

Brochure

W / T H[®]
secure

WithSecure[™] Elements Cloud Security Posture Management

**Gérez votre sécurité cloud en identifiant les
risques liés à votre infrastructure cloud**



Corrigez rapidement les mauvaises configurations cloud

Elements Cloud Security Posture Management (CSPM) vous aide à gérer la sécurité de votre infrastructure cloud en identifiant régulièrement et de manière proactive les problèmes de configuration. Cette solution effectue des analyses de votre environnement cloud et des vérifications complètes des configurations non-sécurisées. Elle vous fournit ensuite des conseils sur les étapes à suivre pour corriger les problèmes de sécurité détectés.

La plupart des entreprises exploitent des configurations hybrides et multi-clouds. Le passage au cloud a, certes, permis de surmonter de nombreux problèmes liés aux installations on-premise mais, désormais, les entreprises font aussi face à de nouvelles responsabilités liées à la sécurisation de leur environnement cloud.

Ces environnements doivent être configurés avec soin : en effet, en cas de mauvaise configuration, les ressources d'une entreprise risquent de devenir accessibles via internet. Les erreurs de configuration représentent un risque énorme. Elles peuvent facilement exposer une infrastructure cloud et les données qu'elle contient aux cyberattaques. Par ailleurs, les plateformes cloud évoluent très rapidement et certaines nouvelles fonctionnalités peuvent exposer à des risques inédits. À cela, s'ajoute la pression des réglementations : les entreprises doivent répondre aux nombreuses exigences des organismes de régulation en matière de sécurité cloud.

Les erreurs de configuration sont si nombreuses et variées qu'elles peuvent être difficiles à détecter et à corriger manuellement. Il est pourtant nécessaire de les mener un travail de correction efficace, car les attaques cloud sont opportunistes : les hackers sont à l'affût de la moindre erreur.

WithSecure™ Elements Cloud Security Posture Management (CSPM) aide les entreprises à faire face à ces nouveaux enjeux. Cette solution vous apporte une visibilité accrue sur votre environnement cloud et sur les risques potentiels. Elle vous permet de gérer la sécurité de toutes les tâches fonctionnant sur les plateformes courantes IaaS (Infrastructure as a Service). CSPM vous fournit des données actualisées en continu sur les mauvaises configurations de votre cloud et vous propose des conseils de correction, axés sur le niveau de risque.

En résumé

✓ Identifiez les erreurs de configuration avant que les hackers ne s'en chargent

Nous proposons une approche couvrant l'ensemble du processus de correction. Pour faciliter le travail de l'utilisateur, des affichages intuitifs résumant l'essentiel de la situation.

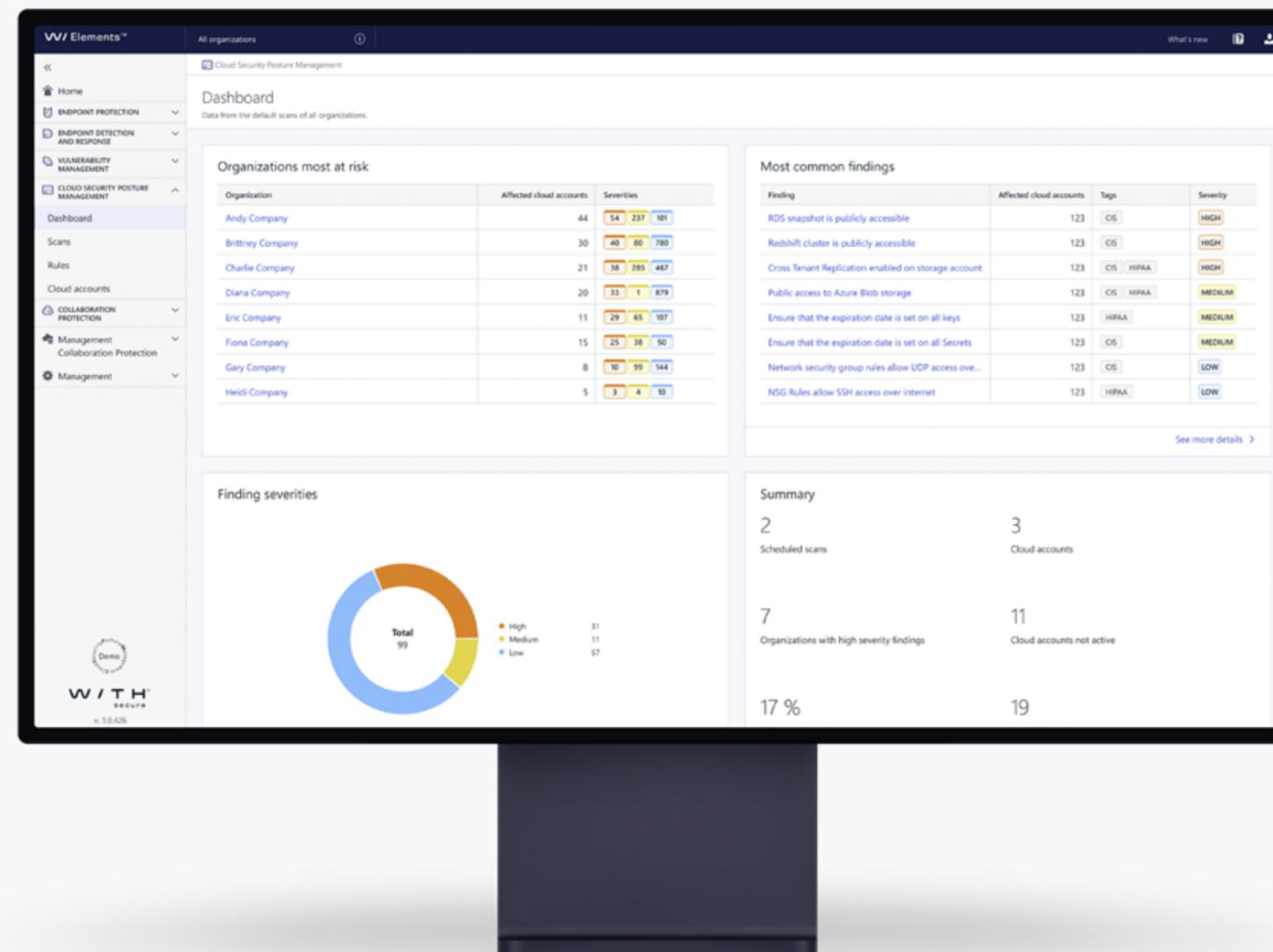
✓ Identifiez rapidement les mauvaises configurations

