forme d'un service cloud. Elle est proposée, soit en service auto-géré, soit en service managé par un fournisseur de services certifié avec possibilité d'intégration à des systèmes tiers.

Nous sommes en mesure de fournir une protection plus efficace et cohérente que celle de nos concurrents : nos résultats aux tests réalisés par des experts et analystes indépendants sont là pour le prouver, année après année.

WithSecure™ est le seul fournisseur à avoir reçu à sept reprises le prestigieux award AV-Test Best Protection. AV-Test effectue des tests de comparaison en continu, tout au long de l'année. Pour obtenir cet award, il est nécessaire d'afficher en continu d'excellents résultats aux tests de protection.

Pour répondre aux besoins les plus exigeants, notre solution s'appuie sur une approche multi-niveaux de la sécurité et exploite plusieurs technologies de pointe. Elle recourt à l'analyse heuristique et comportementale des menaces et exploite des renseignements sur les menaces en temps réel, fournis par le Security Cloud de WithSecure™.

Vous avez ainsi la certitude d'être à la pointe de la cybersécurité.

1. Description de la solution

Face aux cybermenaces comme les ransomwares, les entreprises sont en proie à des risques commerciaux colossaux. WithSecure™ Elements Endpoint Protection est conçu pour répondre aux besoins de sécurité des entreprises avec un minimum de frais de maintenance de gestion. Cette solution protège les environnements Windows et Mac, les appareils iOS et Android ainsi que plusieurs plateformes de serveurs. Grâce à la gestion intégrée des patchs, à la protection par couches et aux analyses comportementales avancées, Elements Endpoint Protection stoppe les cybermenaces de demain, dès aujourd'hui.

WithSecure™ Elements Endpoint Protection :

- **Assure la meilleure protection du secteur, avec une meilleure continuité opérationnelle et une récupération post-incident plus rapide.**
- **Réduit proactivement les risques commerciaux liés aux intrusions informatiques grâce à une gestion des patchs entièrement intégrée.**
- **Est cloud-native, pour gagner du temps dans le déploiement, la gestion et le contrôle de la sécurité.**

WithSecure™ Elements Endpoint Protection est également disponible en service 100% managé. Les fournisseurs de services certifiés WithSecure™ peuvent utiliser la version gérée par un partenaire ou SaaS de cette solution et tirer parti de fonctionnalités uniques : tableau de bord multi-sociétés, outils de reporting, outils de gestion des abonnements, etc. La version SaaS permet notamment aux fournisseurs de services d'utiliser des modèles commerciaux flexibles, comme la facturation basée sur l'utilisation pour tous les produits WithSecure™ Elements.

1.1 Formules proposées

La protection des ordinateurs et serveurs Windows et Mac proposée dans le cadre de Protection Service for Business est disponible en versions standard, premium ou advanced. La formule standard inclut un anti-malwares avancé, la gestion des patchs et de nombreuses autres fonctionnalités de sécurisation des endpoints. Les fonctionnalités premium et advanced intègrent une protection plus poussée contre les attaques par ransomware, ainsi que des fonctionnalités de contrôle des applications. Ces deux formules de protection des endpoints peuvent être complétées par les solutions Elements Endpoint Detection and Response et Elements Vulnerability Management. Les fonctionnalités de détection et de réponse améliorent la visibilité, la détection et la réponse automatisée face aux menaces avancées et aux intrusions informatiques. La gestion des vulnérabilités permet de repérer et de gérer les vulnérabilités critiques présentes sur les endpoints. WithSecure™ Elements Collaboration Protection peut être déployé à l'aide d'une intégration cloud-to-cloud, sans aucun middleware ou logiciel à installer sur les endpoints.

WithSecure™ Elements

	Endpoint Protection standard	Endpoint Protection premium	Detection and Response	Vulnerability Management	Microsoft 365 Protection
Anti-malwares 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					✓

Les différents modules de protection peuvent être activés sans avoir à réinstaller le logiciel client.
Plus d'informations sur WithSecure™ Elements.

Software Updater
Mise à jour automatique pour les applications Microsoft et plus de 2500 logiciels tiers.

DeepGuard
Moteur anti-malware intelligent et heuristique offrant une capacité de détection 0-day. Lire à ce sujet le livre blanc WithSecure DeepGuard.

Contrôle des contenus web
Sécurité et productivité améliorées grâce à un accès contrôlé aux sites web. Blocage de l'accès à certains sites en fonction de leur catégorie et application de votre politique d'entreprise.

Contrôle des connexions
Sécurité supplémentaire pour les transactions sensibles comme les opérations bancaires en ligne.

Protection en temps réel
WithSecure™ Security Cloud protège votre entreprise contre les nouveaux malwares. Cet outil exploite des données sur les menaces recueillies par d'autres ordinateurs protégés afin d'assurer une réponse beaucoup plus efficace.

Anti-malware multi-moteurs
Protection inégalée grâce à un anti-malware multi-moteurs avancé.

Firewall
Règles supplémentaires et fonctionnalités de gestion intégrées au firewall Windows.

Protection de la navigation
Empêchez les employés d'accéder à des sites nuisibles contenant des liens ou des contenus malveillants.

Contrôle des périphériques
Le contrôle des périphériques empêche les cybermenaces de s'introduire sur votre système via des périphériques matériels tels que les clés USB, les lecteurs de CD-ROM et les caméras web. Cet outil permet également de prévenir les fuites de données, notamment via l'accès en lecture seule.

DataGuard
Protection supplémentaire contre les ransomware, pour éviter la destruction et l'altération des données.

