Guide d’achat des solutions de XDR

Évoluer en pro dans le marché de la détection et de l’intervention étendues (XDR)

Comprendre la détection et l'intervention étendues (XDR)

Pourquoi le monde a-t-il besoin d'une autre approche de sécurité?

Dans le paysage hybride, multifournisseur et multivecteur d'aujourd'hui, la complexité est le plus grand défi. Les équipes de sécurité doivent protéger un écosystème en constante expansion, en menant des opérations avec des dizaines d'outils dont l'intégration est incohérente. L'IDO et le travail hybride ont entraîné l'élargissement de la surface d'attaque. Le nombre d'hameçonnage, de logiciels malveillants et de rançongiciels doublent et parfois triplent d'année en année. En même temps, les entreprises sont plus hyperconnectées que jamais. Une faille de sécurité dans une entreprise peut avoir une incidence sur ses fournisseurs, ses partenaires, ses clients et même sur des secteurs entiers de l'économie.

Cette nouvelle normalité exige de la résilience en matière de sécurité, la capacité de protéger l'intégrité de chaque aspect de votre entreprise pour résister aux menaces ou aux changements imprévisibles, et en sortir plus forte. Et la résilience en matière sécurité exige plus que ce que le passé a offert.

Quelle est la solution?

Alors que les menaces deviennent de plus en plus virulentes, l'ancien modèle de détection et d'intervention fondé sur des solutions de sécurité ponctuelles autonomes ne suffit plus. C'est ici que la XDR entre en jeu. La solution de détection et d'intervention étendues (XDR) est un outil unifié de détection et d'intervention d'incidents. Les solutions de XDR collectent et mettent en corrélation automatiquement les données télémétriques provenant de plusieurs outils de sécurité, appliquent des analyses pour détecter les activités malveillantes, puis réagissent aux menaces et les éliminent. Les solutions de XDR efficaces sont complètes et mettent en corrélation les données de tous les vecteurs (courriels, points terminaux, serveurs, charges de travail en nuage et réseaux), ce qui permet une visibilité et un contexte dans votre environnement, même pour les menaces les plus avancées.

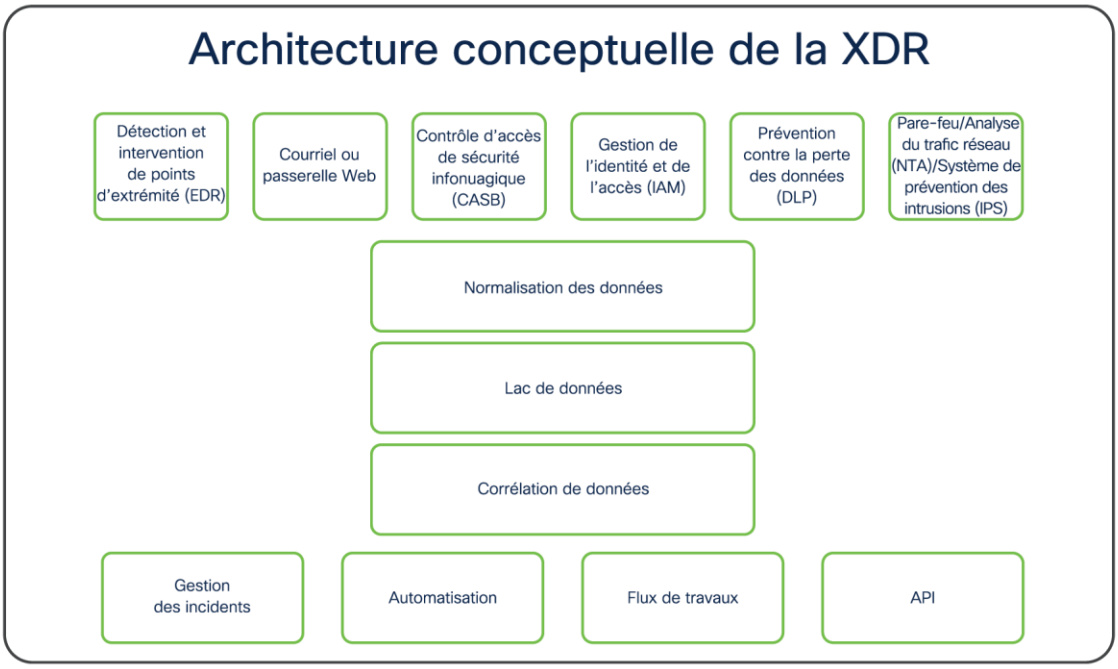
Pourquoi la XDR?

