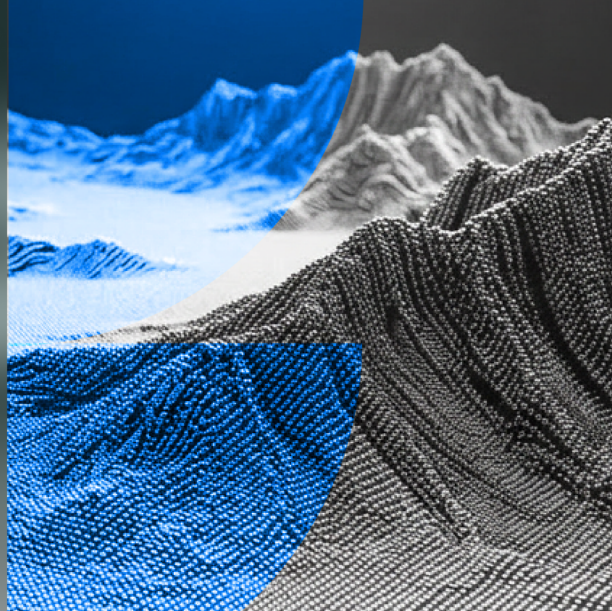


Proofpoint Collaboration Security Prime

Sécurité complète et continue de la collaboration à l'ère de l'IA



Principaux atouts

- Bloque le plus large éventail de menaces avec une précision de 99,999 %
- Contient les compromissions de compte en quelques minutes, que la menace commence par un email, soit véhiculée via d'autres vecteurs ou provienne d'un fournisseur compromis
- Réduit de 40 % les clics sur des liens malveillants réels dans les six mois suivant le déploiement
- Préviend l'usurpation d'identité et met les domaines similaires hors service avant qu'ils n'atteignent vos clients
- Réduit le coût total de possession de 40 % grâce à la consolidation de la plate-forme

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à sécuriser les personnes et les données dans les environnements de travail agentiques.

Présentation

L'IA a transformé le paysage pour tous. Les cybercriminels y ont recours pour lancer des attaques plus novatrices et personnalisées, avec une sophistication et une ampleur accrues. Les campagnes telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise) ont bondi de 27 %, et le phishing généré par l'IA enregistre désormais un taux de clics 4,5 fois supérieur à celui du phishing traditionnel. Les utilisateurs sont devenus plus vulnérables aux contenus générés par l'IA, tandis que les défenseurs sont submergés par le tri des alertes et des outils fragmentés.

Les entreprises ont besoin d'une approche fondamentalement différente, conçue pour l'ère des agents, où des outils et assistants pilotés par l'IA rejoignent la main-d'œuvre élargie au niveau des emails, des outils de messagerie instantanée et des applications cloud, étendant ainsi la surface d'attaque déjà exploitée par les cyberpirates.

Malheureusement, de nombreuses entreprises se voient contraintes d'adopter une approche fragmentée de la sécurité, reposant sur des produits isolés. Cela crée toutefois des failles supplémentaires dans leurs défenses, isole les équipes et augmente la complexité opérationnelle.

Pour se défendre contre les attaques optimisées par l'IA, déployées sur de multiples canaux et en plusieurs phases, ainsi que pour protéger les interactions de confiance, que ce soit entre des personnes, entre des personnes et des assistants d'IA ou entre des personnes et une application cloud, les entreprises ont besoin d'une approche plus globale. Proofpoint Collaboration Security Prime peut les y aider. Proofpoint Prime unifie la détection et la neutralisation des menaces au sein des environnements de travail agentiques.

Vous pouvez ainsi :

- Détecter plus tôt les menaces nouvelles générées par l'IA avec une meilleure visibilité sur la surface d'attaque
- Bloquer avec confiance grâce à une précision de pointe et à peu de faux positifs
- Assurer une protection continue avant et après la remise, dans les navigateurs et les environnements agentiques
- Protéger les communications professionnelles où qu'elles aient lieu, dans le chat, les applications et les agents
- Contenir les compromissions de comptes en quelques minutes, et non en plusieurs jours

Détection plus précoce des menaces nouvelles grâce à une meilleure visibilité

Les attaques nouvelles, générées par l'IA, évoluent plus vite que les défenses traditionnelles ne peuvent les intercepter. Elles parviennent ainsi à contourner les filtres hérités et atteignent les personnes par le biais de la messagerie électronique, des plates-formes de collaboration et des applications cloud.