Contrôle des applications
Blocage des applications et des scripts selon les règles créées par nos testeurs d'intrusion ou par l'administrateur. Pour plus de sécurité, le contrôle des applications peut également être paramétré pour bloquer le chargement de DLL ou d'autres fichiers.

XFENCE
Dispositif de protection unique permettant de protéger les ordinateurs Mac contre les malwares, les chevaux de Troie, les portes dérobées et les applications malveillantes en empêchant les applications d'accéder aux fichiers et aux ressources du système sans une autorisation explicite.

Chiffrement au niveau des endpoints
Monitorez et gérez le chiffrement des disques des ordinateurs Windows. Vous pouvez activer et désactiver le chiffrement Bitlocker et obtenir des clés de récupération directement depuis WithSecure™ Elements Security Center.

Outbreak Control
Outbreak Control permet de modifier automatiquement les profils EPP pour les restreindre en cas de détections EDR de gravité moyenne, élevée ou critique. Une fois l'incident résolu, le endpoint retrouve son profil d'origine.

1.2 Composants de la solution

Cette solution est constituée de quatre composants-clés, décrits en détail dans ce document :

1. **Elements Security Center**, le portail de gestion cloud
2. **Computer Protection**, client de sécurité clients dédié pour les postes de travail (Windows, Mac)
3. **Mobile Protection**, pour les appareils mobiles (iOS, Android)
4. **Server Protection**, compatible avec un large éventail de plateformes de serveurs (Windows, SharePoint, Exchange, Citrix, Linux)

1.3 Déploiement de la solution

Les clients de sécurisation des endpoints peuvent être déployés par e-mail, installation locale, script batch, système de gestion d'entreprise (SolarWinds, Kaseya, Datto) ou encore via un package MSI, par le biais d'outils d'installation à distance basés sur le domaine. De même, les clients Mac sont déployés via macOS Installer ou à l'aide d'outils Mobile Device Management. Ils peuvent être configurés, via des étapes de déploiement supplémentaires, dans des paquets signés personnalisés.

En environnement standard, tous les déploiements des clients de sécurité des endpoints peuvent être lancés depuis le portail, via un flux e-mails. La clé d'abonnement est automatiquement incluse dans le lien ou le programme d'installation : l'utilisateur final n'a qu'à cliquer pour lancer automatiquement le processus d'installation.

Pour les environnements plus complexes, il est possible de créer un package MSI pouvant être déployé soit à partir de vos propres outils d'installation à distance, soit à partir des nôtres. L'agent Windows peut être déployé par l'utilisation d'arguments dans un script batch.

Notre solution est capable de détecter et de désinstaller automatiquement une solution concurrente avant de poursuivre l'installation du logiciel WithSecure. La transition d'un fournisseur à l'autre est de ce fait beaucoup plus rapide et plus fluide.

Lorsqu'un nouvel ordinateur est ajouté à Elements Endpoint Protection, une configuration par défaut (profil) peut lui être automatiquement attribuée dans une hiérarchie Active Directory, en fonction de son emplacement. Vous pouvez ainsi rationaliser le processus de déploiement et réduire les risques de mauvaise configuration.

Mobile Protection est généralement déployé via une application tierce MDM (Mobile Device Management) dotée d'un abonnement prenant en charge l'utilisation de solutions MDM externes.

La gestion des patchs est entièrement intégrée aux clients Windows des serveurs et des postes de travail. Elle peut être contrôlée via le portail de gestion. Contrairement aux solutions traditionnelles de gestion des patchs, il s'agit d'une solution hébergée : aucune installation d'agent, de serveur ou de console de gestion supplémentaire n'est donc nécessaire.

WithSecure™ Elements Connector permet de minimiser l'utilisation de la bande passante lors du téléchargement des mises à jour des clients Computer Protection. Ce proxy met en cache les mises à jour de la base de données des signatures de malwares, les mises à jour du client Computer Protection et les mises à jour du logiciel de gestion des patchs. Par ailleurs, Connector peut être utilisé comme interface entre WithSecure™ Elements et vos systèmes SIEM.

Le logiciel du client de protection des endpoints met automatiquement à jour les bases de signatures de malwares ainsi que le logiciel du client lui-même : l'administrateur n'a donc plus à procéder manuellement aux mises à jour et mises à niveau.

Les partenaires WithSecure™ peuvent personnaliser notre agent ainsi que l'Elements Security Center avec leur logo et leur propre lien de support.

2. Elements Security Center

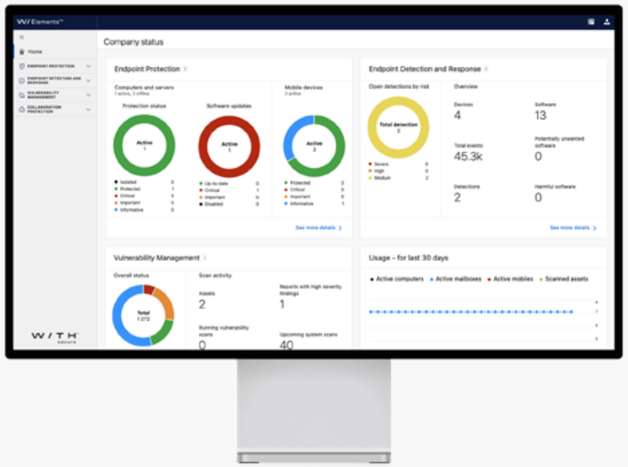
WithSecure™ Elements Endpoint Protection facilite le déploiement, la gestion et le monitoring de la sécurité de vos endpoints grâce à une console unique et intuitive. Vous disposez d'une visibilité optimale sur tous vos appareils.