Premièrement, elle permet aux équipes de détecter les menaces les plus virulentes grâce à la corrélation des événements et aux détections de plusieurs fournisseurs sur les réseaux, les nuages, les points terminaux, les courriels, et plus encore.

Deuxièmement, elle réduit la fatigue liée aux alertes en permettant aux équipes de hiérarchiser les menaces en fonction de leur incidence.

Troisièmement, elle augmente la productivité grâce à l'automatisation des tâches afin que les équipes puissent utiliser plus efficacement les ressources du centre des opérations de sécurité.

Quatrièmement, elle permet aux entreprises de renforcer la résilience de la sécurité en comblant les failles de sécurité et en anticipant la prochaine étape grâce à des informations exploitables.



Cinq éléments clés d'une détection et d'une intervention étendues (XDR) appropriées

1. Fournir des données télémétriques hiérarchisées et exploitables, partout où vous en avez besoin

Pouvez-vous passer efficacement au crible l'océan d'alertes pour trier les menaces?

L'étendue de la visibilité et la profondeur des renseignements sont des éléments fondamentaux de la XDR. De nombreuses menaces virulentes n'attaquent pas seulement les points terminaux ou le réseau. Elles attaquent par divers vecteurs, notamment le courriel, les points terminaux, le réseau, la gestion des identités, la fonction de bac à sable et le pare-feu. Voilà pourquoi vous avez besoin d'une solution de XDR dotée d'un large éventail de données de télémétrie et de qualité qui peuvent éclairer vos résultats de XDR et fournir une vue holistique et complète de ce qui se passe dans l'ensemble de votre environnement. L'objectif n'est pas seulement de recueillir des renseignements, la gestion des incidents est tout aussi importante. Pour que la solution de XDR ait les effets escomptés, ces renseignements doivent être hiérarchisés. Les solutions de XDR qui offrent une hiérarchisation en fonction des risques, et qui hiérarchisent les incidents en fonction du risque important le plus élevé, vous permettront d'agir plus rapidement sur ce qui est vraiment important. Elles doivent également proposer des recommandations pour les étapes suivantes afin que vous puissiez prendre des décisions éclairées sur le meilleur plan d'action.

Principales fonctions et capacités	Domaines de produits connexes
• Efficacité et précision pour minimiser le bruit des faux positifs • Regroupement et corrélation des alertes dans l'ensemble de l'environnement	Détection et intervention au point terminal (EDR)
• Supervision continue du réseau en temps réel	Network Detection and Response (NDR)
• Des analyses avancées qui génèrent des alertes hiérarchisées et contextuelles en cas de détection de logiciels malveillants inconnus et d'autres attaques réseau virulentes	Détection et intervention de réseau (NDR)
• Supervision continue des menaces liées à la messagerie en temps réel et hiérarchisation automatique des mesures correctives	Sécurité de la messagerie

Questions à poser aux fournisseurs

- Comment votre solution m'offre-t-elle une visibilité sur tous mes environnements (points terminaux, appareils, réseau)?
- Comment votre solution fournit-elle des renseignements? Votre solution fournit-elle des données télémétriques hiérarchisées?
- Comment votre solution hiérarchise-t-elle les menaces en fonction de l'incidence sur l'entreprise et des risques?
- Quel type d'informations sur les menaces utilise votre système de détection? D'où viennent ces informations?
- Comment validez-vous les sources de données que vous utilisez dans votre solution?
- Comment ce produit gère-t-il les menaces virulentes telles que Wannacry, NotPetya et Turla?

2. Permettre une détection unifiée, quel que soit le vecteur ou le fournisseur

Votre solution de XDR permet-elle à vos investissements en matière de sécurité de fonctionner comme une unité coordonnée?

