proofpoint.

GUIDE DE PLANIFICATION

Transition d'une passerelle de messagerie héritée à Proofpoint

Les passerelles de messagerie sécurisées (SEG) héritées ont été conçues pour bloquer le spam et les malwares connus. Toutefois, à l'heure actuelle, les acteurs malveillants recourent à des menaces sophistiquées et à des techniques multivectorielles telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise), la prise de contrôle de comptes (ATO, Account Takeover), le phishing par code QR et le contournement MFA. Autant de menaces que ces outils d'ancienne génération n'étaient pas programmés pour contrer. Dès lors, lorsque vous utilisez une passerelle héritée de ce type, votre entreprise court un risque accru de subir une compromission et de voir ses coûts opérationnels flamber.

Si vous souhaitez adopter Proofpoint pour renforcer votre sécurité, ce guide de planification vous aidera à préparer votre parcours de migration. Il est conçu pour les clients Barracuda, Cisco (IronPort), Forcepoint (Websense), Symantec Email Security.cloud (MessageLabs), Trellix (FireEye/McAfee) et Trend Micro.

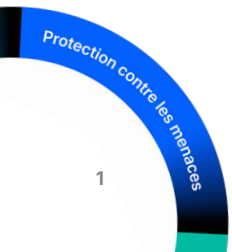
Ces instructions étape par étape vous aideront à évaluer l'efficacité de votre passerelle héritée, à en mesurer les coûts et à établir un calendrier pour la migration. Proofpoint propose des options de déploiement flexibles — migration complète de la passerelle, déploiement d'API ou approche progressive — afin que vous puissiez choisir ce qui convient le mieux à votre environnement. Pour simplifier ce processus, votre équipe Proofpoint peut vous fournir des outils gratuits (évaluation rapide des risques, rapport d'écart, évaluation de la valeur ajoutée) afin que vous puissiez quantifier la réduction des risques et le retour sur investissement.

Étape 1 : Quantifier l'efficacité de votre protection actuelle

Commencez par le facteur visibilité. Mesurez l'efficacité de vos défenses actuelles (et ce qui leur échappe) afin d'établir une base de référence claire.

- Passez en revue les rapports de faux négatifs, qui se trouvent dans les journaux d'administration et les tickets SIEM/IR. Ces informations peuvent vous aider à comprendre l'ampleur et la portée des détections manquées.
- Documentez le pourcentage d'emails signalés par les utilisateurs qui ont été confirmés comme de vrais positifs, car ces données chiffrées vous aideront à quantifier le temps passé par les analystes à résoudre les faux positifs.
- Identifiez les incidents de prise de contrôle de comptes (ATO) détectés par d'autres systèmes. Citons par exemple l'exploitation abusive des règles de boîte email, les alertes liées au déplacement impossible ou à la géolocalisation, de même que le contournement de l'authentification multifacteur.
- Passez en revue les tentatives de phishing interne ou latéral détectées par d'autres systèmes ou signalées par les utilisateurs.
- Effectuez une évaluation des risques liés à la messagerie de Proofpoint. Ce service vous procurera une visibilité fondée sur les données quant aux menaces que votre passerelle existante ou votre système Microsoft 365 pourrait ne pas détecter.

Cette suite de solutions fait partie de la plate-forme Human-Centric Security de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.



Étape 2 : Calculer le coût du statu quo

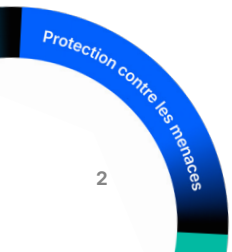
La sécurité ne se mesure pas uniquement en termes d'éléments bloqués, mais aussi en termes d'efficacité des opérations. Évaluez le temps, les efforts et le niveau de vigilance des analystes liés au tri manuel, aux faux positifs et aux workflows fragmentés afin de mettre en évidence le véritable coût du maintien de votre passerelle héritée.

- Documentez le nombre de clics et de minutes/heures qu'il faut à vos analystes pour examiner un seul incident de phishing. (Il n'est pas rare que les analystes utilisent plus de 12 clics et passent plusieurs heures à résoudre chaque incident.) Identifiez également les endroits où les retards surviennent généralement.
- Suivez les heures passées par les analystes au triage de la boîte de signalement d'abus. Calculez combien de temps les analystes passent à examiner les emails signalés par les utilisateurs chaque semaine. Déterminez également quel pourcentage de ces messages s'avère de vraies menaces par rapport aux fausses alertes.
- Calculez le temps que votre équipe passe à préparer des rapports. Notez le temps qu'il faut à votre équipe pour compiler et mettre en forme les métriques de sécurité pour élaborer des rapports destinés aux dirigeants ou au conseil d'administration. Cette tâche nécessite souvent des exportations de données manuelles et des opérations dans des feuilles de calcul.
- Dialoguez avec les analystes en sécurité et relevez leurs sujets de frustration. Quels problèmes surviennent le plus fréquemment ? À titre d'exemple : le bruit, les faux positifs et la multiplication des consoles.