Elements Security Center a été conçu pour simplifier et accélérer la gestion de la sécurité dans des environnements complexes, multi-appareils et multi-sites. Voici quelques exemples montrant comment cette solution peut réduire considérablement le temps et les ressources nécessaires à la maintenance et à la gestion de la sécurité :

- Les clients endpoint reçoivent automatiquement les mises à jour de sécurité (bases de données, signatures) de manière à minimiser le temps consacré à la maintenance.
- La gestion des outils et la sécurité des endpoints sont assurées depuis un seul et unique portail web. L'administration est de ce fait considérablement rationalisée.
- La gestion des patchs permet de déployer automatiquement les correctifs de sécurité manquants dès qu'ils sont disponibles.
- Il s'agit d'un service hébergé : vous n'avez besoin que d'un navigateur.
- Ce portail a été conçu par des spécialistes en expérience utilisateur, pour une meilleure accessibilité et une efficacité optimale.

La communication console-endpoints est assurée en temps réel, pour permettre aux administrateurs de gérer et de monitorer la sécurité de leur environnement informatique sans perturbations ni retards causés par les intervalles d'interrogation (polling intervals).

Les administrateurs peuvent ainsi configurer, déployer et valider des changements sans délai. Si un incident de sécurité doit être résolu immédiatement, vous êtes en mesure d'intervenir et de mener une action sans attendre.



Vous pouvez créer et personnaliser des politiques de sécurité (profils), puis les assigner aux hôtes de manière dynamique. Ces stratégies peuvent être imposées sur un appareil sans qu'elles puissent être ensuite modifiées par l'utilisateur final. Elles peuvent aussi être définies pour un groupe d'appareils puis appliquées automatiquement, par exemple via Active Directory.

Le portail de gestion vous donne un aperçu complet de l'état de sécurité de votre environnement. Vous visualisez les vulnérabilités logicielles potentielles, les mises à jour de sécurité manquantes ainsi que le statut des fonctions de sécurité (comme l'analyse en temps réel et le firewall). Les administrateurs informatiques peuvent consulter toutes les alertes depuis cette console centralisée.

Ce portail vous permet de connaître le nombre d'infections bloquées et d'identifier les appareils les plus attaqués. Vous pouvez définir des alertes automatiques par e-mail pour que certains types d'infection spécifiques attirent votre attention. S'il vous faut plus d'informations sur une alerte en particulier, vous pouvez consulter directement notre base de données de sécurité.

Le portail de gestion propose de nombreux rapports graphiques dans un format intuitif, pour vous permettre de comprendre la situation rapidement et avec facilité. Les informations relatives à la sécurité des appareils peuvent être exportées sous forme de fichiers CSV si nécessaire.

3. Computer Protection

Computer Protection constitue le socle de la sécurisation des environnements informatiques. Cette protection va bien au-delà des anti-malwares traditionnels. Avec WithSecure™ Elements Endpoint Protection, vous bénéficiez d'une protection puissante et respectueuse des performances, pour vos ordinateurs Windows, Mac et Linux.

3.1 Intégration tout-en-un des différentes protections des endpoints

Les solutions de pointe destinées à la sécurisation des endpoints recourent à une approche multi-niveaux. Elles intègrent des technologies telles que le filtrage du réseau, l'analyse des réseaux, l'analyse comportementale et le filtrage des URL, pour compléter les composants traditionnels d'analyse des fichiers. WithSecure™ Ultralight est dotée de cette approche multi-niveaux : si un niveau de protection échoue à stopper une menace, un autre niveau peut intervenir. À mesure que les cybermenaces évoluent, certains niveaux de protection peuvent être supprimés et de nouveaux niveaux peuvent être ajoutés, au niveau des endpoints et sur le cloud.

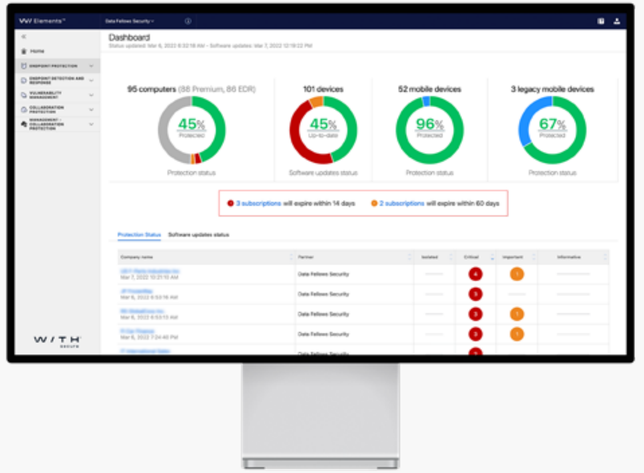
Ultralight intègre l'ensemble des technologies de protection des endpoints de WithSecure. Cet outil est composé de pilotes, de moteurs et de services système fournissant des mécanismes capables de protéger à la fois l'appareil et ses utilisateurs. Ultralight fournit des fonctionnalités anti-virus traditionnelles, telles que l'analyse des fichiers en temps réel et l'analyse du réseau. Il comprend par ailleurs des technologies de protection proactives destinées à neutraliser les exploits 0-day et à garder une longueur d'avance sur les nouvelles attaques. Le Security Cloud de WithSecure fournit aux composants d'Ultralight des informations en temps réel sur l'évolution des cybermenaces.