Proofpoint Collaboration Security Prime comble cette faille grâce à une protection continue couvrant l'ensemble du cycle de vie des menaces, de la pré-remise à la post-remise dans l'architecture de messagerie électronique, et du moment du clic à la connexion, sur tous les canaux utilisés par les collaborateurs.

Proofpoint Prime prévient un large éventail de menaces :

- Phishing avancé, y compris le phishing d'identifiants de connexion et le phishing de rappel
- BEC et usurpation de l'identité du PDG
- Distribution de malwares
- Attaques par code QR
- Attaques par téléphone (TOAD)
- Envoi en masse d'emails
- Ransomwares
- Prise de contrôle de comptes
- Exploitation de services légitimes
- Attaques générées par l'IA et techniques d'exploitation de l'IA, telles que l'injection d'invites

Au cœur de cette protection se trouve Proofpoint Nexus® AI, le moteur de détection le plus avancé du secteur. Entraîné avec l'un des plus grands ensembles de données du secteur, Nexus AI évalue plus de 1 000 attributs par message. Il combine cinq types de modèles : modèles de langage, graphiques relationnels, apprentissage automatique, threat intelligence et vision par ordinateur. Ces modèles travaillent ensemble et apprennent en permanence de chaque verdict.

Il offre ainsi une efficacité de détection de 99,999 % et le taux de faux positifs le plus bas du secteur, ce qui permet de bloquer les menaces réelles sans inonder les équipes d'informations parasites.

Protection contre les compromissions de comptes

Les compromissions de comptes ne se limitent pas aux emails de phishing. L'IA permet aux cybercriminels de déployer plus facilement des attaques de collecte d'identifiants de connexion bien au-delà de la boîte de réception, de la création de pages de connexion ressemblant à s'y méprendre aux originales au contournement de l'authentification multifactor grâce à l'envoi en masse d'invites automatisées.

Dans un environnement de travail axé sur la collaboration et assisté par des agents, il est crucial de contrer ces menaces à chaque étape, avant, pendant et après la compromission.

Proofpoint Collaboration Security Prime aide à prévenir les compromissions avant qu'elles ne se produisent. SSO Password Guard de Proofpoint Prime détecte lorsque les collaborateurs réutilisent leur mot de passe d'entreprise sur des sites

non professionnels, fermant l'un des points d'entrée les plus courants pour les attaques basées sur les identifiants de connexion et étendant la protection au-delà des emails jusqu'au navigateur lui-même.

Lorsque la prévention ne suffit pas, Proofpoint Prime détecte les compromissions au fur et à mesure. Il met en corrélation les signaux d'identité et post-accès sur Microsoft 365, Google Workspace et Okta afin d'identifier les comptes présentant des signes de compromission.

Une fois qu'une compromission est identifiée, Proofpoint Prime vous aide à l'analyser et à la contenir en quelques minutes, et non en plusieurs jours, limitant ainsi le rayon d'impact avant qu'un cyberpirate ne puisse progresser davantage dans l'environnement.