Ajoutez simplement votre compte et démarrez l'analyse. Nous faisons gagner du temps à nos clients et partenaires en leur permettant de détecter efficacement les problèmes de configurations. Les analyses sont rapides et vous pouvez aisément suivre l'évolution des mesures correctives*.

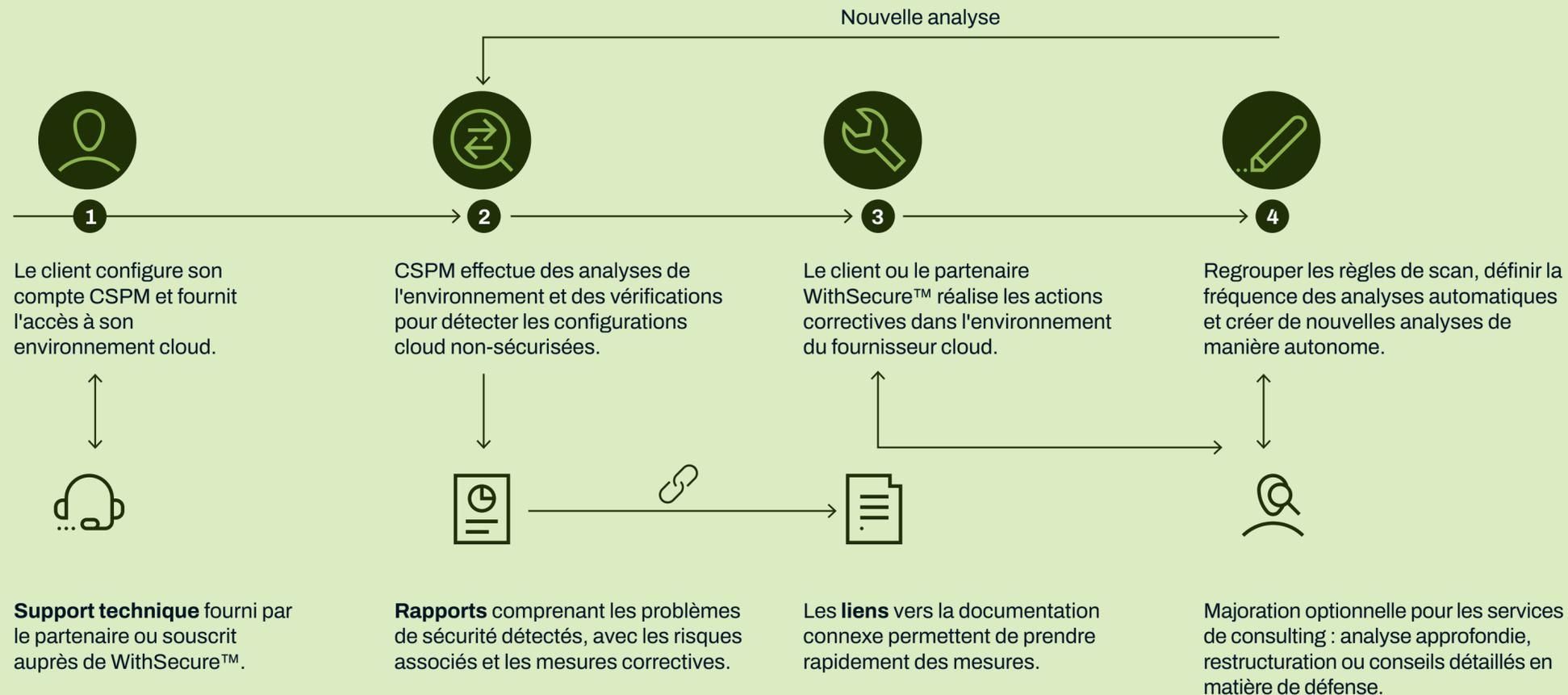
✓ Réduisez les risques, simplifiez les process, gagnez en efficacité