Pour plus d'informations sur les technologies de protection intégrées à Ultralight, consultez ce livre blanc technique.

3.2 Analyse heuristique et comportementale des menaces

L’analyse heuristique et comportementale des menaces est assurée par le module DeepGuard. Ce module est essentiel pour identifier et bloquer les malwares les plus sophistiqués. Il permet une protection immédiate et proactive. Cette technologie se focalise sur le comportement dynamique des objets malveillants plutôt que sur l’identification statique de menaces spécifiques et connues.

Ce changement d'approche permet d'identifier et de bloquer des malwares jusque-là inconnus. DeepGuard est en mesure de garantir votre protection face à des menaces inédites, jusqu'à ce que les chercheurs en sécurité soient en mesure de les analyser et de les détecter.



En communiquant avec le Security Cloud de WithSecure, DeepGuard peut disposer des toutes dernières données de réputation et de prévalence disponibles pour un objet donné rencontré précédemment, de manière à affiner ses évaluations de sécurité. En procédant ainsi, DeepGuard réduit les risques de faux positifs ou d'analyses redondantes susceptibles d'interférer avec l'expérience utilisateur.

L'analyse comportementale on-host permet, par ailleurs, d'intercepter les attaques cherchant à exploiter des vulnérabilités logicielles. DeepGuard est capable d'identifier et de bloquer les procédés caractéristiques des tentatives d'exploit, de manière à empêcher l'infection. Les utilisateurs sont protégés, même lorsque des programmes vulnérables sont présents sur l'ordinateur.

Pour plus d'informations sur l'analyse heuristique et comportementale des menaces menée par DeepGuard, consultez notre livre blanc technique.

3.3 Threat Intelligence en temps réel

Le client de sécurité s'appuie sur les renseignements sur des menaces en temps réel fournis par le Security Cloud de WithSecure : toutes les menaces nouvelles ou émergentes sont ainsi identifiées, analysées et bloquées en quelques minutes.

Comparé aux approches traditionnelles, l'analyse cloud des menaces présente certains avantages. WithSecure recueille des renseignements sur les menaces provenant de dizaines de millions de clients : nous sommes ainsi en mesure de dresser un tableau en temps réel des menaces au niveau mondial.

Si une analyse heuristique et comportementale identifie une attaque 0-day sur un endpoint situé à l'autre bout du monde, les données sont partagées avec tous les appareils protégés via le Security Cloud : cette attaque avancée est alors rendue inoffensive, seulement quelques minutes après la détection initiale.

Pour plus d'informations sur les fonctions et les avantages du Security Cloud de WithSecure, consultez notre livre blanc technique.

3.4 Protection macOS sur mesure

WithSecure™ Computer Protection for macOS comprend XFENCE, un dispositif de sécurité unique destiné aux Mac. XFENCE assure une protection contre les malwares, les chevaux de Troie, les portes dérobées et les logiciels indésirables.

Cet outil empêche les programmes d'accéder à vos fichiers et ressources système sans une autorisation explicite. Pour ce faire, il s'appuie sur une analyse avancée basée sur des règles. Cette analyse est complétée par les renseignements sur les menaces fournis par le Security Cloud : les faux positifs sont

ainsi minimisés, tout en réduisant le nombre de messages d'autorisation/interdiction affichés à l'utilisateur.

WithSecure™ Computer Protection for macOS fournit un firewall au niveau de la couche application, pour configurer et contrôler l'accès réseau des applications. Ce firewall peut être utilisé pour isoler les hôtes, pour limiter l'accès réseau aux seules applications de confiance ou encore pour blacklister/whitelister des applications sur la base de leur Bundle ID.

WithSecure™ Computer Protection for macOS est livré avec des outils d'administration qui facilitent le déploiement et la gestion des clients Mac.

3.5 Gestion intégrée des patchs

Les endpoints Windows bénéficient de la gestion automatisée des patchs. Celle-ci est entièrement intégrée aux clients. Aucune installation supplémentaire d'agent, de serveur ou de console de gestion n'est nécessaire.

Cette fonctionnalité recherche les mises à jour manquantes, crée un rapport de vulnérabilités puis télécharge et déploie automatiquement les patchs manquants. Si nécessaire, vous pouvez choisir d'installer certaines mises à jour manuellement.

Les mises à jour de Microsoft et de plus de 2500 applications tierces telles que Flash, Java ou OpenOffice sont prises en charge.

Vous pouvez ainsi sécuriser des programmes souvent utilisés comme vecteurs d'attaque en raison de leur popularité et du nombre important de vulnérabilités qu'ils présentent.

Pour le mode automatique, les administrateurs peuvent définir des exclusions détaillées en utilisant le nom des logiciels ou les ID de bulletins. Certaines mises à jour sont exclues par définition, comme les Service Packs. Les administrateurs peuvent également définir de manière flexible le jour et l'heure auxquels les installations doivent être effectuées. Ils peuvent aussi contrôler la manière dont les redémarrages sont forcés et définir le délai de grâce applicable avant de forcer un redémarrage après l'installation.

La gestion des patchs est un élément-clé de la sécurité. Il s'agit du premier niveau de protection qui intervient lorsqu'un contenu malveillant atteint un endpoint. Cette fonctionnalité peut prévenir jusqu'à 80 % des attaques en procédant simplement à l'installation des mises à jour de sécurité logicielles, dès que celle-ci sont disponibles.