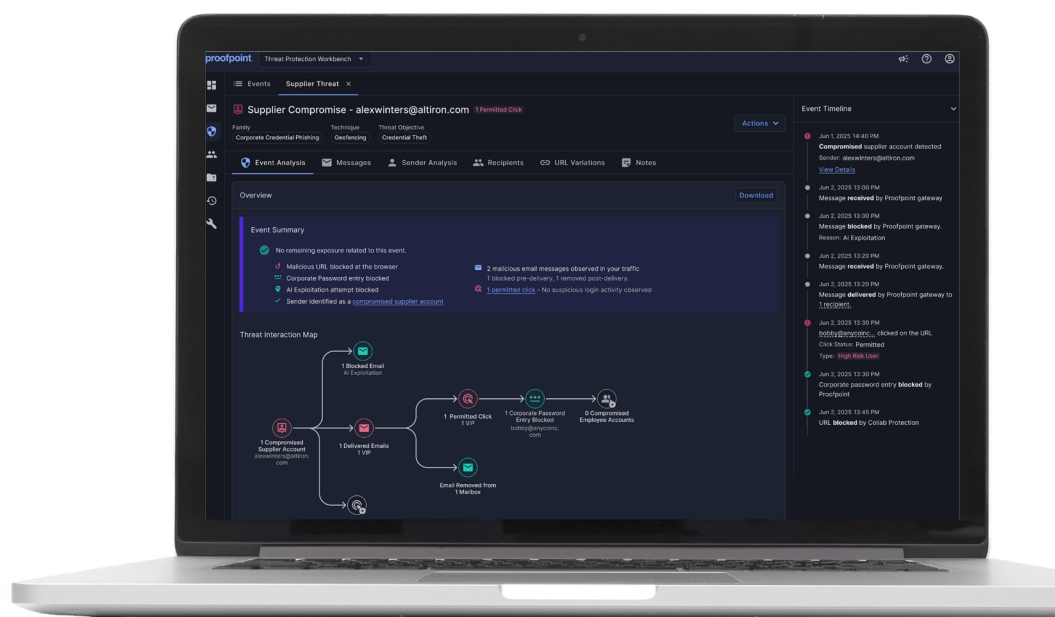


Figure 1. Proofpoint Collaboration Security Prime arrête et corrèle les menaces au niveau des emails, des outils de messagerie instantanée et de collaboration, du cloud et des canaux des fournisseurs.

Les modèles Nexus® AI sont entraînés avec l'un des ensembles de données les plus vastes et les plus diversifiés du secteur de la cybersécurité.

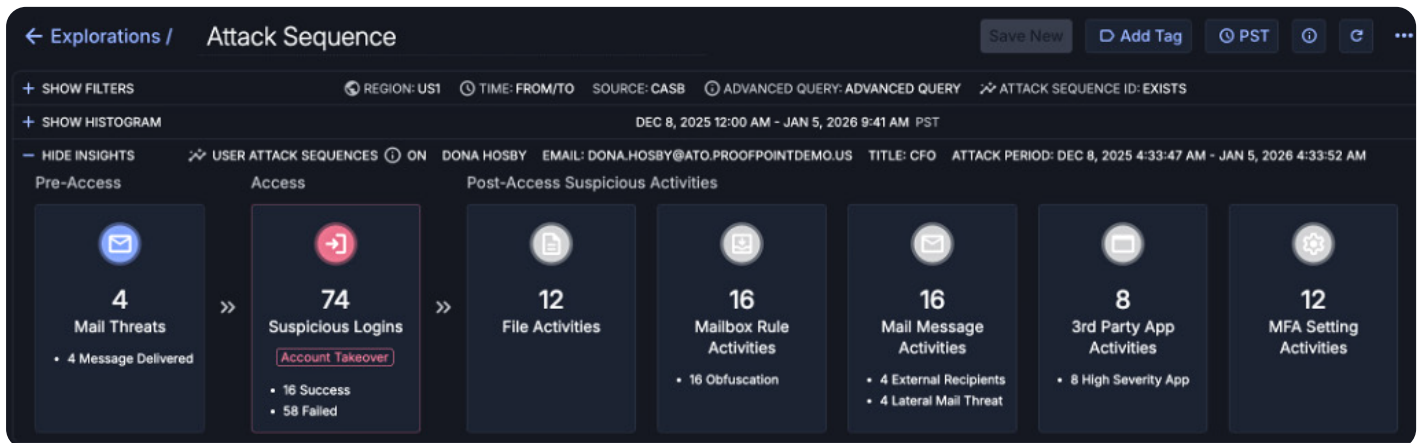


Figure 2. Proofpoint Collaboration Security Prime offre une visibilité sur les séquences d'attaque et automatise le confinement.

Protection de vos communications d'entreprise de confiance

Les cybercriminels ont souvent recours à des tactiques d'usurpation d'identité pour infiltrer des communications d'entreprise de confiance, que ce soit via l'usurpation directe de domaines, des domaines similaires ou des comptes fournisseurs compromis. Lorsque votre entreprise ou ses partenaires sont victimes d'une usurpation d'identité ou d'une compromission, vos collaborateurs et vos clients sont exposés à des risques, et votre marque peut subir de graves dommages.

Proofpoint Collaboration Security Prime peut vous aider à réduire ces risques d'usurpation d'identité de façon proactive. Il vous offre une visibilité complète sur tous les emails sortants envoyés depuis vos domaines de confiance, y compris par des tiers. Vous avez accès à des outils puissants ainsi qu'à des consultants experts qui vous guideront à chaque étape de votre déploiement de l'authentification des emails. Vous pouvez ainsi assurer votre conformité DMARC et empêcher les cybercriminels d'usurper vos domaines.

Notre protection s'étend au-delà des emails générés par les utilisateurs de sorte à inclure un environnement dédié sécurisé pour relayer les messages générés par les applications ainsi que les emails envoyés par des fournisseurs SaaS tiers en votre nom.

