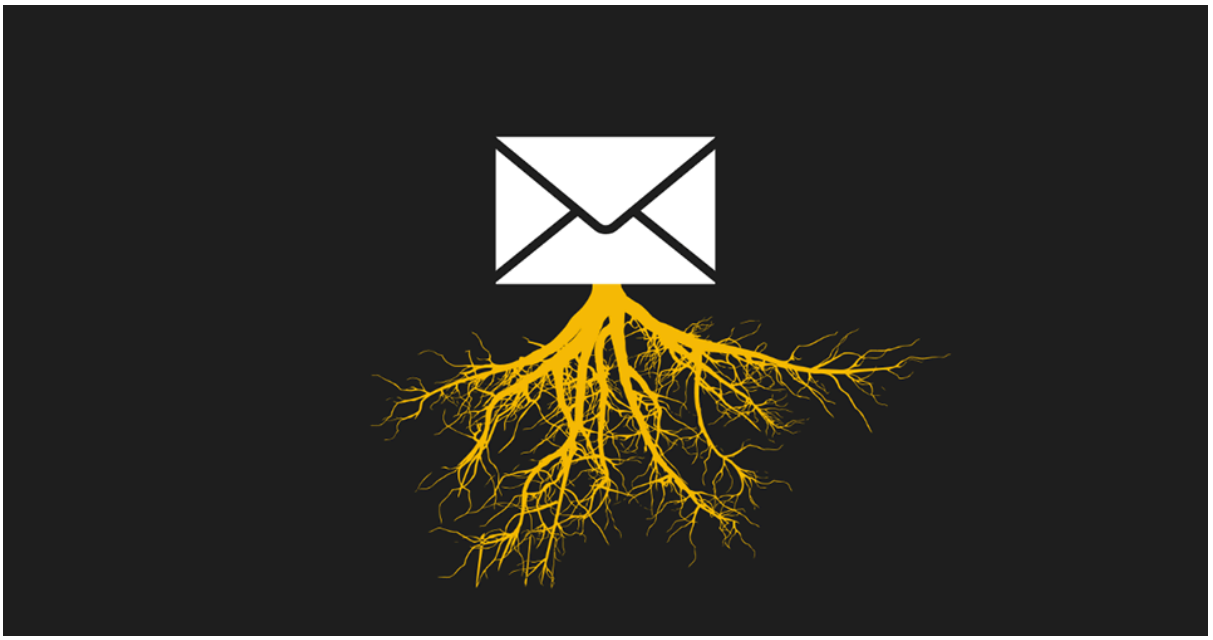
Rapport SOC-SIEM 5 décembre 2024



Par Fayçal ZEROUALI & Abdel-Malik FOFANA

Introduction à la Sécurité des Emails

La sécurité des emails est devenue un enjeu majeur pour les entreprises modernes, car les emails représentent l'un des vecteurs d'attaque les plus courants et les plus efficaces pour les cybercriminels. Par exemple, une étude récente a montré que 90 % des attaques de cybercriminalité débutent par un email de phishing. Malgré les avancées technologiques dans le domaine de la cybersécurité, les emails restent une porte d'entrée privilégiée pour des attaques telles que le phishing, les ransomwares ou encore les attaques par compromission de comptes professionnels (BEC). En 2023, une entreprise de finance a perdu des millions de dollars après qu'un employé ait cliqué sur un lien malveillant dans un email, permettant ainsi aux attaquants de dérober des informations sensibles. Ces attaques peuvent entraîner des fuites de données sensibles, des pertes financières considérables et des dommages à la réputation de l'entreprise.

Dans ce contexte, mettre en place une solution de sécurité des emails robuste est essentiel pour protéger les informations critiques. Par exemple, une solution efficace pourra bloquer les tentatives de phishing avant qu'elles n'atteignent l'utilisateur, comme l'illustre l'exemple d'une grande entreprise de vente en ligne qui a évité une attaque par ransomware grâce à une solution de filtrage d'emails avancée. Une bonne solution de sécurité des emails permet non seulement de bloquer les attaques avant qu'elles n'atteignent les utilisateurs, mais aussi de réduire les risques liés aux erreurs humaines, souvent responsables de l'ouverture de pièces jointes ou de liens malveillants. En investissant dans la sécurité des emails, les entreprises renforcent leur défense contre l'une des failles les plus exploitables de leur infrastructure informatique.