Les menaces deviennent de plus en plus virulentes et couvrent une plus grande variété de vecteurs d'attaque. Il n'a donc jamais été aussi important de garantir une détection cohérente dans l'ensemble votre environnement. À l'heure actuelle, les équipes de sécurité sont confrontées à un niveau de complexité hors du commun, tant dans leur environnement de sécurité que dans un écosystème composé de chaînes logistiques mondiales, d'attaquants et de défenseurs. Les solutions de XDR peuvent vous aider à atteindre cet objectif en regroupant, en corrélant et en hiérarchisant les détections en fonction de leur gravité et de leur incidence. Pour y parvenir, votre pile de sécurité doit fonctionner à l'unisson. En sélectionnant une solution de XDR ouverte, extensible et axée sur le nuage, vous profiterez d'une détection unifiée et d'une corrélation des événements dans l'ensemble de votre environnement sans ajouter de couches de complexité supplémentaires. Chaque composant de votre pile de sécurité possède des éléments de détection uniques (réseautage, courriel, pare-feu, etc.) et chacun devient plus puissant lorsqu'ils sont réunis. Il est important de considérer que la XDR devrait englober les six sources de données télémétriques, y compris les points terminaux, le réseau, le pare-feu, le courriel, l'identité et le DNS, afin de fournir une vue d'ensemble des menaces potentielles. Votre solution de XDR doit s'intégrer facilement à l'ensemble de votre pile de sécurité grâce à l'intégration native dorsale et frontale, afin que la couverture reste cohérente même lorsque les fournisseurs apportent des modifications à leur gamme ou si vous changez de fournisseur. Finalement, afin d'optimiser les capacités de détection des menaces de votre système de sécurité, il convient d'explorer les solutions de XDR qui peuvent fournir un contexte local précieux et délivrer des verdicts d'informations sur les menaces précis sur lesquels vous pouvez compter.

Principales fonctions et capacités	Domaines de produits connexes
• Détecter et bloquer les comportements anormaux des programmes en cours d'exécution sur les points terminaux, y compris les attaques par injection de mémoire basées sur des exploits. • Déterminer les indicateurs de compromission (IoC) avec la cartographie MITRE ATT&CK • Superviser la réputation des fichiers afin de détecter et d'isoler les menaces au point d'entrée • Détecter les vulnérabilités du système d'exploitation dans votre environnement, ce qui permet aux administrateurs de hiérarchiser les mesures correctives en fonction des risques et de réduire la surface d'attaque	Détection et intervention au point terminal (EDR), gestion des vulnérabilités
• Utiliser des analyses avancées pour détecter rapidement les logiciels malveillants inconnus, les menaces internes telles que l'exfiltration de données, les infractions aux politiques et autres attaques virulentes. • Détecter les attaques de réseau en temps réel grâce à des alertes haute fidélité	Détection et intervention étendues (XDR), détection et intervention de réseau (NDR)
• Détecter et bloquer les courriels indésirables grâce au filtrage de réputation • Déceler les attaques par courriel fondées sur la tromperie, telles que l'ingénierie sociale et les imposteurs, et s'en protéger	Sécurité de la messagerie

Questions à poser aux fournisseurs

- Sur combien de mes investissements existants votre plateforme de XDR peut-elle tirer parti?
- Votre plateforme de XDR est-elle compatible avec mes solutions, indépendamment du fournisseur?
- Vos solutions ont-elles des intégrations prêtes à l'emploi les unes avec les autres?
- En quoi vos technologies de détection sont-elles meilleures que les autres technologies sur le marché?
- Quels types de menaces votre solution permet-elle de détecter? Associe-t-elle les alertes au cadre MITRE ATT&CK?

3. Prendre en charge une intervention rapide et précise aux menaces

Une fois les menaces détectées, à quelle vitesse pouvez-vous intervenir en toute confiance?

L'unification des informations provenant du réseau, des points terminaux et des courriels (pour n'en nommer que quelques-uns) permet de comprendre plus précisément ce qui s'est passé, comment cela a progressé et quelles mesures doivent être prises pour éliminer la menace. L'idéal serait que vous puissiez visualiser les incidences et la portée des menaces à partir d'un seul endroit et que vous puissiez prendre des mesures en un ou deux clics. Une solution de XDR efficace nécessite des capacités d'intervention et de correction natives, comme l'isolation d'un hôte ou la suppression d'un courriel malveillant de toutes les boîtes de réception. La XDR devrait également faciliter la création de mesures d'intervention personnalisées, avec des possibilités d'automatisation, afin que les équipes puissent faire évoluer la sécurité au fil du temps.