Dans le cas de menaces émanant de fournisseurs, Proofpoint Prime protège vos collaborateurs contre le risque d'exploitation par des cybercriminels utilisant des comptes tiers compromis. Il identifie les activités suspectes provenant de comptes fournisseurs et applique des protections adaptatives, telles que des indicateurs d'alerte et l'isolation des URL, afin de réduire les risques sans perturber les communications d'entreprise légitimes.

Proofpoint Prime propose également des fonctionnalités avancées de détection de domaines similaires. Il surveille dynamiquement Internet afin d'identifier les domaines très similaires au vôtre. Il fournit en outre des informations détaillées sur leur enregistrement ainsi que sur toute utilisation abusive potentielle.

Nous ne nous arrêtons pas à la détection. Nous pouvons mettre hors service les URL et domaines malveillants en votre nom grâce aux relations étroites que nous entretenons avec des bureaux d'enregistrement, des hébergeurs et des fournisseurs de domaines de premier niveau. Nos professionnels gèrent le processus de bout en bout, afin que vos équipes puissent se concentrer sur votre cœur de métier.

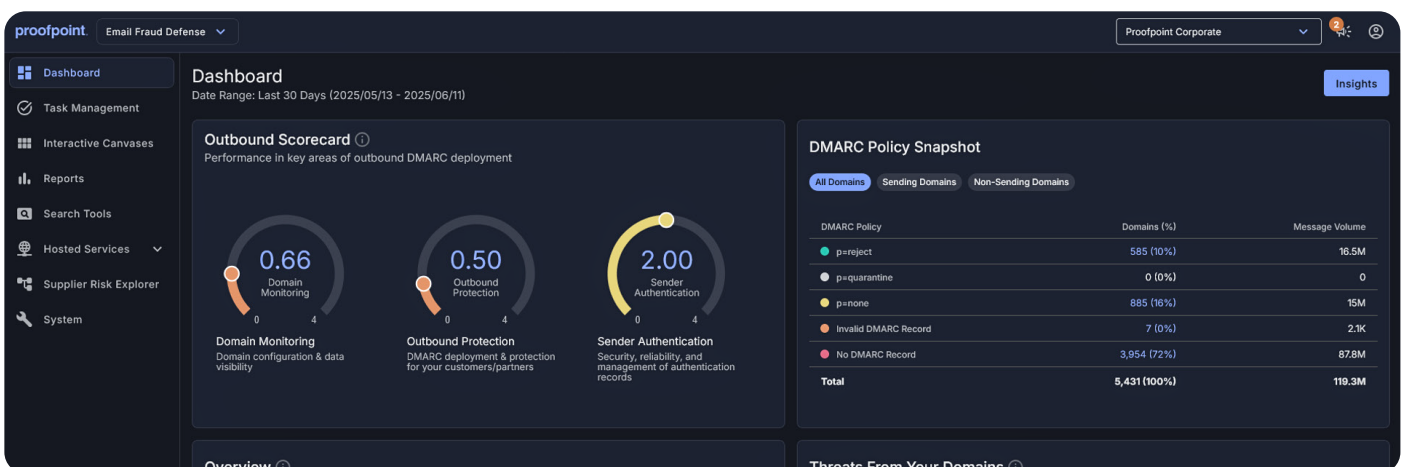


Figure 3. Proofpoint Collaboration Security Prime offre une visibilité sur les menaces d'usurpation d'identité, telles que l'usurpation de domaines et l'utilisation de domaines similaires à des fins malveillantes.

Renforcement de la résilience des utilisateurs grâce à des conseils basés sur les risques

À mesure que le travail devient plus collaboratif et dynamique, une plus grande résilience des collaborateurs face aux cyberattaques est essentielle. Cela nécessite d'aller au-delà d'une formation axée sur la conformité pour englober la gestion des risques liés aux utilisateurs – une formation en temps réel qui reflète la manière dont les utilisateurs travaillent et les véritables risques auxquels ils sont confrontés.

Proofpoint Collaboration Security Prime renforce la résilience des utilisateurs de manière systématique, non pas via une formation ponctuelle, mais par le biais d'un cycle continu lié aux risques réels.

Tout commence par le ciblage. Le Human Resilience Workbench capte les signaux de comportement et de risque de toute la plate-forme, identifiant automatiquement les utilisateurs à haut risque, les nouvelles recrues et les collaborateurs qui se laissent le plus piéger afin que les équipes de sécurité puissent concentrer leur attention là où cela compte le plus.