Tableau récapitulatif

Critères	Cofense	Microsoft Defender	CheckPoint	Proofpoint	Mimecast
Protection anti-spam	9/10	8/10	7/10	9/10	9/10
Détection des malwares	8/10	9/10	9/10	10/10	8/10
Anti-phishing avancé	9/10	9/10	8/10	10/10	9/10
Chiffrement des emails	7/10	8/10	8/10	9/10	8/10
Protection BEC	9/10	8/10	8/10	10/10	9/10
Gestion des données (DLP)	8/10	9/10	7/10	10/10	8/10
Intégration SIEM/EDR	8/10	10/10	8/10	9/10	9/10

Facilité de déploiement	7/10	9/10	8/10	8/10	9/10
Modèle de licence	SaaS	SaaS/On-premise	SaaS	SaaS	SaaS

Présentation de Cofense

Cofense, anciennement connu sous le nom de PhishMe, est une entreprise spécialisée dans la sécurité des emails et la lutte contre le phishing. Fondée en 2011, elle appartient actuellement à un consortium de sociétés de capital-investissement dirigé par *Pamplona Capital Management*. Cofense se distingue par sa capacité à combiner l'intelligence humaine et les technologies avancées pour prévenir, détecter et répondre aux menaces par email.

Explication des notations

Nous avons attribué des notes sur 10 pour évaluer les principales fonctionnalités de Cofense :

- **Protection anti-spam (9/10)** : Cofense offre une excellente détection des emails malveillants grâce à des algorithmes basés sur l'analyse comportementale. Cependant, certains utilisateurs signalent des ajustements nécessaires pour réduire les faux positifs.
- **Détection des malwares (8/10)** : L'intégration d'une analyse approfondie avec des solutions sandbox est solide, mais elle pourrait être plus performante face à certaines menaces polymorphes.
- **Anti-phishing avancé (9/10)** : Cofense excelle dans la détection des campagnes de phishing sophistiquées, grâce à sa capacité à recueillir et partager des rapports en temps réel à partir de son réseau mondial.
- **Chiffrement des emails (7/10)** : Bien que la solution prenne en charge le chiffrement, elle repose souvent sur des intégrations externes, ce qui peut limiter son adoption directe.
- **Protection contre les BEC (9/10)** : L'approche comportementale de Cofense lui permet d'identifier efficacement les tentatives de compromis de comptes professionnels.
- **Gestion des données (DLP) (8/10)** : Cofense propose des fonctionnalités de DLP efficaces, mais celles-ci nécessitent une configuration avancée pour maximiser leur efficacité.
- **Intégration SIEM/EDR (8/10)** : Cofense s'intègre bien avec les solutions SIEM et EDR, bien que certaines options d'intégration nécessitent un effort technique supplémentaire.

- **Facilité de déploiement (7/10)** : La mise en œuvre initiale de Cofense peut être complexe pour les petites organisations sans ressources spécialisées.

Avantages de Cofense

- **Approche collaborative** : Cofense utilise les rapports de phishing envoyés par les employés pour affiner en continu ses algorithmes.
- **Réactivité** : Les réponses aux menaces sont rapides, grâce à des systèmes automatisés et des analyses humaines.
- **Adaptabilité** : Les solutions peuvent s'intégrer à des environnements variés, y compris ceux des grandes entreprises.

Inconvénients de Cofense

- **Coût élevé** : Les solutions Cofense sont souvent plus chères que d'autres alternatives, ce qui peut dissuader les petites structures.
- **Courbe d'apprentissage** : La formation des équipes et la configuration initiale demandent un investissement de temps significatif.
- **Dépendance externe** : Certaines fonctionnalités avancées nécessitent des outils complémentaires, comme pour le chiffrement.

