Guide d'achat des solutions XDR

Maîtriser le marché des technologies de détection et de réponse étendues (XDR)

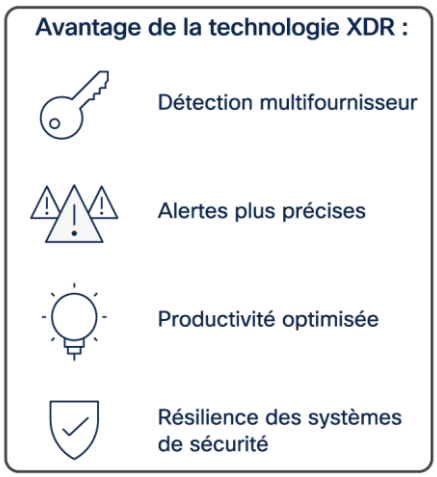
© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Comprendre les technologies de détection et de réponse étendues (XDR)

Le monde a-t-il besoin d'une nouvelle solution de sécurité ?

Dans le paysage hybride, multifournisseur et multimenaces d'aujourd'hui, la complexité représente le plus grand défi. Les équipes de sécurité doivent protéger un écosystème en constante expansion, exécutant des opérations sur plusieurs dizaines d'outils sans intégration homogène. En effet, l'émergence des objets connectés et du travail hybride ont élargi la surface d'exposition aux attaques. Les menaces que représentent le phishing, les malwares et les ransomwares doublent, voire triplent chaque année. Dans le même temps, les entreprises sont plus hyperconnectées que jamais. Une faille de sécurité peut avoir un impact sur les fournisseurs, les partenaires, les clients et même sur des secteurs entiers de l'économie.

Dans ce nouveau contexte, les systèmes de sécurité doivent être résilients, c'est-à-dire capables de protéger l'intégrité de tous les aspects de l'entreprise afin qu'elle résiste aux menaces et aux imprévus, et en ressorte plus forte. Et cette résilience doit aller plus loin que jamais.



Quelle est la solution ?

Face à des menaces de plus en plus sophistiquées, l'ancien modèle de détection et de réponse reposant sur des outils ponctuels et autonomes ne suffit plus. C'est là que la technologie XDR (Extended Detection and Response) entre en jeu pour unifier la détection des incidents liés à la sécurité et les moyens de réponse. Les solutions XDR collectent et mettent en corrélation automatiquement les données télémétriques de plusieurs outils de sécurité, effectuent des analyses pour détecter les activités malveillantes, puis traitent les menaces et les éliminent. Une solution XDR efficace doit être complète et analyser les données de tous les vecteurs d'attaque (e-mails, terminaux, serveurs, workloads cloud et réseaux), pour obtenir une visibilité et des informations contextuelles sur l'ensemble de votre environnement, et repérer les menaces les plus avancées.

Pourquoi opter pour la technologie XDR ?

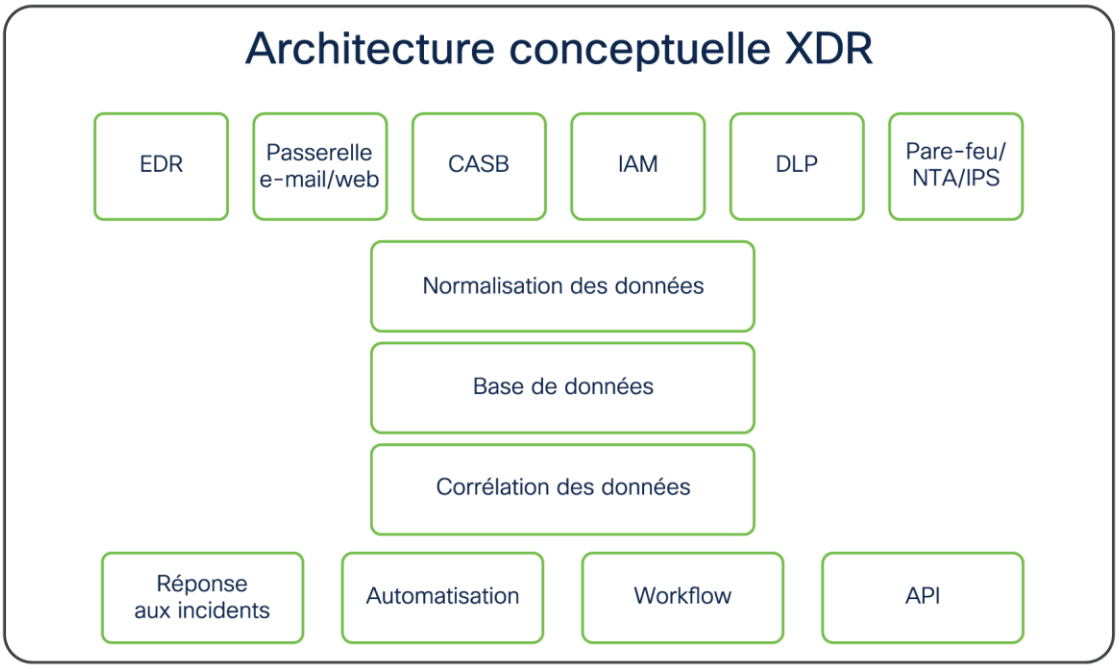
Premièrement, cette solution permet aux équipes de détecter les menaces les plus sophistiquées grâce à la mise en corrélation des événements et aux détections multifournisseurs sur le réseau, le cloud, les terminaux, la messagerie e-mail et bien plus encore.