Hiérarchisez efficacement les mesures correctives en fonction des niveaux de risque et d'efforts requis. Corrigez rapidement les mauvaises configurations sur la base de données pratiques. Nos rapports visuels vous permettent d'optimiser votre sécurité tout en récoltant des preuves pour les auditeurs et aux organismes de réglementation.

* L'évolution basée sur les données historiques sera disponible dans la version généralisée, au cours du mois de novembre 2023.



Fonctionnement



1. Le client fournit l'accès à son environnement cloud. CSPM est rapide et facile à configurer. Si un support technique est nécessaire pour l'utilisation de la solution, il peut être fourni par le partenaire WithSecure™ ou directement par WithSecure™, par exemple via l'achat d'un support technique de niveau avancé ou premium. En outre, les services Technical Service Manager (TSM), disponibles auprès de WithSecure™, permettent de bénéficier de conseils personnels et d'un support pour l'utilisation de l'ensemble de la plateforme Elements, y compris CSPM.
2. La technologie CSPM de WithSecure™ effectue des analyses de votre environnement et des vérifications prêtes à l'emploi pour les configurations non sécurisées. Elle génère des rapports sur les problèmes de sécurité détectés, les risques associés et les étapes de correction. Des liens vers la documentation correspondante sont également proposés, pour vous permettre d'agir rapidement.
 - Les clients peuvent poser des questions sur les conclusions de ces rapports et demander conseil en souscrivant aux services de consulting de WithSecure™.
3. Le client ou le partenaire de WithSecure™ effectue les actions correctives dans l'environnement du fournisseur cloud.
4. Les entreprises peuvent créer de nouvelles analyses, déterminer les règles d'analyse utilisées et la fréquence d'analyse. Elles peuvent regrouper des règles d'analyse et configurer les comptes cibles pour ces analyses. Et pour optimiser leur sécurité, elles peuvent souscrire aux services de consulting pour bénéficier d'une analyse approfondie, reconcevoir leur environnement et mettre en place une protection en profondeur.

Les entreprises ont le choix entre gérer elles-mêmes Elements CSPM ou souscrire à Elements CSPM auprès de l'un de nos partenaires. Elles peuvent aussi externaliser Cloud Security Posture Management auprès de WithSecure™ en souscrivant à la formule 100% managée, dans le cadre de notre solution Countercept.

Fonctionnalités

Il peut être difficile d'implémenter des services cloud de manière sécurisée tout en répondant aux exigences de conformité. CSPM change la donne et vous permet d'y parvenir.

Avec CSPM, vous gérez vos identifiants et votre sécurité depuis un portail unique, avec vos outils existants de sécurisation des endpoints, de protection collaborative et de gestion des vulnérabilités. WithSecure™ Elements Cloud Security Posture Management (CSPM) vous fournit une visibilité accrue sur votre environnement cloud et sur les risques potentiels. Cette solution vous fournit en continu des données relatives aux mauvaises configurations cloud et vous propose des conseils correctifs axés sur le niveau de risque.

Vous pouvez programmer des analyses planifiées des comptes cloud pour évaluer la sécurité des configurations cloud. Vous effectuez également des analyses à la demande et appliquez des groupes de règles de sécurité à vos environnements cloud.

* L'évolution basée sur les données historiques sera disponible dans la version généralisée, au cours du mois de novembre 2023.

