proofpoint.

FICHE SOLUTION

Proofpoint Collaboration Security Prime

Protection contre les attaques optimisées par l'IA ciblant la messagerie électronique

Principaux atouts

- Bloque le plus large éventail de menaces avec une précision de 99,999 %.
- Étend la protection des utilisateurs par email et sur d'autres canaux
- Renforce la résilience des utilisateurs grâce à des informations et à des conseils basés sur les risques
- Réduit l'impact des compromissions de comptes internes et fournisseurs.
- Simplifie les opérations grâce à une plate-forme unifiée qui automatise les workflows

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 l'espace de travail agentique.

Présentation

À mesure que les entreprises entrent dans l'ère agentique, elles adoptent des outils et des assistants optimisés par l'IA pour aider leurs collaborateurs à travailler plus efficacement. Ces agents d'IA deviennent une composante de la main-d'œuvre étendue, interagissant avec les collaborateurs, les applications et d'autres agents à travers les emails, les plates-formes de messagerie, les applications cloud, et bien plus encore. À mesure que l'espace de travail s'étend, la surface d'attaque fait de même, et les cybercriminels n'ont pas tardé à exploiter ces canaux de communication de confiance.

En réponse, 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 de l'environnement de travail agentique.

Vous pouvez ainsi :

- Vous protéger contre des attaques multicanales en plusieurs phases avec une précision inégalée
- Réduire l'impact des compromissions de comptes des collaborateurs et des fournisseurs
- Sécuriser les communications professionnelles de confiance avec les fournisseurs, les partenaires et les clients
- Renforcer la résilience humaine grâce à des formations ciblées basées sur les risques liés aux utilisateurs
- Rationaliser les opérations de sécurité grâce à l'automatisation

Protection des personnes sur tous les canaux de collaboration, notamment l'email

À mesure que la migration vers des environnements de travail plus connectés et assistés par l'IA se poursuit, Proofpoint Collaboration Security Prime protège les collaborateurs où qu'ils travaillent. Il bloque les attaques multicanales par email ainsi que via les outils de collaboration et de messagerie tels que Microsoft Teams, Slack, les réseaux sociaux et les applications cloud, et ce sans perturber les méthodes de travail.

Proofpoint Prime protège les collaborateurs dans cet espace de travail étendu contre un large éventail de menaces, y compris :

- Phishing avancé
- Piratage de la messagerie en entreprise (BEC, Business Email Compromise)
- Attaques par téléphone (TOAD)
- Envoi en masse d'emails
- Ransomwares
- Prise de contrôle de comptes
- Attaques générées par l'IA et techniques d'exploitation de l'IA, telles que l'injection d'invites

De plus, il arrête les attaques à tous les stades du cycle de vie des menaces : avant la remise, après la remise, au moment du clic et lors de la connexion.