Deuxièmement, elle permet de faire face au grand nombre d'alertes en permettant aux équipes de hiérarchiser les menaces en fonction de leur impact.

Troisièmement, elle optimise la productivité grâce à l'automatisation des tâches afin que les équipes puissent utiliser plus efficacement les ressources du SOC.

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

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



5 atouts clés d'une stratégie XDR

1. Des données de télémétrie hiérarchisées et exploitables, partout où vous en avez besoin

Comment passer en revue efficacement la multitude d'alertes pour trier les menaces ?

Une visibilité complète et des informations détaillées sont essentielles à la technologie XDR. De nombreuses menaces parmi les plus sophistiquées ne s'attaquent pas uniquement aux terminaux ou au réseau : elles exploitent divers vecteurs d'attaque, notamment la messagerie e-mail, les terminaux, le réseau, l'identification des utilisateurs, le sandboxing et les pare-feu. C'est pourquoi vous avez besoin d'une solution XDR avec un large éventail de données télémétriques et de qualité pouvant informer vos résultats XDR et fournir une vue globale et complète de ce qui se passe dans votre environnement. Mais il ne s'agit pas seulement de collecter des informations, la gestion des incidents est tout aussi importante. Pour que la technologie XDR ait l'impact attendu, ces informations doivent être hiérarchisées. Les solutions XDR qui offrent une hiérarchisation basée sur les risques (en hiérarchisant les incidents en fonction des risques les plus importants) vous permettent d'agir plus rapidement sur les véritables menaces. Elles doivent également proposer des recommandations pour les prochaines étapes, afin que vous puissiez prendre des décisions abouties sur la meilleure marche à suivre.

Principales fonctions et capacités	Types de produits associés
• Efficacité et précision pour minimiser le bruit des faux positifs • Agréger et mettre en corrélation les alertes dans tout l'environnement	Détection et réponse au niveau des terminaux (EDR)
• Supervision en temps réel et continue du réseau	Détection réseau et réponse (NDR)
• Des analyses avancées qui génèrent des alertes hiérarchisées avec contexte lorsque des malwares inconnus et d'autres	Détection et réponse étendues (XDR)

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Principales fonctions et capacités	Types de produits associés
attaques sophistiquées du réseau sont détectés.	
• Surveillance en temps réel et continue des menaces visant les e-mails et hiérarchisation automatique des mesures correctives	Sécurité des e-mails

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Questions à poser aux fournisseurs

- Comment votre solution m'offre-t-elle une visibilité sur tous mes environnements (terminaux, équipements, réseau) ?
- Comment votre solution fournit-elle les informations ? Votre solution propose-t-elle des données de télémétrie hiérarchisées ?
- Comment votre solution hiérarchise-t-elle les menaces en fonction de l'impact sur l'entreprise et des risques ?
- Quel type de Threat Intelligence alimente votre détection ? D'où proviennent ces informations ?
- Comment validez-vous les sources de données que vous utilisez dans votre solution ?
- Comment ce produit gère-t-il les menaces sophistiquées telles que Wannacry, NotPetya et Turla ?