Suite aux analyses, CSPM vous fournit des conclusions sur votre sécurité cloud ainsi que des recommandations. Vous pouvez ainsi hiérarchiser les priorités et procéder à des actions correctives en fonction du niveau de risque, pour éliminer rapidement les failles de sécurité.

Les recommandations axées sur le niveau de risque permettent de corriger les mauvaises configurations cloud. Le niveau de risque peut être catégorisé comme faible, moyen ou élevé. Grâce à des rapports clairs, les administrateurs IT peuvent réagir efficacement tout en répondant aux exigences de sécurité des auditeurs et organismes de réglementation. CSPM permet également de consulter les données historiques et votre niveau de sécurité à un instant donné dans le passé*.



Avantages



Analyses régulières

Menez des analyses complètes de la sécurité cloud. Ces analyses s'appuient sur l'expertise de terrain de notre équipe de recherche sur les menaces.



Votre cloud, sécurisé

Prise en charge des infrastructures des plateformes cloud AWS et Azure.



Priorisation efficace

Avec le tableau de bord CSPM, consultez les informations essentielles, sous forme de graphiques faciles à interpréter.



Conseils basés sur les risques

Nous fournissons des données liées au degré de sévérité, pour vous permettre de mieux évaluer les risques qui ciblent votre entreprise.



Reporting simplifié

Des rapports clairs, pour visualiser les risques cloud et donner aux administrateurs les moyens de réagir efficacement. Ces rapports permettent aussi de rendre compte des pratiques de sécurité auprès des auditeurs et des autorités de régulation.



Gestion intégrée de la sécurité

Gérez votre sécurité cloud depuis un portail intuitif. Utilisez ce même portail pour la sécurisation des endpoints, la protection collaborative et la gestion des vulnérabilités.

Principales fonctionnalités

Analyses et ré-analyses régulières

Bénéficiez d'une visibilité accrue sur les risques liés à votre infrastructure cloud. L'analyse peut être programmée pour être exécutée chaque semaine, toutes les deux semaines, chaque mois ou à la demande, afin de vous donner du temps entre les cycles de rapport pour les actions correctives. CSPM fournit des informations qui vous permettent de hiérarchiser les priorités, ainsi que des instructions pour corriger les erreurs de configuration en fonction de leur niveau de risque. Vous pouvez également télécharger les résultats des analyses au format PDF ou CSV.

Tableau de bord

Nous vous présentons les informations qui requièrent votre attention dans des graphiques faciles à interpréter. Vous pouvez consulter l'évolution de votre sécurité au fil du temps*. Vous visualisez l'évolution des résultats d'analyse et identifiez les changements de configuration qui déclenchent des investigations approfondies*. En tant que partenaire WithSecure™, vous pouvez également visualiser les entreprises les plus à risque et voir comment leur sécurité évolue au fil du temps* grâce aux différentes mesures.

Sécurité des tâches exécutées sur les plateformes cloud public les plus courantes

Actuellement, CSPM prend en charge AWS et Azure. Au total, pour les deux versions, il existe actuellement environ deux cents contrôles de configuration. Nos contrôles sont sans cesse actualisés pour s'adapter à l'évolution des environnements cloud. Ces contrôles sont le produit de notre expertise, de cas pratiques rencontrés par nos consultants, et des principaux référentiels de conformité.

Support MSP et MSSP

Possibilité pour les partenaires, comme les MSP et les MSSP, de proposer CSPM sous forme de service managé. Certaines fonctionnalités comme les templates de règles CSPM, ou encore Elements Common Scope Selector, permettent aux administrateurs partenaires de gérer un grand nombre de clients. Nos partenaires peuvent concevoir et fournir différents niveaux de service CSPM pour différents clients.

Expertise et recherche

Nous nous appuyons sur notre vaste expertise de consulting pour vous proposer cette technologie. Notre équipe de recherche l'a développée en se basant sur notre modélisation des menaces, qui tient compte des erreurs de configuration ciblées par les hackers. Les contrôles portent notamment sur les privilèges IAM trop permissifs, les données non-chiffrées au repos, les instances cloud ayant accès à des adresses IP publiques, et sur l'activation des logs pour les investigations post-incident.