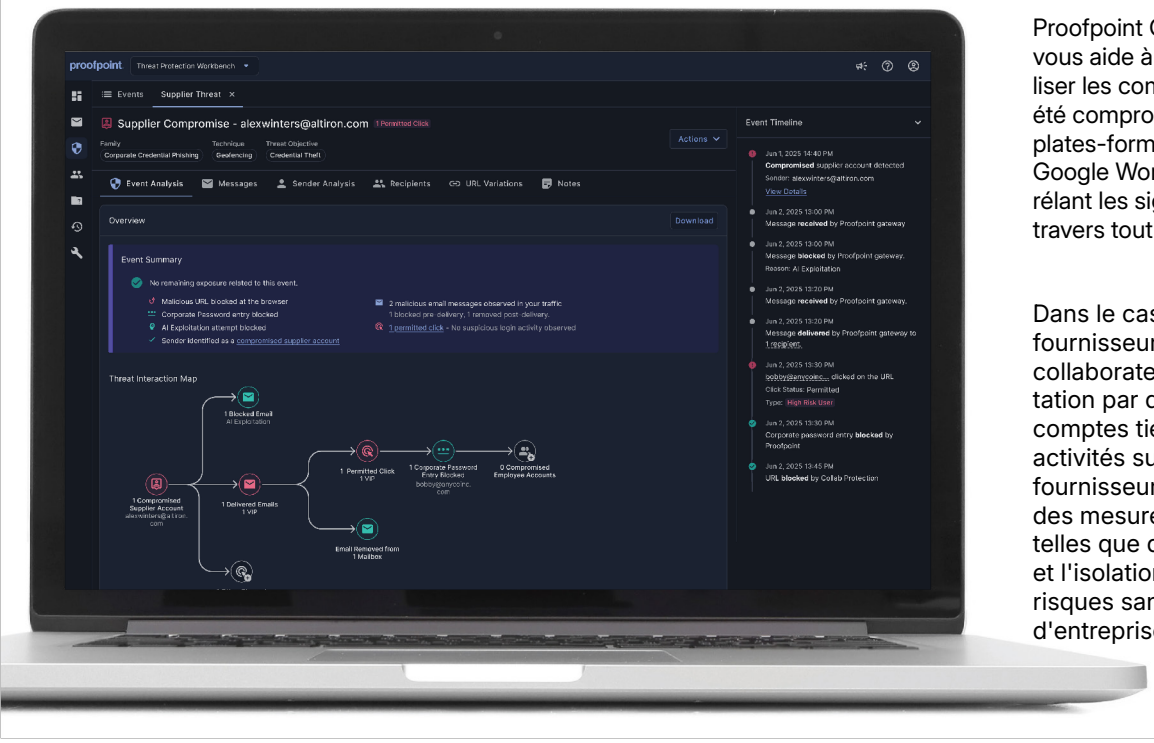

Figure 1. Proofpoint Collaboration Security Prime arrête et corrèle les menaces au niveau des emails, des outils de messagerie et de collaboration, du cloud et des canaux des fournisseurs.

Optimisé par la technologie Proofpoint Nexus® AI, Proofpoint Prime offre une protection inégalée contre les menaces avec une efficacité de 99,999 %. Pour ce faire, il allie threat intelligence riche, modèles de langage avancés, graphiques relationnels, apprentissage automatique, analyse comportementale et vision par ordinateur. Toutes ces technologies fonctionnent de concert pour détecter et bloquer les menaces avant qu'elles ne provoquent des dégâts.

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.

Protection contre la compromission de

Les cybercriminels utilisent des identités compromises pour accéder à des comptes légitimes et lancer des attaques en plusieurs phases. Ils exploitent les comptes compromis de vos collaborateurs et de vos fournisseurs de confiance. Dans un espace de travail guidé par la collaboration et assisté par des agents, il est essentiel de réduire au minimum l'impact de ces menaces.

Proofpoint Collaboration Security Prime vous aide à détecter, investiguer et neutraliser les comptes de collaborateurs qui ont été compromis. Il intervient sur diverses plates-formes — telles que Microsoft 365, Google Workspace, Okta, etc. —en corrélant les signaux d'identité et d'activité à travers tout l'écosystème Proofpoint.

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 émanant de comptes fournisseurs. Il met en outre en œuvre des mesures de protection adaptatives — telles que des indicateurs d'avertissement et l'isolation des URL — pour réduire les risques sans perturber les communications d'entreprise légitimes.

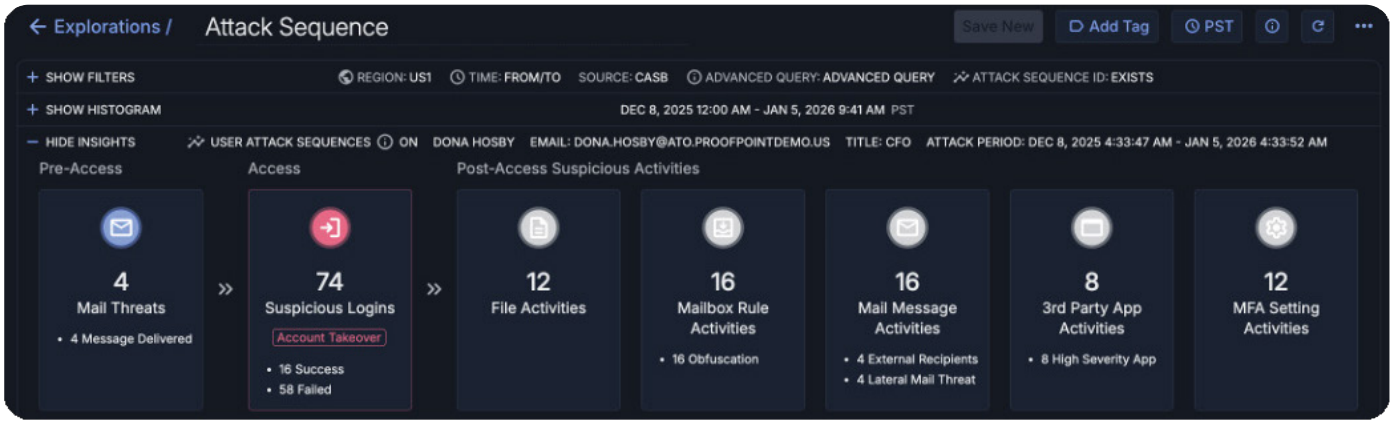

Figure 2. Proofpoint Collaboration Security Prime offre une visibilité sur les séquences d'attaque et automa-

Protection de vos communications d'entreprise de confiance

Les cyberpirates emploient souvent des tactiques d'usurpation d'identité pour s'immiscer dans des communications d'entreprise de confiance. L'usurpation de l'identité de votre entreprise — que ce soit par le biais de l'usurpation directe de domaines ou de l'enregistrement de domaines imitant les vôtres — met en danger vos collaborateurs, clients et partenaires. Elle peut en outre être très dommageable pour votre marque.