3.6 Anti-malware multi-moteurs

Ce composant s'appuie sur une plateforme propriétaire multi-moteurs destinée à détecter et prévenir les malwares. Cette protection offre une sécurité supérieure à celle proposée par les technologies traditionnelles basées sur les signatures :

- Elle détecte un plus large éventail de caractéristiques et de tendances malveillantes, de manière à garantir des détections plus fiables et plus précises, même pour des variantes de malwares jusqu'alors inconnues.
- Grâce aux consultations en temps réel du Security Cloud de WithSecure, elle peut bloquer plus rapidement les menaces nouvelles et émergentes, avec un impact minimal sur les performances.
- L'émulation permet de détecter les malwares utilisant des techniques d'obfuscation : elle assure un niveau de sécurité supplémentaire avant l'exécution du fichier .

3.7 Profils par localisation

WithSecure™ Elements Endpoint Protection peut être configuré pour déclencher différentes configurations en fonction de l'emplacement du endpoint concerné. Par exemple, l'administrateur peut configurer différentes règles réseau pour qu'à la maison, la gestion des patchs et le firewall soient activés, mais qu'au bureau, ils soient désactivés.

3.8 Flexibilité avec l'automatisation des tâches

WithSecure™ Elements Endpoint Protection peut être configuré pour exécuter certaines tâches automatisées. Par exemple, les mises à jour de produits peuvent être configurées pour installer immédiatement les mises à jour critiques et autres mises à jour de sécurité, rechercher quotidiennement

les mises à jour de sécurité manquantes, installer les mises à jour à une heure spécifique, ou encore exécuter une analyse complète du système tous les jours de la semaine. En utilisant les tâches automatisées, vous pouvez configurer la protection des endpoints pour sécuriser votre entreprise tout en minimisant l'impact sur les performances.

3.9 Protection web extensive et proactive

Vous disposez d'une protection étendue et proactive du vecteur d'attaque le plus exploité : le web.

- L'accès aux sites malveillants et aux sites de phishing est bloqué de manière proactive avant même que l'utilisateur ne tente d'y accéder (via une recherche sur Google ou un lien web). Cette mesure anticipée réduit considérablement l'exposition globale aux contenus malveillants et donc aux attaques.
- Cette solution empêche l'exploitation de contenus actifs tels que Java et Flash, qui sont utilisés dans la grande majorité des attaques en ligne. Ces composants sont automatiquement bloqués sur les sites inconnus et suspects en fonction de leurs données de réputation. Il reste toutefois possible de définir des exceptions.
- Vous avez la possibilité de refuser l'accès à des sites non professionnels, comme les réseaux sociaux ou les sites pour adultes : vous maximisez ainsi la productivité des employés tout en évitant les sites malveillants.
- Après avoir franchi les premiers niveaux de protection web, les contenus HTTP sont soumis à une analyse complémentaire contre les malwares, avant que ces derniers ne puissent atteindre l'appareil.
- Les administrateurs informatiques peuvent également affecter un niveau de sécurité supplémentaire aux activités HTTPS critiques de l'entreprise (comme l'intranet ou les services cloud sensibles, par exemple les CRM). Lorsque ce niveau de sécurité est actif, toutes les connexions réseau non-fiables sont fermées, de manière à prévenir les attaques ou exfiltrations de données à partir de ces services.

Les caractéristiques de sécurité varient en fonction du système d'exploitation. À la page suivante, vous trouverez un aperçu des fonctionnalités disponibles pour Windows, macOS et Linux.

	Windows	macOS
Sécurité		
Anti-malware	**Oui**	**Oui**
DeepGuard	**Oui**	Non
DataGuard	**Oui**	**Oui***
Security cloud	**Oui**	**Oui**
Gestion des patchs	**Oui**	Non
Contrôle des applications	**Oui**	Non
Protection de la navigation	**Oui**	**Oui**

* Fonctionnalité assurée par XFENCE

	Windows	macOS
Sécurité		
Analyse du trafic web	**Oui**	Non
Web content control : Contrôle des contenus web	**Oui**	**Oui**
Filtrage par type de contenu	**Oui**	Non
Contrôle des connexions	**Oui**	**Oui**
Firewall	**Oui**	**Oui**
Vérification de l'intégrité	Non	Non
Chiffrement au niveau des endpoints	**Oui**	Non

4. Protection mobile

Le contrôle des appareils mobiles représente désormais un aspect fondamental de la cybersécurité. Avec Elements Mobile Protection, les administrateurs informatiques disposent d'un outil simple pour la sécurisation et le contrôle des appareils mobiles Android et iOS.

WithSecure™ Elements Mobile Protection comprend tout ce dont vous avez besoin pour offrir à vos appareils mobiles une protection optimale : VPN personnel, sécurité Wi-Fi, protection proactive des applications (Android) et protection du web. Le client mobile est également conçu pour compléter les solutions MDM tierces, avec un déploiement via ces solutions.

4.1 VPN pour mobiles

Le VPN mobile chiffre automatiquement le trafic entre votre appareil mobile et un point de terminaison WithSecure™, pour que vos employés puissent utiliser les réseaux mobiles et Wi-Fi publics en toute sécurité.