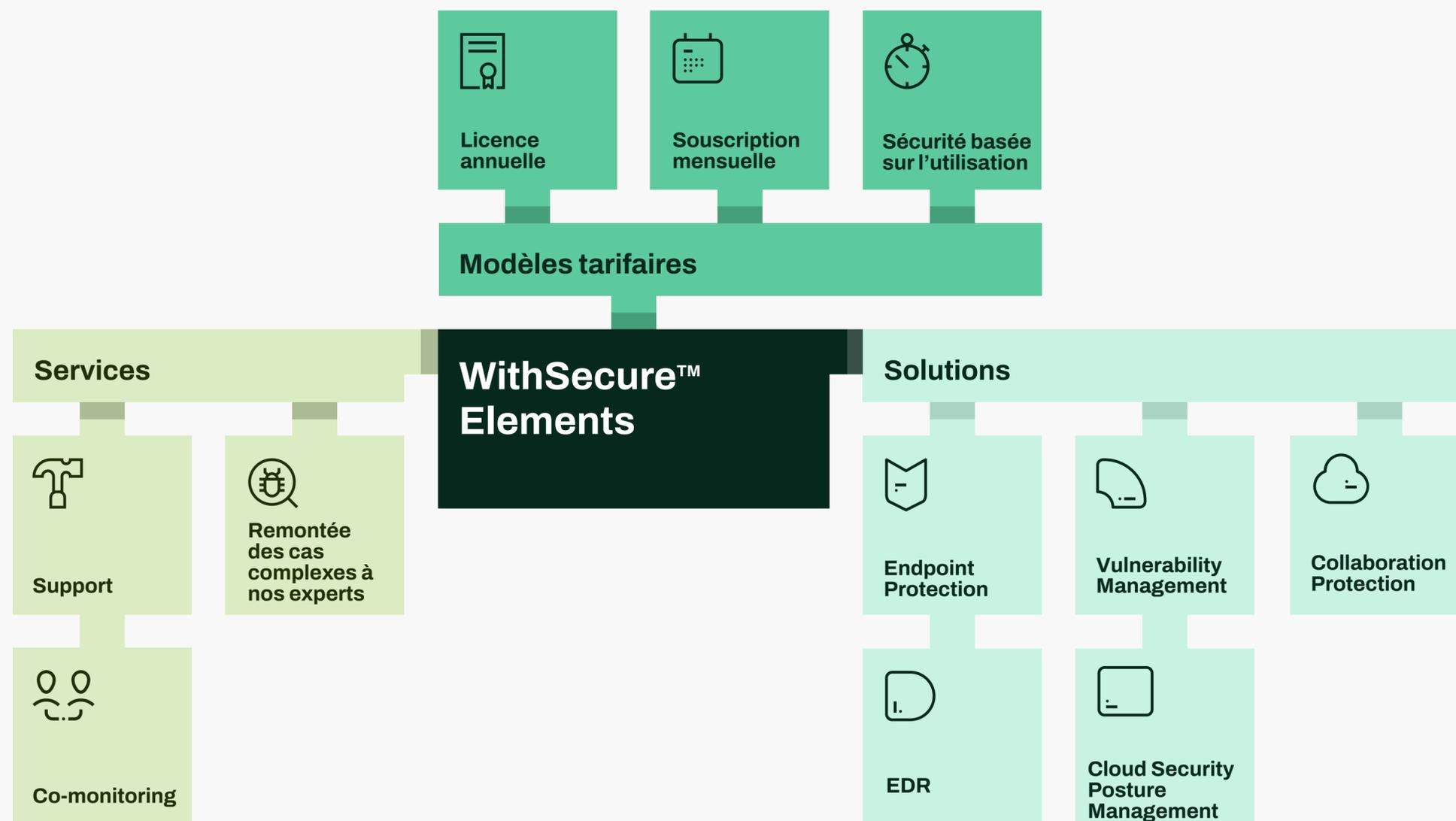
* L'évolution basée sur les données historiques sera disponible dans la version généralisée, au cours du mois de novembre 2023.

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

WithSecure™ Elements Cloud Security Posture Management est disponible en solution autonome ou en tant que composant de WithSecure Elements™, notre plateforme de cybersécurité modulaire.

WithSecure™ Elements offre aux clients une protection complète via une plateforme unifiée et un centre de sécurité intuitif. Cette plateforme centralisée associe de puissantes capacités de sécurité prédictives, préventives et réactives, pour une protection intelligente contre les menaces, les ransomwares et les attaques ciblées. Grâce à sa simplicité inégalée, Elements permet aux entreprises de se concentrer sur l'essentiel : leur cœur d'activité.

À tout moment, nos clients peuvent soumettre les cas les plus critiques à nos Threats Hunters pour qu'ils enquêtent et leur apportent des conseils de réponse. Notre offre modulaire et nos modèles tarifaires flexibles offrent une grande évolutivité. WithSecure™ Elements peut également s'intégrer aux divers systèmes de sécurité des entreprises clientes (SIEM, SOAR, systèmes de gestion de la sécurité, systèmes de surveillance ou de reporting).



Essayez Elements !

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