Étape 3 : Choisir votre chemin de migration

Votre environnement et vos priorités évolueront, et la sécurité de votre messagerie doit faire de même. Proofpoint vous offre une flexibilité que les fournisseurs à modèle unique ne peuvent pas vous procurer. Nous nous distinguons en ce sens que nous proposons trois chemins de migration :

- **Option 1 : Renforcement de la sécurité avec une protection basée sur API.** Cette option demande peu d'efforts et a un impact élevé. Intégrez l'API Proofpoint Core Email Protection à Microsoft 365 pour une protection immédiate contre des menaces telles que le piratage de la messagerie en entreprise (BEC), la prise de contrôle de comptes (ATO) et le phishing. Ce modèle prend également en charge la transition d'une passerelle de messagerie héritée à un modèle Microsoft + Proofpoint, en assurant une protection continue pendant et après la migration.
- **Option 2 : Déploiement de l'API suivi de la migration de la passerelle.** Cette option exige un effort modéré, mais a un impact plus important. Commencez par déployer l'API Proofpoint pour obtenir des gains opérationnels rapides et réduire les risques. Effectuez ensuite une transition graduelle vers la passerelle de messagerie sécurisée Proofpoint pour disposer d'un contrôle sur le routage, répondre à l'évolution des besoins en matière de conformité ou assurer une défense multicouche avancée.
- **Option 3 : Remplacement complet de la passerelle.** Mettez complètement hors service votre passerelle de messagerie héritée et migrez vos enregistrements MX vers la solution Proofpoint pour un contrôle maximal et une protection complète de la messagerie avant livraison.



Étape 4 : Planifier la migration et lancer un projet pilote

Validez les résultats avant le déploiement complet. Un projet pilote contrôlé vous permet de tester Proofpoint parallèlement à votre passerelle existante, de confirmer les gains en termes de détection plus performante et de réponse plus rapide, et de renforcer la confiance de la direction grâce à des données probantes.

- Définissez vos critères de réussite dès le départ. Quels résultats souhaitez-vous obtenir ? Par exemple : une détection des menaces améliorée, une réduction des faux positifs, une remédiation plus rapide et la prévention de la prise de contrôle de comptes (ATO).
- Observez les améliorations potentielles de la détection en exécutant la protection de la messagerie de Proofpoint en mode silencieux.
- Déterminez si votre projet pilote offre les livrables suivants :
    - Une comparaison claire indiquant les menaces que Proofpoint a détectées et que votre passerelle de messagerie héritée a manquées
    - Un résumé intelligible des failles identifiées dans la protection offerte par la passerelle
    - Un rapport sur la valeur ajoutée qui quantifie, en euros, le gain de temps pour votre équipe et la réduction des risques pour l'entreprise

Étape 5 : Établir votre calendrier

Planifiez une transition progressive tenant compte des cycles de renouvellement, de votre dotation en personnel et de votre tolérance au risque. Avec le soutien à la migration de Proofpoint, vous pouvez moderniser la protection sans interruption de service.

- Créez un plan en trois phases :
    1. Projet pilote
    2. Exécution en parallèle
    3. Basculement final
- Passez en revue votre calendrier de renouvellement des licences et vos cycles budgétaires. Si nécessaire, recherchez des opportunités d'achat de contrat.
- Exécutez votre ancien système en parallèle comme mesure de sécurité supplémentaire jusqu'à ce que le nouveau déploiement ait reçu l'aval de la direction.
- Utilisez les Services Premium Proofpoint pour bénéficier d'une expérience de migration haut de gamme. Nos équipes des services Proofpoint Advisory et Applied fournissent une expertise pratique pour optimiser les configurations, accélérer le déploiement et assurer une protection continue pendant votre transition.

Conclusion

Lorsque vous adoptez Proofpoint, nous vous soutenons lors de la phrase de transition. Ainsi, nous fournissons des guides de migration, des modèles de projets pilotes et des témoignages de réussite client pour vous accompagner dans votre démarche. Que vous ayez opté pour un déploiement initial d'API, pour une transition progressive ou pour un remplacement complet de votre passerelle de messagerie héritée, nous vous aidons à migrer en toute confiance et à obtenir rapidement des résultats mesurables.

Pourquoi choisir Proofpoint ?

À propos de Proofpoint

Protection des personnes

3,4 Mrd
d'emails analysés chaque année

+1,4 Mrd
de SMS/MMS analysés chaque année

124 M
d'attaques BEC bloquées chaque mois

> 183 M
de simulations d'attaques de phishing chaque année

0,8 Mrd
de pièces jointes analysées chaque année

21 Mrd
d'URL analysées chaque année

177 M
d'attaques par téléphone (TOAD) bloquées chaque année

Adoption par le marché

+2,7 M
clients

+150
FAI et opérateurs mobiles mondiaux

> 80 %
des entreprises du F100 protégées par Proofpoint

57 %
des entreprises du F100 utilisent la DLP Proofpoint

> 63 %
des entreprises du F1000 protégées par Proofpoint

proofpoint.

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 →