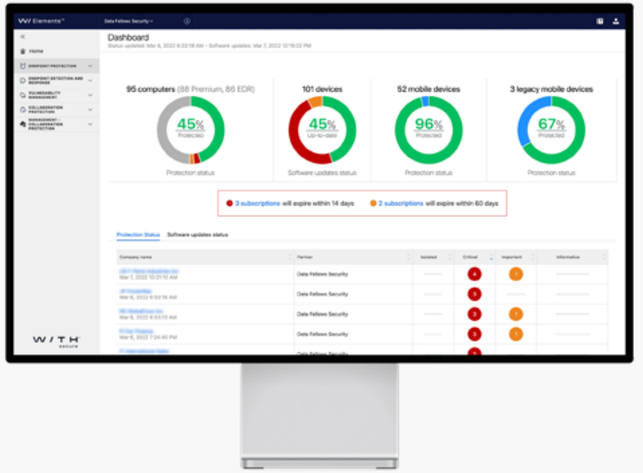
Ce VPN empêche l'interception des e-mails. Il protège les sessions de navigation et l'utilisation des services en ligne. Il fournit également un niveau de sécurité supplémentaire pour les connexions HTTPS. Enfin, il vous permet de changer votre emplacement virtuel, de masquer votre adresse IP et d'accéder aux services locaux lorsque vous êtes à l'étranger.

4.2 Security Cloud

Notre client de sécurité s'appuie sur les renseignements sur les menaces en temps réel fournis par le Security Cloud de WithSecure : toutes les menaces nouvelles ou émergentes peuvent ainsi être identifiées, analysées et bloquées en quelques minutes.

Un service d'analyse des menaces cloud offre de nombreux avantages comparé aux approches traditionnelles. Nous recueillons des renseignements sur les menaces à partir de dizaines de millions de nœuds clients, ce qui nous permet de dresser un tableau en temps réel des menaces au niveau mondial. Par exemple, lorsqu'un APK ou un fichier est téléchargé, celui-ci est scanné et sa réputation est vérifiée sur le Security Cloud. L'exécution des fichiers malveillants est bloquée et les applications ou fichiers inconnus sont uploadés pour une analyse approfondie. Les résultats de l'analyse profitent ensuite à tous les utilisateurs : les faux positifs sont minimisés et les nouvelles attaques sont rendues inoffensives en seulement quelques minutes.

Pour plus d'informations sur les fonctions et avantages du Security Cloud de WithSecure, consultez notre livre blanc technique.



4.3 Protection des applications

Lorsque la connexion VPN est active, les appareils mobiles sont automatiquement protégés contre les malwares et les contenus malveillants. Les points de terminaison WithSecure analysent le trafic au niveau du réseau en utilisant l'ensemble des analyses de sécurité disponibles. Ce mode opératoire nous permet d'offrir une sécurité supérieure à celles des solutions de sécurité mobiles traditionnelles :

- La sécurité n'est pas entravée par les performances limitées des appareils mobiles
- Les opérations de sécurité n'ont pas d'incidence sur les performances des appareils et la durée de vie des batteries
- L'analyse réseau empêche tout contact initial avec un contenu malveillant

Pour les appareils Android, la sécurité est encore renforcée par l'analyse locale, avec des contrôles de réputation en temps réel réalisés depuis le Security Cloud de WithSecure™, même lorsque le VPN n'est pas connecté.

4.4 Protection de la navigation

La protection de la navigation est un niveau de sécurité essentiel destiné à bloquer la consultation de sites malveillants. Cette mesure s'avère particulièrement efficace, car une intervention précoce réduit considérablement l'exposition globale aux contenus malveillants, et donc aux attaques.

La protection de la navigation empêche les utilisateurs de cliquer sur des sites de phishing en apparence légitimes, d'accéder à des sites malveillants par le biais d'un lien e-mail ou encore d'être infectés par des publicités tierces malveillantes diffusées sur des sites autrement fiables.

4.5 Navigation plus rapide et utilisation réduite des données

Cet outil est conçu pour avoir un impact minimal sur les performances mobiles et la durée de vie de la batterie. En utilisant la compression du trafic au niveau du VPN et en empêchant le suivi et la publicité en ligne grâce à l'anti-tracking, il parvient à augmenter la vitesse de navigation.

4.6 Déploiement tiers MDM

Ce client mobile est également conçu pour compléter les solutions MDM tierces telles que AirWatch, MobileIron, Intune et MaaS360, avec un déploiement via ces solutions.

En utilisant un composant de sécurité dédié en plus des capacités de base fournies par leur solution MDM, les administrateurs informatiques peuvent augmenter considérablement la protection des appareils mobiles contre les malwares, les vols de données et les tentatives de phishing.

5. Protection des serveurs

Les serveurs sont essentiels pour la communication, la collaboration et le stockage des données d'une entreprise. Elements Endpoint Protection assure la sécurité des serveurs Windows, Citrix et Linux tout en leur permettant de fonctionner au maximum de leurs capacités.

Voici un aperçu des principales fonctionnalités disponibles pour les différentes plateformes de serveurs :

	Windows	CITRIX	Linux
Sécurité de base			
Anti-malware	**Oui**	**Oui**	**Oui**
DeepGuard	**Oui**	**Oui**	Non
Security Cloud	**Oui**	**Oui**	**Oui**
Gestion des patchs	**Oui**	**Oui***	Non
Protection de la navigation	**Oui**	**Oui**	Non
Analyse du trafic web	**Oui**	**Oui**	Non
Firewall	**Oui**	Non	Non
Vérification de l'intégrité	Non	Non	**Oui**
Gestion à distance via le portail			
Gestion de la sécurité	**Oui**	**Oui**	**Oui**
Monitoring de la sécurité	**Oui**	**Oui**	**Oui**