2. Une détection unifiée sur les outils de tous les fournisseurs et sur tous les vecteurs d'attaques

Votre solution XDR vous permet-elle de regrouper vos investissements dans la sécurité sous une entité unique et coordonnée ?

Alors que les menaces sont de plus en plus sophistiquées et couvrent une plus grande variété de vecteurs d'attaque, il n'a jamais été aussi important d'assurer une détection cohérente dans votre environnement. Aujourd'hui, les équipes chargées de la sécurité sont confrontées à un niveau extraordinaire de complexité à la fois dans leur environnement de sécurité et dans un écosystème de chaînes d'approvisionnement, de hackers et de défenseurs du monde entier. Les solutions XDR peuvent vous aider en agrégeant, en mettant en corrélation et en hiérarchisant les détections en fonction de leur gravité et de leur impact. Mais pour cela, votre pile de sécurité doit fonctionner à l'unisson. En choisissant une solution XDR ouverte, extensible et axée sur le cloud, vous bénéficiez d'une détection et d'une mise en corrélation unifiées des événements de votre environnement au lieu d'ajouter des couches de complexité supplémentaires. Chaque composant de votre pile de sécurité comporte des éléments de détection uniques (réseau, messagerie, pare-feu, etc.) qui sont plus performants une fois réunis. C'est pourquoi la technologie XDR doit englober six sources de télémétrie : terminal, réseau, pare-feu, messagerie e-mail, identification des utilisateurs et DNS, pour fournir une vue complète des menaces potentielles. Votre solution XDR doit s'intégrer facilement à l'ensemble de votre pile de sécurité grâce à l'intégration native du back-end au front-end, afin de disposer d'une couverture cohérente, même lorsqu'un fournisseur modifie sa gamme ou que vous changez de fournisseur. Enfin, pour optimiser les fonctionnalités de détection des menaces dans votre pile de sécurité, il est recommandé de vous tourner vers les solutions XDR, qui peuvent fournir un contexte local ainsi que des verdicts de Threat Intelligence précis et fiables.

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Principales fonctions et capacités	Types de produits associés
• Détecter et bloquer les comportements anormaux des programmes exécutés sur les terminaux, y compris les attaques par injection de mémoire basées sur les exploits • Déterminer les indicateurs de compromission (IoC) en s'alignant sur MITRE ATT&CK • Surveiller la réputation des fichiers pour détecter et isoler les menaces au point d'entrée • Identifier les vulnérabilités des systèmes d'exploitation dans votre environnement, ce qui permet aux administrateurs de hiérarchiser les mesures correctives en fonction des risques et de réduire votre surface d'exposition aux attaques	Détection et réponse au niveau des terminaux (EDR), gestion des vulnérabilités
• Utiliser l'analytique avancée pour détecter rapidement les malwares inconnus, les menaces internes – comme l'exfiltration de données –, les violations de politiques et les autres attaques sophistiquées • Détecter les attaques réseau en temps réel grâce à des alertes haute fidélité	Détection et réponse étendues (XDR), détection et réponse réseau (NDR)
• Détecter et bloquer les e-mails indésirables grâce au filtrage par réputation • Identifier et contrer les e-mails falsifiés, tels que ceux utilisés dans le cadre de l'ingénierie sociale et autres impostures	Sécurité des e-mails

Questions à poser aux fournisseurs

- Parmi mes investissements précédents, lesquels peuvent être exploités par votre plateforme XDR ?
- Votre plateforme XDR est-elle compatible avec mes solutions, quel qu'en soit leur fournisseur ?
- Vos solutions offrent-elles des intégrations clés en main les unes avec les autres ?
- En quoi vos technologies de détection sont-elles supérieures aux autres solutions disponibles sur le marché ?
- Quels types de menaces votre solution permet-elle de détecter ? Aligne-t-elle les alertes sur le cadre MITRE ATT&CK ?

3. Une réponse rapide et précise aux menaces

Une fois identifiées, à quelle vitesse pouvez-vous contrer les menaces ?