Principales fonctions et capacités	Domaines de produits connexes
• Intervenir rapidement aux menaces sur les points terminaux une fois compromis	Détection et intervention au point terminal (EDR)
• Déterminer et isoler la cause première d'un problème ou d'un incident de réseau en quelques secondes	Détection et intervention étendues (XDR), détection et intervention de réseau (NDR)
• Bloquer rapidement les sites Web malveillants grâce à une analyse en temps réel des clics	Sécurité de la messagerie

Questions à poser aux fournisseurs

- Quelles interventions le produit fournit-il?
- La correction peut-elle être effectuée sur le point terminal à l'aide d'une solution de XDR à un emplacement et adaptée à d'autres?
- Comment le produit s'intègre-t-il aux outils de sécurité existants qui permettent l'intervention?
- Comment votre solution accélère-t-elle la correction?
- De l'alerte de menace à la correction, quel est le temps d'intervention (p. ex. pour une attaque par hameçonnage)?

4. Offrir un point de vue d'enquête unique pour une expérience utilisateur simplifiée

La détection des menaces, l'intervention et la correction sont-elles gérées à partir d'une interface unique?

Lors de l'évaluation des solutions de XDR, il est important de considérer l'expérience de l'analyste de sécurité. Les équipes des opérations de sécurité (SecOps) ont suffisamment de choses à gérer. Il n'est pas nécessaire de les ralentir avec des dizaines d'outils et une pléthore de consoles. C'est pourquoi nous recommandons les solutions de XDR qui sont conçues pour aider les analystes à détecter et à intervenir aux menaces plus rapidement et plus efficacement en fournissant une vue unifiée des données de sécurité sur plusieurs outils de sécurité et sources de données. Cela peut contribuer à rationaliser les flux de travail et à réduire le temps et les efforts nécessaires pour enquêter sur les incidents de sécurité et y remédier. Les solutions de XDR devraient fournir un tableau de bord du cycle de vie complet couvrant chaque vecteur de menace et chaque point d'accès. Elles devraient faciliter la recherche de menaces, grâce à des modèles tels que MITRE ATT&CK, qui rendra accessible la recherche de menaces basée sur des hypothèses pour les personnes novices avec le processus, et facilitera l'anticipation de la prochaine étape. Un autre facteur à considérer est l'incidence de la conception sur l'expérience de l'analyste. Elle devrait accroître la productivité, améliorer les délais de prise de décision associés aux fonctions clés de détection, d'investigation et d'intervention et permettre à un analyste débutant ou intermédiaire d'effectuer des tâches avancées dans le cadre des opérations de sécurité en fournissant un meilleur contexte pour les alertes avec une divulgation progressive permettant de déterminer rapidement l'étendue et la gravité d'une menace.

Principales fonctions et capacités	Domaines de produits connexes
• Fournir un tableau de bord du cycle de vie complet couvrant chaque vecteur de menace et chaque point d'accès. • Offrir un ensemble d'outils unifiés qui s'étendent à vos équipes d'ITOps, de SecOps et de NetOps • Accéder aux données, aux analyses et à l'automatisation et les gérer à partir d'un emplacement unifié	Détection et réponse étendues (XDR)

Questions à poser aux fournisseurs

- Comment votre solution aide-t-elle mon équipe dans ses efforts de recherche des menaces?
- Comment la solution s'intègre-t-elle aux technologies de sécurité existantes telles que les solutions d'orchestration, d'automatisation et d'intervention de sécurité (SOAR) et de gestion des informations et des événements liés à la sécurité (GIES)?
- Puis-je utiliser votre solution de XDR pour comprendre l'incidence d'une menace, découvrir l'étendue de la violation et prendre des mesures en un seul clic à partir d'une seule interface?

- Votre solution prend-elle en charge la sécurité basée sur les rôles en limitant tout ou partie de l'accès au système ou au sous-système à des groupes autorisés et à des utilisateurs individuels?
- Pouvez-vous centraliser et analyser les données télémétriques de toutes mes technologies de sécurité existantes?
- Votre solution simplifie-t-elle les flux de travail d'intervention aux incidents pour réduire la durée globale de l'enquête?

5. Offrir la possibilité d'augmenter la productivité et de renforcer la posture de sécurité

Vos solutions de XDR augmentent-elles l'efficacité de la détection des menaces et de l'intervention, avec moins de frais généraux?