5.1 Analyse heuristique et comportementale

L'analyse heuristique et comportementale des menaces effectuée par DeepGuard est essentielle pour identifier et bloquer les malwares les plus sophistiqués. DeepGuard fournit une protection immédiate et proactive contre les menaces nouvelles et émergentes, en se concentrant sur le comportement des applications malveillantes plutôt que sur l'identification statique de menaces spécifiques et connues. Ce changement d'approche permet d'identifier et de bloquer des malwares jusqu'alors inconnus en se basant uniquement sur le comportement. DeepGuard est en mesure de garantir votre protection face à ces menaces inédites, jusqu'à ce que les chercheurs en sécurité soient en mesure de les analyser et de les détecter. En communiquant avec le Security Cloud de WithSecure, DeepGuard peut consulter les dernières données de réputation et de prévalence disponibles pour tout objet précédemment rencontré, de manière à affiner ses évaluations de sécurité. En procédant ainsi, DeepGuard réduit les risques de faux positifs ou d'analyses redondantes susceptibles d'interférer avec l'expérience utilisateur.

L'analyse comportementale on-host permet également d'intercepter les attaques ciblant les vulnérabilités logicielles. DeepGuard est capable d'identifier et de bloquer les procédés caractéristiques des tentatives d'exploit, pour empêcher l'infection. Les utilisateurs sont ainsi protégés, même lorsque des programmes vulnérables sont présents sur l'ordinateur.

Pour plus d'informations sur l'analyse heuristique et comportementale des menaces menée par DeepGuard, consultez notre livre blanc technique.

5.2 Threat Intelligence en temps réel

Le client de sécurité s'appuie sur les renseignements sur les menaces en temps réel fournis par le Security Cloud de WithSecure : toutes les menaces nouvelles ou émergentes sont identifiées, analysées et prévenues en quelques minutes. Comparé aux approches traditionnelles, l'analyse cloud des menaces présente certains avantages. WithSecure™ recueille des renseignements sur les menaces provenant de dizaines de millions de clients : nous sommes ainsi en mesure de dresser un tableau en temps réel des menaces au niveau mondial. Si une analyse heuristique et comportementale identifie une attaque de type 0-day sur un endpoint situé à l'autre bout du monde, les données sont partagées avec tous les appareils protégés via le Security Cloud. Cette attaque avancée est alors rendue inoffensive, seulement quelques minutes après sa détection initiale.

Pour plus d'informations sur les fonctions et les avantages du Security Cloud de WithSecure, consultez notre livre blanc technique.

5.3 Gestion des patchs intégrée

Ce composant inclut une fonction de gestion automatisée des patchs entièrement intégrée aux clients pour serveurs Windows. Aucune installation supplémentaire d'agents, de serveurs ou de console de gestion n'est nécessaire. Cet outil recherche les mises à jour manquantes, crée un rapport de vulnérabilités puis télécharge et déploie automatiquement les patchs manquants. Si nécessaire, vous pouvez choisir d'installer certaines mises à jour manuellement.

Les mises à jour de Microsoft et de plus de 2500 applications tierces telles que Flash ou OpenOffice sont prises en charge. Vous pouvez ainsi sécuriser des programmes souvent utilisés comme vecteurs d'attaque en raison de leur popularité et du nombre important de vulnérabilités qu'ils présentent.

5.4 Anti-malware multi-moteurs

Ce composant de protection s'appuie sur une plateforme propriétaire multi-moteurs destinée à détecter et prévenir les malwares. Il offre une sécurité supérieure aux technologies traditionnelles basées sur les signatures :

- Il détecte un plus large éventail de caractéristiques et tendances malveillantes, de manière à garantir des détections plus fiables et plus précises, même pour des variantes de malwares jusqu'alors inconnues.
- Grâce aux consultations en temps réel du WithSecure™ Security Cloud, il peut réagir plus rapidement aux menaces nouvelles et émergentes, avec un impact minimal sur les performances.
- L'émulation permet de détecter les malwares utilisant des techniques d'obscurcissement, pour assurer ainsi un niveau de sécurité supplémentaire avant l'exécution du fichier.

5.5 Protection proactive du web

Les terminaux disposent d'une protection étendue et proactive contre le vecteur d'attaque le plus exploité : le web.

- L'accès aux sites malveillants et aux sites de phishing est bloqué de manière proactive avant même que l'utilisateur ne tente d'y accéder. Cette intervention anticipée réduit considérablement l'exposition globale aux contenus malveillants et donc aux attaques.
- Après avoir franchi les premiers niveaux de protection web, le contenu du trafic HTTP est soumis à une analyse complémentaire contre les malwares, avant que ces derniers ne puissent atteindre l'appareil.

5.6 Server Share Protection

Le partage de fichiers sur des serveurs locaux peut exposer à des risques d'attaques par ransomware, notamment si des appareils extérieurs accèdent à ces serveurs. Des fichiers critiques peuvent alors être chiffrés et devenir inutilisables. Avec Server Share Protection, vous pouvez continuer à utiliser les partages de fichiers Windows en toute sécurité. Ce composant assure une protection supplémentaire contre les ransomwares. Il identifie et annule immédiatement tout chiffrement ou toute destruction involontaire de fichiers.

5.7 Citrix et Terminal-serveurs

En plus d'assurer les mêmes fonctions de base que pour les serveurs Windows, le composant Citrix intègre une protection supplémentaire, via la gestion intégrée des patchs pour les applications publiées. Le client est certifié « Citrix Ready » et garantit ainsi un fonctionnement sans faille en environnement Citrix. De même, ce composant assure la protection des Terminal-serveurs Windows. Veuillez noter que les clients utilisant Server Protection en environnement desktop à distance ont également besoin d'une licence pour WithSecure™ Remote Desktop Protection.