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.

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.

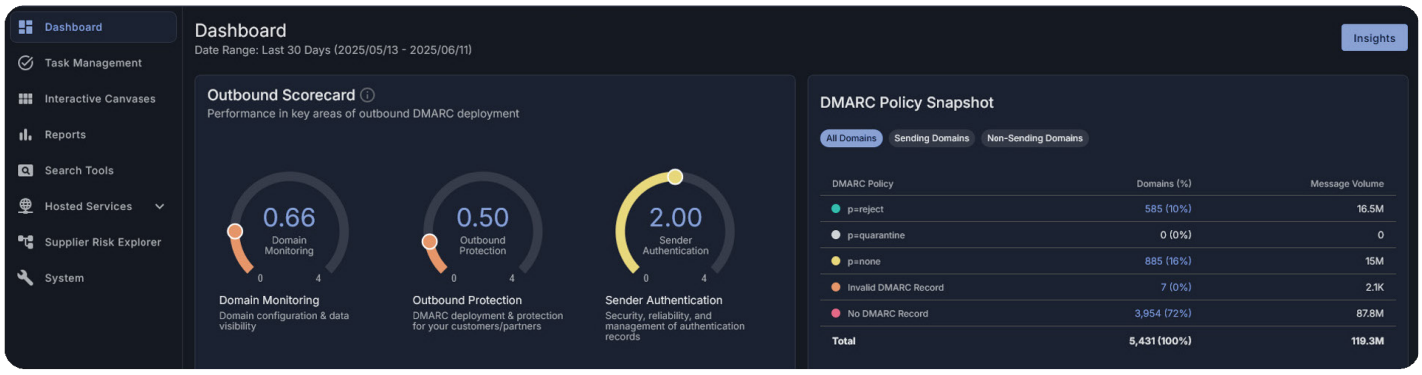

Figure 3. Proofpoint Collaboration Security Prime offre une visibilité sur les menaces d'usurpation d'identité, telles que l'usurpation de domaines et l'utilisation de domaines similaires à des fins malveillantes.

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 aide votre entreprise à effectuer ce changement de cap en encourageant vos collaborateurs à faire des choix plus sûrs. Il propose une formation automatisée, ciblée et basée sur les risques liés aux personnes, qui est adaptée au comportement, au rôle, à l'exposition aux attaques et au profil de risque unique de chaque utilisateur. Grâce à l'IA, Proofpoint Prime convertit les menaces du monde réel en simulations instantanées d'un simple clic. Les formations sont ainsi alignées sur les signaux de risque actifs de façon à amener des changements de comportement mesurables et durables.

Non seulement les modules de formation s'adaptent aux signaux de risque individuels, mais ils sont proposés dans le cadre d'expériences attrayantes et gamifiées. Cela motive les utilisateurs à y participer, et l'adoption de comportements plus sûrs est ainsi renforcée au fil du temps. Les apprenants peuvent suivre facilement leurs progrès grâce à un tableau de bord intuitif, qui les tient informés et veille à ce qu'ils assument leurs responsabilités.

En parallèle, les administrateurs peuvent facilement adapter les programmes en fonction des priorités de l'entreprise en matière de risques. Les résultats parlent d'eux-mêmes : engagement plus élevé, changement de comportement mesurable et culture de la sécurité plus forte au sein de votre entreprise.

Figure 4. Proofpoint Collaboration Security Prime offre une visibilité sur le comportement réel des utilisateurs, ce qui permet de propo-

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 espace de travail unifié pour une efficacité maximale.

Proofpoint Prime aide également les équipes à établir les priorités de manière efficace. La Threat Interaction Map corrèle les menaces et les événements de sécurité sur l'ensemble des points de contrôle — et fournit une carte visuelle des voies d'attaque. Cela permet aux analystes d'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 la compromission de comptes, la réduction des risques liés aux personnes et la protection avancée de la marque.

Découvrez les fonctionnalités disponibles sur la page suivante.

proofpoint.

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 confiance. Pour en savoir plus, consultez le site www.proofpoint.com/fr.

Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →

	Fonctionnalités disponibles	Proofpoint Core Email Protection	Proofpoint Collaboration Security Tier 2	Proofpoint Collaboration Security Tier 3	Proofpoint Collaboration Security Prime
Protection de la messagerie	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 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	●	●	●	●
	Personnes très attaquées (VAP)™, cybercriminels et theat intelligence mondiale	●	●	●	●
Protection contre les menaces multicanales et en plusieurs phases	Détection et correction des comptes cloud compromis		●	●	●
	Blocage des URL malveillantes envoyées via des applications de messagerie et de collaboration		●	●	●
	Protection contre les comptes fournisseurs compromis		●	●	●
Résilience humaine et sensibilisation à la sécurité informatique	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			●	●

SEG = déploiement d'une passerelle de mes-

***** Disponible uniquement pour les