L'automatisation et l'orchestration sont des éléments importants pour renforcer la résilience de sécurité de votre entreprise. Votre personnel de sécurité a des tâches importantes à accomplir. Lorsqu'ils sont confrontés à une menace de sécurité, il n'est pas nécessaire qu'ils perdent leur temps à suivre des flux de travail complexes, manuels et répétitifs. Les solutions de XDR qui améliorent la productivité en automatisant les flux de travail essentiels, comme la découverte d'une alerte, sa corrélation, la hiérarchisation et l'intervention rapide, libéreront vos équipes tout au long du cycle de vie. Une solution de XDR efficace doit réduire le délai moyen d'intervention en permettant une enquête qui présente des décisions et des actions claires qui permettent aux analystes d'intervenir automatiquement et de manière cohérente conformément à leurs politiques et procédures. Cela signifie que vos équipes des opérations de sécurité (SecOps) peuvent consacrer leur temps et leur énergie à des tâches de sécurité plus stratégiques et plus proactives, renforçant ainsi la posture de sécurité de votre entreprise.

Principales fonctions et capacités	Domaines de produits connexes
• Recherche automatique des menaces sur les points terminaux, y compris les menaces à faible prévalence • Permettre aux administrateurs de rédiger et de rechercher des indicateurs de compromission personnalisés (IoC)	Détection et intervention au point terminal (EDR)
• Correction préventive des menaces réseau grâce à des informations fondées sur l'analyse comportementale	Détection et intervention étendues (XDR), détection et intervention de réseau (NDR)
• Hiérarchiser automatiquement les mesures correctives contre les menaces liées aux courriels	Sécurité de la messagerie

Questions à poser aux fournisseurs

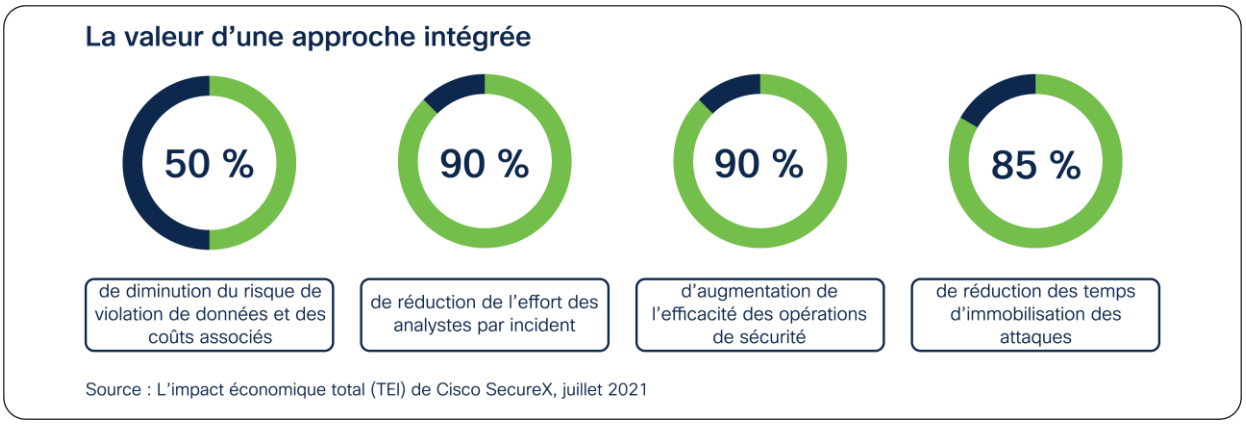
- Pour vos intégrations tierces, les modifications apportées par les fournisseurs à l'interface API interrompent-elles vos scripts d'automatisation?
- Comment votre solution prend-elle en charge la surveillance vers et depuis les charges de travail en nuage?
- Aurai-je besoin de changer d'environnement ou de déployer de nouvelles technologies avec la solution de XDR?
- Votre solution de XDR offre-t-elle des intégrations prédéfinies et prêtes à l'emploi avec des technologies de sécurité tierces?
- La solution de XDR réduit-elle le temps nécessaire à l'analyste pour enquêter sur un incident et le résoudre?
- Votre solution de XDR éclaire-t-elle la gestion de vos politiques en vue de renforcer la résilience?