Unifier les informations du réseau, des terminaux et de la messagerie e-mail permet notamment de comprendre plus précisément de quelle manière une attaque s'est produite, comment elle a progressé et quelles mesures sont nécessaires pour y remédier. Idéalement, vous devez pouvoir visualiser l'impact et la portée des menaces depuis une seule et même console, et agir en un clic ou deux. Une stratégie XDR efficace nécessite des fonctionnalités natives de réponse et de remédiation, telles que l'isolation d'un hôte ou la suppression d'un e-mail malveillant de toutes les boîtes de réception. La technologie XDR doit aussi faciliter la création de réponses personnalisées avec possibilités d'automatisation pour que les équipes puissent faire évoluer la sécurité au fil du temps.

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Principales fonctions et capacités	Types de produits associés
• Répondre rapidement aux menaces sur les terminaux une fois compromis	Détection et réponse au niveau des terminaux (EDR)
• Identifier et isoler la cause première d'un problème ou d'un incident réseau en quelques secondes	Détection et réponse étendues (XDR), détection et réponse réseau (NDR)
• Bloquer rapidement les sites web malveillants grâce à une analyse en temps réel des clics	Sécurité des e-mails

Questions à poser aux fournisseurs

- Quels moyens de réponse le produit propose-t-il ?
- Peut-on effectuer une remédiation au niveau d'un terminal à l'aide d'une solution XDR à un emplacement et l'étendre à d'autres ?
- Comment le produit s'intègre-t-il aux outils de réponse déjà en place ?
- Comment votre solution accélère-t-elle la remédiation ?
- Quel est le délai de réponse entre l'alerte et la remédiation (par exemple, pour une attaque par phishing) ?

4. Un point de vue unique pour une expérience d'utilisation simplifiée

Dans votre environnement, la détection, la réponse et la remédiation aux menaces sont-elles gérées depuis une même interface ?

Lors de l'évaluation des solutions XDR, il est important de prendre en compte l'expérience des analystes de la sécurité. Les équipes SecOps ont suffisamment à gérer. Inutile de les ralentir avec des dizaines d'outils et une pléthore de consoles. C'est pourquoi nous recommandons des solutions XDR conçues pour aider les analystes à détecter les menaces et à y répondre plus rapidement et plus efficacement en offrant une vue unifiée des données issues de plusieurs outils et sources. Elles vous permettent de rationaliser les workflows et de réduire le temps et les efforts nécessaires pour analyser les incidents liés à la sécurité, et y remédier. Les solutions XDR doivent fournir un tableau de bord couvrant le cycle de vie complet des menaces, pour chaque vecteur d'attaque et chaque point d'accès. Elles doivent faciliter la recherche active des menaces, grâce à des modèles comme MITRE ATT&CK, rendre le processus de Threat Hunting basé sur des hypothèses accessible aux personnes novices en la matière et permettre de mieux anticiper les risques à venir. Un autre facteur à prendre en compte est l'impact de la conception sur l'expérience des analystes. Il s'agit d'augmenter la productivité, d'accélérer la prise de décision associée aux fonctions de détection, d'analyse et de réponse, et de permettre à un analyste de niveau débutant ou intermédiaire d'effectuer des tâches avancées dans le cadre des opérations de sécurité. Pour cela, il faut enrichir les informations contextuelles des alertes afin de déterminer rapidement la portée et la gravité d'une menace potentielle.

Principales fonctions et capacités	Types de produits associés
• Fournir un tableau de bord couvrant le cycle de vie complet des menaces, pour chaque vecteur d'attaque et chaque point d'accès • Fournir un ensemble d'outils unifié qui s'étend à vos équipes ITOps, SecOps et NetOps • Consulter et gérer les données, les analyses et l'automatisation à partir d'une seule et même console	Détection et réponse étendues (XDR)

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

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 SOAR et SIEM ?
- Puis-je utiliser votre solution XDR pour comprendre l'impact d'une menace, déterminer la portée de la faille et prendre des mesures en un clic à partir d'une seule interface ?
- Votre solution prend-elle en charge la sécurité basée sur les rôles en limitant l'accès à tout ou partie du système/sous-système aux groupes et utilisateurs autorisés ?
- Pouvez-vous centraliser et analyser les données de télémétrie de tous mes outils de sécurité actuels ?
- Votre solution rationalise-t-elle les workflows de réponse aux incidents pour accélérer globalement les enquêtes techniques ?