5.8 Linux

La protection Linux assure des fonctionnalités de sécurité essentielles pour les clients Linux : analyses multi-moteurs pour les accès, analyses programmées ou manuelles, vérifications de l'intégrité... Cette protection est conçue pour détecter et prévenir les attaques Windows et Linux : elle est de ce fait particulièrement utile en environnements mixtes, où un dispositif Linux non protégé peut être facilement utilisé par les pirates informatiques comme vecteur d'attaque.

5.9 Anti-malware multi-moteurs

Une plateforme de sécurité propriétaire multi-moteurs est utilisée par les clients pour détecter et bloquer les logiciels malveillants. Cette plateforme offre une protection supérieure aux technologies traditionnelles basées sur les signatures, sans dépendre d'une seule technologie. Elle détecte un plus large éventail de caractéristiques et de patterns malveillants, ce qui permet des détections plus fiables et plus précises, même pour des variants encore jamais observés.

5.10 Contrôle de l'intégrité

Ce composant est doté d'un contrôle de l'intégrité intégré, capable de détecter et de bloquer les tentatives de falsification des kernels, fichiers systèmes et configurations. Il s'agit d'un dispositif de sécurité essentiel, qui protège le système contre des modifications non-autorisées, autrement susceptibles de passer inaperçues.

Le contrôle de l'intégrité peut être configuré pour envoyer des alertes à l'administrateur en cas de tentative de modification des fichiers surveillés. Il peut alors prendre sans délai les mesures nécessaires en cas d'incident. Si des changements fondamentaux sont nécessaires, par exemple en raison de mises à jour du système d'exploitation, de la sécurité et des logiciels, les administrateurs peuvent utiliser un outil d'installation protégé pour effectuer les mises à jour nécessaires, en toute simplicité.

6. Intégrations SIEM/RMM

WithSecure™ Elements Endpoint Protection s'intègre parfaitement aux SIEM, RMM et aux autres outils tiers d'audit, de gestion ou de reporting comme ceux proposés par Kaseya, Tableau, N-Able et Splunk.

Cette intégration permet aux entreprises de tirer le meilleur de leurs investissements existants et de bénéficier d'outils centralisés. Elles peuvent ainsi rationaliser la gestion de la sécurité et la réponse aux incidents.

L'intégration vous permet d'exploiter les capacités de votre SIEM/RMM pour bénéficier d'une automatisation plus poussée et de workflows et rapports personnalisés. Vous réduisez ainsi votre charge de travail.

Cette intégration peut être plus ou moins poussée : toute opération est accessible individuellement via les appels API. Par exemple, les administrateurs informatiques peuvent choisir de n'envoyer que les données pertinentes à un système de reporting, de journalisation ou d'audit, sans nécessairement procéder à l'intégration des capacités de gestion.

L'intégration est réalisée via une API REST baptisée WithSecure™ Management. Elle donne accès à toutes les opérations et données disponibles via le portail de gestion.

Pour plus d'informations sur cette API de gestion et sur l'intégration SIEM/RMM, voir la description de notre API de gestion sur connect.withsecure.com.

7. Services professionnels

Les packs d'assistance complémentaires de WithSecure incluent des services destinés à vous offrir une expérience de support plus flexible et plus complète. Cette assistance est disponible soit durant les horaires de bureau, soit en service 24h/24, 7j/7. Nos formules Advanced et Premium présentent différents niveaux de service, pour mieux répondre à vos besoins.

Advanced	Premium
Horaires de bureau régionaux (anglais, finnois, français, allemand, japonais et suédois)	**24h/24, 7j/ 7 (anglais)**
Accès prioritaire au support technique	Réponse aux incidents critiques dans l'heure
Outils en ligne de ticketing et de suivi	Management level escalation : Remontée des dossiers
Téléphone et rappel	Consultation de mise à niveau
Chat et support à distance	Recommandations pour la suppression des malwares

8. Sécurité des données

La plateforme WithSecure™ Elements Endpoint Protection utilise les services web d'Amazon (AWS). Cela nous permet d'assurer une grande disponibilité, une meilleure résistance aux défaillances, de meilleurs temps de réponse et une évolutivité optimale. Ces services sont actuellement disponibles en Europe, en Amérique du Nord et en région APAC.

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 : https://aws. amazon.com/compliance/

WithSecure™ se conforme aux réglementations et lois relatives à la protection de la vie privée dans tous les pays où nous opérons.

Nous prenons très au sérieux la protection de nos centres de données. Nous assurons leur sécurité en utilisant plusieurs dizaines de mesures de sécurité, telles que :

- **La « sécurité par conception » :** nos systèmes sont conçus d'emblée pour être sécurisés. Nous intégrons le respect de la vie privée et la sécurité au développement de nos technologies et systèmes, depuis les premières étapes de la conceptualisation jusqu'à l'exploitation.
- **Des contrôles d'accès rigoureux :** seul un groupe réduit d'employés de WithSecure™ ayant fait l'objet d'une enquête approfondie a accès aux données des clients. Les droits et les niveaux d'accès sont basés sur leur fonction et leur rôle, selon le principe du moindre privilège, au regard des responsabilités qui leur sont attribuées.
- **Une sécurité opérationnelle renforcée :** avec une gestion attentive des vulnérabilités, la prévention des malwares et des processus solides de gestion des incidents, nous traquons chaque danger susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité des systèmes ou des données.

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.

W / T H®
secure