À partir de là, Proofpoint Prime encourage des comportements plus sûrs au moment où le risque est le plus élevé. Grâce au système ThreatFlip optimisé par l'IA, il transforme les vraies menaces actives en simulations instantanées en un clic, montrant aux collaborateurs à quoi ressemble exactement une attaque dès qu'ils y sont confrontés, et non plusieurs semaines plus tard dans un module de formation générique.

Enfin, Proofpoint Prime prouve l'impact. Les scores de risque et les analyses comparatives offrent aux administrateurs une visibilité claire sur les domaines où les comportements s'améliorent et ceux où subsistent des lacunes. Les entreprises qui adoptent cette approche enregistrent 40 % de clics en moins sur des liens malveillants réels dans les six mois suivant le déploiement, preuve que la résilience, et non la sensibilisation seule, est ce qui génère un changement durable.

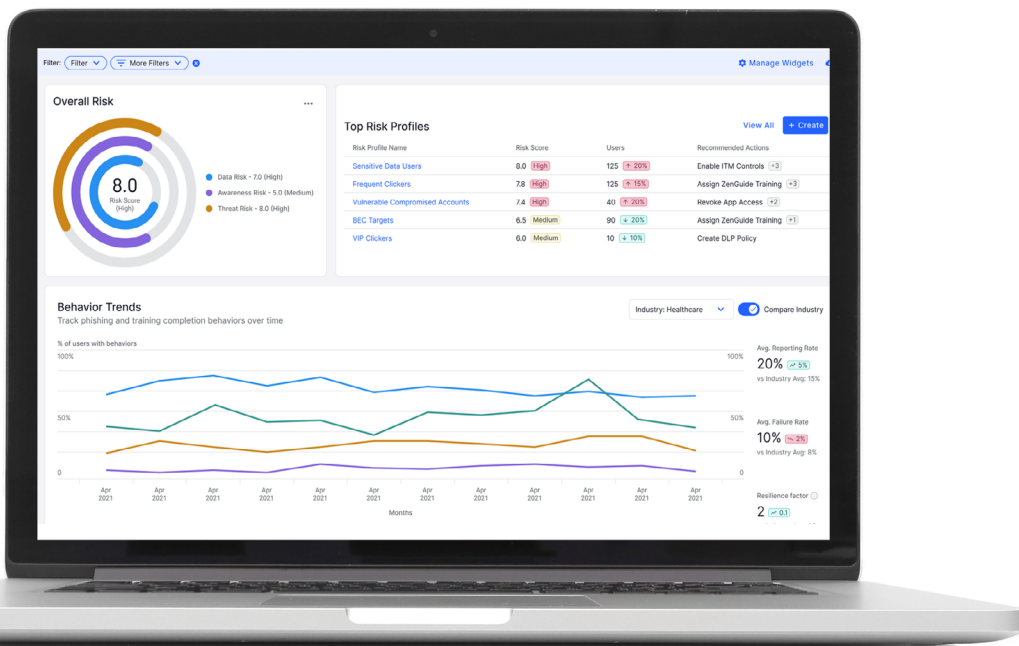


Figure 4. Proofpoint Collaboration Security Prime offre une visibilité sur le comportement réel des utilisateurs, ce qui permet de proposer des formations ciblées et basées sur les risques.

Simplification des opérations de sécurité

À mesure que les menaces s'étendent au-delà des emails pour s'attaquer aux outils de collaboration, aux plates-formes cloud et aux écosystèmes des fournisseurs, les équipes de sécurité subissent des pressions afin de faire toujours plus avec moins. Dans un tel contexte, les solutions ponctuelles déconnectées ne leur facilitent pas la tâche. Non seulement elles augmentent la complexité, mais elles ralentissent également les temps de réponse et augmentent les coûts opérationnels. Tout cela complique singulièrement la réduction des risques à grande échelle.

Proofpoint Collaboration Security Prime simplifie les opérations de sécurité en unifiant la détection et l'investigation des menaces, et en automatisant les workflows et la réponse. Grâce à des intégrations natives, le Threat Protection Workbench est en mesure de rassembler les informations en matière de détection et les analyses détaillées des attaques provenant des plates-formes de messagerie électronique, de messagerie instantanée et de collaboration, des comptes cloud et des écosystèmes de fournisseurs. Les équipes peuvent ainsi enquêter sur les incidents et prendre des mesures décisives – le tout à partir d'un environnement de travail unifié pour une efficacité maximale.