5. L'opportunité d'augmenter la productivité et de renforcer la sécurité

Vos solutions XDR améliorent-elles la détection des menaces et l'efficacité de la réponse, avec moins d'efforts ?

L'automatisation et l'orchestration sont des éléments essentiels pour renforcer la résilience de la sécurité de votre entreprise. Les membres de votre équipe de sécurité ont des tâches importantes à accomplir. Lorsqu'ils sont confrontés à une menace, suivre des workflows manuels complexes et répétitifs est une perte de temps. Les solutions XDR qui améliorent la productivité en automatisant les workflows critiques, tels que la détection d'une alerte, sa mise en corrélation, sa hiérarchisation et la mise en place d'une riposte rapide, libèrent vos équipes tout au long du cycle de vie. Une solution XDR efficace doit réduire le délai moyen de réponse en présentant clairement les décisions et les actions aux analystes afin qu'ils puissent répondre de manière automatisée et cohérente, conformément à leurs politiques et procédures. Cela signifie que vos équipes SecOps peuvent consacrer leur temps et leur énergie à des tâches plus stratégiques et plus proactives, renforçant ainsi la sécurité de votre entreprise.

Principales fonctions et capacités	Types de produits associés
• Threat Hunting automatisé sur les terminaux, y compris pour les menaces à faible prévalence • Permettre aux administrateurs d'écrire et de rechercher des indicateurs personnalisés de compromission (IoC)	Détection et réponse au niveau des terminaux (EDR)
• Remédiation prédictive des menaces sur le réseau grâce à des informations basées sur l'analyse comportementale	Détection et réponse étendues (XDR), détection et réponse réseau (NDR)
• Hiérarchiser automatiquement la remédiation des menaces par e-mail	Sécurité des e-mails

Questions à poser aux fournisseurs

- Les modifications apportées aux API des fournisseurs perturbent-elles vos scripts d'automatisation dans le cadre de vos intégrations tierces ?
- Comment votre solution permet-elle de superviser les workloads basés dans le cloud ?
- Dois-je changer d'environnement ou déployer de nouvelles technologies avec la solution XDR ?
- Votre solution XDR offre-t-elle des intégrations prédéfinies et prêtes à l'emploi avec des technologies de sécurité tierces ?

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

- La solution XDR réduit-elle le temps nécessaire aux analystes pour examiner et traiter un incident ?
- Votre solution XDR alimente-t-elle la gestion des politiques pour renforcer la résilience ?

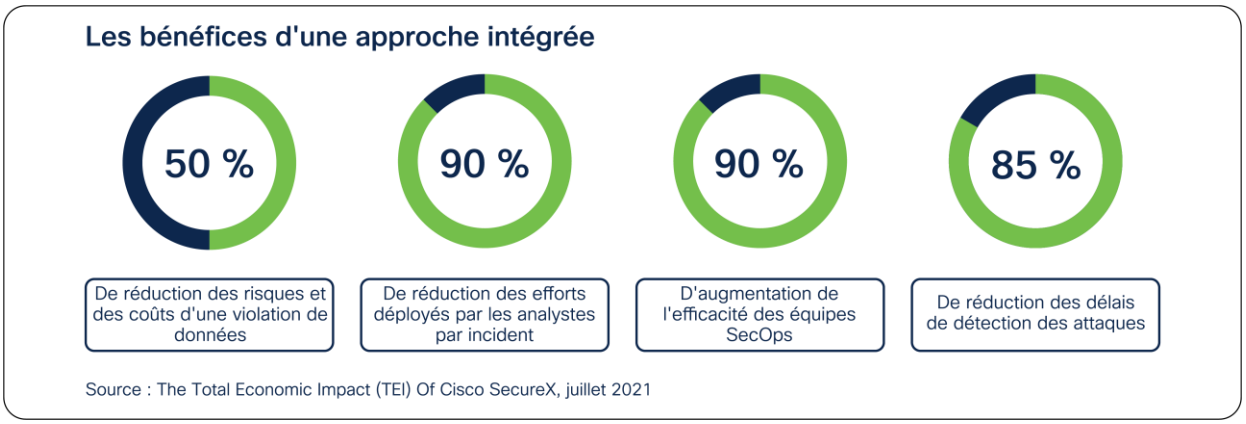
© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Cisco XDR

L'approche XDR est un composant essentiel d'une sécurité résiliente

Aujourd'hui, l'incertitude est devenue la norme. En réponse, les entreprises investissent dans la résilience de tous les aspects de leur activité, des finances jusqu'aux chaînes d'approvisionnement. Mais cela ne suffit pas si vous n'investissez pas aussi dans la résilience de vos systèmes de sécurité, c'est-à-dire la capacité à protéger votre entreprise en toutes circonstances, à vous adapter au changement en toute confiance et à renforcer vos activités.