Cisco XDR

La XDR est un composant essentiel de la résilience de sécurité

Aujourd'hui, l'incertitude est une garantie. Ainsi, les entreprises investissent dans la résilience à tous les niveaux de leur activité, du service des finances jusqu'aux chaînes logistiques. Toutefois, ces mesures ne seront pas suffisantes sans un investissement dans la résilience de la sécurité, c'est-à-dire la capacité de protéger votre entreprise contre les menaces et les perturbations et de réagir aux changements en toute confiance afin d'en ressortir encore plus fort.

La XDR est un composant essentiel à l'adoption d'une résilience de la sécurité pour votre entreprise. En appliquant correctement la solution de XDR, vous renforcerez votre sécurité en donnant aux équipes de sécurité les moyens de hiérarchiser les menaces en fonction de leur incidence, de les détecter plus rapidement et d'accélérer l'intervention. Les capacités d'automatisation et d'orchestration facilitent ce processus et libèrent les équipes de sécurité pour qu'elles puissent se concentrer sur ce qui importe le plus.



Opérations de sécurité simplifiées avec Cisco XDR

Cisco ouvre la voie à la XDR avec la gamme de produits de sécurité la plus complète du marché. Chez Cisco, nous avons investi de manière proactive dans la création de la gamme de produits de sécurité la plus complète du marché, en anticipant les besoins de sécurité de l'avenir et en intégrant les composants pour rendre la sécurité efficace, simple et accessible à toutes les équipes, quel que soit le fournisseur ou le vecteur. Nous comprenons que la mise en place d'une approche de XDR est tout un processus, et nous voulons que vos équipes sortent du cercle vicieux de la couverture disparate d'un secteur sursaturé de solutions ponctuelles. Avec Cisco XDR, notre objectif est de découvrir le chemin le plus court entre la détection et l'intervention avec le moins de difficultés possible.

Conçu par des experts de centre des opérations de sécurité pour des experts de centre des opérations de sécurité, Cisco XDR simplifie les opérations de sécurité pour permettre aux analystes de sécurité de rester proactifs et résilients face aux menaces les plus virulentes. Notre solution est ouverte, extensible, et axée sur le nuage, ce qui vous permet de tirer parti des investissements existants en matière de sécurité et de bénéficier d'une détection de sécurité unifiée dans l'ensemble de votre environnement.

Chez Cisco, la protection des ressources des clients est une responsabilité que nous prenons très au sérieux, car nous sommes aussi les clients de nos clients. Nous souhaitons vous accompagner dans votre démarche de résilience en matière de sécurité grâce à Cisco Security Cloud, une plateforme de sécurité ouverte qui vous aide à protéger l'ensemble de votre écosystème, quelle que soit la suite des événements. Joignez-vous à nous et découvrez la puissance d'une sécurité complète.

Prêt à mettre en place dès aujourd'hui les opérations de sécurité de demain?

Explorez Cisco XDR

Principaux éléments et fonctionnalités de XDR

Utilisez ce tableau (pages 10 et 11) pour une référence rapide lors des conversations avec les fournisseurs de XDR.

Principal élément	Principales capacités	Produits Cisco harmonisés
Fournir des données télémétriques hiérarchisées et exploitables, partout où vous en avez besoin	• Détection et intervention au point terminal (EDR) intégrées qui peuvent être entièrement gérées, recherche proactive des menaces • Gestion intégrée des vulnérabilités en fonction des risques qui permet de déterminer rapidement les vulnérabilités, d'évaluer les risques, de les hiérarchiser et de les corriger.	Secure Endpoint
	• Analyse continue de l'activité du nuage • Analyses avancées, y compris la modélisation comportementale et les algorithmes d'apprentissage automatique • Une vue unique de votre infrastructure de sécurité pour une visibilité unifiée et des informations agrégées et exploitables.	Cisco XDR
	• Filtres d'épidémie avancés avec analyse en temps réel des clics	Cisco Secure Email
Permettre une détection unifiée, quel que soit le vecteur ou le prestataire	• Détection et blocage du comportement anormal d'un programme en cours d'exécution • Possibilité d'effectuer des requêtes de système d'exploitation avancées sur le point terminal en temps réel • Recherche de menaces intégrée qui est conforme au cadre MITRE ATT&CK	Secure Endpoint
	• Détecter les attaques dans le nuage en temps réel grâce à des alertes de haute qualité enrichies de contextes comme l'utilisateur, l'appareil, l'emplacement, l'horodatage et l'application • Détecter et isoler les menaces grâce à des détections confirmées • Détecter les entités non autorisées avec la détection et l'intervention de réseau (NDR) et automatiser la mise en quarantaine avec les points terminaux • Détecter les hôtes internes communiquant avec un hôte externe • Fournir une piste d'audit complète de toutes les transactions effectuées dans le nuage, ce qui permet de mener des enquêtes plus efficaces. • Intégrations intégrées à d'autres solutions de XDR dans la gamme de produits • Intégrations des solutions tierces par le biais d'intégrations intégrées, clés en main ou personnalisées, pour une architecture dorsale connectée et une expérience frontale uniforme. • Intégrations intégrées à d'autres technologies dans le nuage, les points terminaux, le réseau et les applications (y compris d'autres technologies tierces)	Cisco Secure Network Analytics et Cisco XDR
	• Antipourriel, protection et contrôle liés aux URL, analyse antivirus haute performance, filtres d'épidémie et analyse de la réputation pour les fonctionnalités de domaine • Détection des courriels falsifiés qui protège contre les attaques de type compromission de la messagerie d'entreprise ciblant la haute direction • Analyse automatisée des logiciels malveillants et fonction de bac de sable	Cisco Secure Email