Proofpoint Prime aide également les équipes à établir les priorités de manière efficace. La Threat Interaction Map corréle les menaces et les événements de sécurité sur l'ensemble des points de contrôle – et fournit une carte visuelle des voies d'attaque. Les analystes peuvent ainsi identifier rapidement les incidents les plus critiques. En parallèle, elle inspecte automatiquement les messages signalés par les utilisateurs, neutralise le contenu malveillant et fournit des commentaires aux utilisateurs. Cela permet de réduire les interventions manuelles et de renforcer les comportements sûrs des utilisateurs.

Le résultat ? Une réponse plus rapide et une complexité opérationnelle réduite. Votre équipe de sécurité peut en outre faire plus avec moins, sans sacrifier la protection.

Choix du niveau adéquat de protection

Proofpoint Collaboration Security Prime se décline en plusieurs niveaux, ce qui vous permet de choisir une protection en fonction du profil de risque et des besoins opérationnels de votre entreprise. Chaque niveau repose sur le précédent.

La couverture s'étend des menaces email de base aux canaux de collaboration, en passant par les compromissions de comptes, la réduction des risques liés aux personnes et la protection avancée de la marque.

Découvrez les fonctionnalités disponibles sur la page suivante.



Visitez le site **proofpoint.com/fr** pour en savoir plus

À propos de Proofpoint. Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et en toute confiance. Pour en savoir plus, consultez le site proofpoint.com/fr.

Suivez-nous : [LinkedIn](#)

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.

Tous les niveaux de Proofpoint Collaboration Security sont disponibles aussi bien pour des déploiements SEG que pour des déploiements API. La disponibilité des fonctionnalités peut varier selon le modèle de déploiement.

	Fonctionnalités disponibles	Core Email Protection	Collaboration Security Tier 2	Collaboration Security Tier 3	Collaboration Security Prime
Protection de la messagerie électronique	Protection contre les attaques BEC, le phishing, le phishing de rappel et les malwares	✓	✓	✓	✓
	Pile de détection multicouche optimisée par Nexus AI	✓	✓	✓	✓
	Données inégalées sur les menaces provenant de plus de 2,8 millions de clients	✓	✓	✓	✓
	Sandboxing des pièces jointes et des URL	✓	✓	✓	✓
	Réécriture des URL et sandboxing au moment du clic	SEG	SEG	SEG	SEG
	Isolation des clics suspects sur des URL réécrites	VAP*	Tous les utilisateurs*	Tous les utilisateurs*	Tous les utilisateurs*
	Antispam et détection du graymail	✓	✓	✓	✓
	Affichage d'avertissements contextuels en cas d'emails suspects	✓	✓	✓	✓
	Outils adaptatifs d'intégrité de la messagerie électronique avec autoapprentissage en fonction du comportement des utilisateurs	✓	✓	✓	✓
	Règles de routage des emails configurables	SEG	SEG	SEG	SEG
	Neutralisation automatisée des messages	✓	✓	✓	✓
	Automatisation de la boîte email de signalement d'abus	✓	✓	✓	✓
Protection contre les menaces multicanales et en plusieurs phases	Personnes très attaquées (VAP)™, cybercriminels et threat intelligence mondiale	✓	✓	✓	✓
	Détection et correction des comptes cloud compromis		✓	✓	✓
	Blocage des URL malveillantes envoyées via des applications de messagerie instantanée et de collaboration		✓	✓	✓
	Détection de l'utilisation abusive de mots de passe d'entreprise sur des sites Web à risque ou non approuvés		✓	✓	✓
Résilience humaine et sensibilisation à la sécurité	Protection contre les comptes fournisseurs compromis		✓	✓	✓
	Automatisation des formations basées sur le niveau de risque			✓	✓
	Renforcement de la sensibilisation des collaborateurs au moyen de simulations basées sur des menaces réelles			✓	✓
	Conversion des menaces actives en simulations sûres			✓	✓
Protection contre l'usurpation d'identité	Détection et priorisation des utilisateurs à risque en fonction des comportements, des données télémétriques sur les menaces et des rôles			✓	✓
	Prévention des usurpations de marque via l'authentification des emails				✓
	Détection et neutralisation des domaines similaires malveillants				✓
	Relais sécurisé des emails générés par des applications (250 Go)				✓

SEG = Déploiement d'une passerelle de messagerie sécurisée uniquement

* = Disponible uniquement pour les déploiements SEG.