La technologie XDR est un composant essentiel de la résilience des systèmes de sécurité de votre entreprise. Avec la bonne stratégie XDR, vous renforcez votre niveau de sécurité en permettant aux équipes de hiérarchiser les menaces selon leur impact, de détecter les incidents plus tôt et d'accélérer la réponse. Les fonctionnalités d'automatisation et d'orchestration facilitent ce processus, laissant aux équipes de sécurité le temps de se concentrer à des projets plus importants pour l'entreprise.



Simplifier les opérations de sécurité avec Cisco XDR

Cisco ouvre la voie vers la technologie XDR avec la gamme de solutions de sécurité la plus complète du marché. Nous avons investi de manière proactive dans la création de la gamme de solutions de sécurité la plus complète du marché. Nous avons anticipé les besoins futurs en matière de sécurité et intégré les composants nécessaires pour proposer une solution simple et accessible à toutes les équipes qui prend en charge les outils de tous les fournisseurs et tous les vecteurs d'attaque. Nous le savons, mettre en place une approche XDR est un processus à long terme, et nous voulons sortir du cercle vicieux qui consiste à déployer un patchwork d'outils hétérogènes dans un secteur déjà saturé de solutions ponctuelles. Avec Cisco XDR, l'objectif est de déterminer le chemin le plus court entre la détection d'une menace et le moyen d'y répondre.

Conçu par des experts SOC pour les experts SOC, Cisco XDR simplifie les opérations de sécurité pour aider les analystes à rester proactifs et résilients contre les menaces les plus sophistiquées. Notre solution est ouverte, extensible et axée sur le cloud, ce qui permet de tirer parti de vos investissements de sécurité précédents et de bénéficier d'une détection unifiée dans l'ensemble de votre environnement.

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Protéger les ressources de nos clients est une responsabilité que Cisco prend au sérieux, car nous sommes nous-mêmes également clients de ces clients. Nous vous accompagnons avec Cisco Security Cloud, une plateforme de sécurité ouverte qui vous aide à protéger l'ensemble de votre écosystème et à gagner en résilience pour faire face à tout ce que l'avenir vous réserve. Rejoignez-nous et découvrez tout le potentiel d'une solution de sécurité complète.

Mettre en place les opérations de sécurité de demain, dès aujourd'hui.

En savoir plus sur Cisco XDR

Éléments fondamentaux et fonctionnalités du modèle XDR

Utilisez ce tableau (pages 10-11) comme référence rapide lors de vos conversations avec les fournisseurs XDR.

Éléments fondamentaux	Fonctionnalités clés	Produits Cisco correspondants
Des données de télémétrie hiérarchisées et exploitables, partout où vous en avez besoin	• Détection et réponse au niveau des terminaux (EDR) intégrées, pouvant être entièrement managées, recherche proactive des menaces • Gestion intégrée des vulnérabilités basée sur les risques, qui permet d'identifier les vulnérabilités, d'évaluer les risques, de hiérarchiser les problèmes et d'y remédier plus rapidement	Cisco Secure Endpoint
	• Analyse continue de l'activité cloud • Analytique avancée, y compris la modélisation comportementale et les algorithmes d'apprentissage automatique • Visibilité unifiée sur l'ensemble de votre infrastructure de sécurité, avec des informations agrégées exploitables	Cisco XDR
	• Filtres antipropagation avancés avec analyse en temps réel des clics	Cisco Secure Email
Une détection unifiée sur les outils de tous les fournisseurs et sur tous les vecteurs d'attaques	• 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 terminal en temps réel • Recherche proactive des menaces intégrée, alignée sur le cadre MITRE ATT&CK	Cisco Secure Endpoint
	• Détecter les attaques en temps réel sur l'ensemble du cloud grâce à des alertes haute fidélité enrichies d'informations contextuelles (comme l'utilisateur, l'équipement, l'emplacement, l'horodatage et l'application) • Détecter et isoler les menaces • Détecter les entités non autorisées avec notification de non-remise et automatiser la mise en quarantaine avec les terminaux • Détecter les hôtes internes communiquant avec un hôte externe • Fournir une piste d'audit complète de toutes les transactions cloud pour optimiser l'efficacité des enquêtes techniques • S'intégrer avec d'autres solutions XDR de la gamme • Prendre en charge des solutions tierces avec intégrations prêtes à l'emploi ou personnalisées, pour une architecture back-end connectée et une expérience front-end homogène • S'intégrer avec d'autres technologies dans le cloud, les terminaux, le réseau et les applications (y compris d'autres technologies tierces)	Secure Network Analytics et Cisco XDR
	• Anti-spam, protection et contrôle des URL, analyse antivirus ultraperformante, filtres antipropagation et analyse de la réputation des fonctionnalités du domaine	Cisco Secure Email