Principal élément	Principales capacités	Produits Cisco harmonisés
Prendre en charge une intervention rapide et précise aux menaces	• Accéder à une protection permanente grâce à des informations sur les menaces et à des informations provenant de centres d'opérations de sécurité (SOC) dédiés à l'échelle mondiale pour une large base de clients.	Tous les produits Cisco Secure
	• Supervision continue de toutes les activités des points terminaux, assurant la détection et le blocage des comportements anormaux pendant l'exécution	Secure Endpoint
	• Repérer et isoler les menaces du trafic chiffré sans compromettre la confidentialité et l'intégrité des données • Déclencher des flux de travail d'« intervention » à partir d'un emplacement unique • Une intervention aux menaces qui regroupe la connaissance contextuelle des sources de données des produits de sécurité et les informations sur les menaces globales provenant de Talos® et de sources tierces par l'intermédiaire d'interfaces API. • Créer des dossiers d'enquêtes sur les incidents	Cisco XDR
	• Protection permanente contre les menaces basées sur les URL grâce à l'analyse en temps réel des liens potentiellement malveillants • Exploitation continue de la supervision, des analyses et des informations sur les menaces de Talos® en temps réel afin d'identifier des menaces précédemment inconnues ou des changements soudains	Cisco Secure Email
Offrir un point de vue d'enquête unique pour une expérience utilisateur simplifiée	• Rassembler et mettre en corrélation des informations globales dans une vue unique afin d'accélérer les enquêtes sur les menaces • Créer des interventions personnalisées pour réduire le temps d'intervention • Automatiser l'enrichissement à partir de sources de données multiples, superposées à des informations sur les menaces	Cisco XDR
Offrir la possibilité d'augmenter la productivité et de renforcer la posture de sécurité	• Identification automatique et analyse des menaces des exécutables à faible prévalence • Possibilité d'écrire des indicateurs de compromission personnalisés pour analyser les indicateurs post-compromission sur l'ensemble du déploiement des points terminaux.	Secure Endpoint
	• Modélisation comportementale, apprentissage automatique multicouche et vigie des cybermenaces mondiales • Classification automatique des nouveaux rôles d'appareils à mesure qu'ils sont ajoutés au réseau • Intégration avec une solution de XDR pour permettre l'automatisation de chaque vecteur de menace et de chaque point d'accès	Cisco Secure Network Analytics et Cisco XDR
	• Déclencher automatiquement une analyse dynamique de la réputation et fournir une visibilité sur l'origine des logiciels de messagerie malveillants, sur les systèmes affectés et sur les activités des logiciels malveillants • Prendre des mesures sur les courriels entrants et sortants en se basant sur les renseignements relatifs à la correction	Cisco Secure Email
	• Automatiser les tâches de sécurité de routine au moyen de flux de travail prédéfinis qui s'harmonisent avec les scénarios d'utilisation les plus courants • Partager des guides entre les équipes des opérations de sécurité • Tri et hiérarchisation automatisés des alertes provenant d'autres solutions de la gamme de produits de sécurité	Cisco XDR

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (USA) Pad Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C07-3236254-03 04/23