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

Éléments fondamentaux	Fonctionnalités clés	Produits Cisco correspondants
	• Détection des e-mails falsifiés qui protège contre les attaques BEC visant l'équipe dirigeante • Analyse automatisée des malwares et sandboxing	
Une réponse rapide et précise aux menaces	• Protection permanente grâce à des informations sur les menaces mises en commun à partir de centres opérationnels de sécurité (SOC) mondiaux dédiés pour une large base de clients	Toutes les solutions Cisco Secure
	• Surveillance continue de toutes les activités au niveau des terminaux, assurant la détection et le blocage des comportements anormaux au moment de l'exécution	Cisco Secure Endpoint
	• Identification et isolement les menaces chiffrées sans compromettre la confidentialité et l'intégrité des données • Déclenchement de workflows de « réponse » à partir d'un emplacement unique • Réponse aux menaces regroupant les informations contextuelles issues des sources de données sur les produits de sécurité ainsi que les informations sur les menaces mondiales provenant de Talos®, et de sources tierces via des API • Création de dossiers d'analyse des incidents	Cisco XDR
	• Protection permanente contre les menaces basées sur les URL via l'analyse en temps réel des liens potentiellement malveillants • Exploitation en continu et en temps réel de la surveillance, de l'analytique et des informations sur les menaces de Talos® pour identifier les risques auparavant inconnus ou les changements soudains	Cisco Secure Email
Un point de vue unique pour une expérience d'utilisation simplifiée	• Collection et mise en corrélation des informations globales dans une vue unique, pour accélérer l'analyse des menaces • Création d'actions personnalisées pour accélérer les capacités de réponse • Automatisation de l'enrichissement des données à partir de plusieurs sources, avec des informations sur les menaces	Cisco XDR
L'opportunité d'augmenter la productivité et de renforcer la sécurité	• Identification automatique et analyse des menaces pour les exécutables à faible prévalence • Possibilité de définir des IoC personnalisés pour rechercher des indicateurs post-compromission sur l'ensemble du déploiement des terminaux	Cisco Secure Endpoint
	• Modélisation comportementale, apprentissage automatique à plusieurs niveaux et informations sur les menaces à l'échelle mondiale • Classer automatiquement les rôles des nouveaux équipements à mesure qu'ils s'ajoutent au réseau • Intégration avec une solution XDR pour permettre l'automatisation pour l'ensemble des vecteurs de menaces et points d'accès	Secure Network Analytics et Cisco XDR
	• Déclenchement automatique d'une analyse dynamique de la réputation et visibilité sur l'origine des malwares, les systèmes affectés et leurs activités • Action sur les e-mails entrants et sortants en fonction des informations de remédiation	Cisco Secure Email
	• Automatisation des tâches de routine à l'aide de workflows prédéfinis alignés sur les cas d'usage les plus fréquents • Partage de guides entre les équipes SecOps • Tri et hiérarchisation automatisés des alertes provenant d'autres solutions de sécurité	Cisco XDR

© 2023 Cisco et/ou ses filiales. Tous droits réservés.

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

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. 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 de fax sont répertoriés sur le site web de Cisco, à l'adresse : **www.cisco.com/go/offices**.

Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : www.cisco.com/go/trademarks. Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)

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

© 2023 Cisco et/ou ses filiales. Tous droits réservés.