Présentation de Microsoft Defender

Microsoft Defender for Office 365 est une solution de sécurité des emails développée par Microsoft, une entreprise leader dans le domaine des technologies et des logiciels. Créée en 1975 par Bill Gates et Paul Allen, Microsoft est connue pour son écosystème complet, comprenant des solutions Cloud, des logiciels bureautiques, et des outils de cybersécurité. Microsoft Defender for Office 365 s'intègre naturellement dans l'écosystème Microsoft 365, offrant une protection avancée contre les menaces liées aux emails, telles que le phishing, les ransomwares, et les malwares, tout en profitant de l'intelligence artificielle et de l'apprentissage automatique.

Explication des notations

Nous avons attribué des notes sur 10 pour évaluer les fonctionnalités principales de Microsoft Defender for Office 365 :

- **Protection anti-spam (8/10)** : La solution offre un excellent filtrage des spams et des emails indésirables. Cependant, elle peut nécessiter un ajustement manuel pour certains scénarios spécifiques, notamment en environnement hybride.
- **Détection des malwares (9/10)** : Grâce à son intégration avec Microsoft Threat Intelligence, Defender détecte efficacement les malwares, y compris les attaques zero-day, tout en bénéficiant d'un sandboxing avancé.

- **Anti-phishing avancé (9/10)** : L'analyse comportementale et l'intelligence artificielle permettent d'identifier des campagnes de phishing ciblées. Les alertes en temps réel renforcent la sécurité.
- **Chiffrement des emails (8/10)** : Le chiffrement intégré est performant et facile à activer via Microsoft 365. Toutefois, il peut être limité pour des communications interorganisations nécessitant des normes spécifiques.
- **Protection BEC (8/10)** : Microsoft Defender offre une bonne protection contre les compromissions de comptes professionnels en détectant les comportements inhabituels et les modèles de langage frauduleux.
- **Gestion des données (DLP) (9/10)** : Les politiques DLP sont riches et facilement configurables dans l'interface Microsoft Compliance Center, avec une couverture étendue des réglementations comme RGPD ou HIPAA.
- **Intégration SIEM/EDR (10/10)** : La solution s'intègre parfaitement avec Sentinel, le SIEM natif de Microsoft, ainsi qu'avec d'autres outils EDR comme Defender for Endpoint.
- **Facilité de déploiement (9/10)** : Pour les organisations utilisant déjà l'écosystème Microsoft 365, le déploiement est rapide et simplifié, bien que des ajustements soient parfois nécessaires pour des environnements non Microsoft.

Avantages de Microsoft Defender

- **Intégration native** : S'intègre parfaitement avec les autres services de Microsoft 365, offrant une expérience utilisateur cohérente.
- **Intelligence avancée** : Bénéficie de la base de données mondiale de Microsoft Threat Intelligence, assurant une détection proactive des menaces.
- **Efficacité en temps réel** : Les mises à jour automatiques et les analyses en temps réel garantissent une protection constante contre les menaces émergentes.

Inconvénients de Microsoft Defender

- **Dépendance à l'écosystème Microsoft** : Les organisations utilisant des solutions non-Microsoft pourraient trouver les intégrations limitées ou nécessitant des efforts supplémentaires.
- **Coût additionnel** : Certaines fonctionnalités avancées requièrent des licences Microsoft 365 Premium, ce qui peut augmenter le coût global.
- **Complexité des politiques** : Bien que la configuration soit intuitive, les politiques complexes nécessitent parfois une expertise pour maximiser leur efficacité.

Présentation de CheckPoint

CheckPoint Software Technologies, fondée en 1993 en Israël, est une entreprise reconnue mondialement pour ses solutions de cybersécurité. Pionnière dans la protection des réseaux et des infrastructures critiques, elle appartient à CheckPoint Software Technologies Ltd, une société cotée en bourse (NASDAQ: CHKP). CheckPoint est réputée pour son expertise dans

les pare-feu, la protection cloud, et les solutions de sécurité des emails, intégrant des technologies avancées comme le sandboxing et la prévention des menaces Zero-Day.

Explication des notations

Nous avons attribué des notes sur 10 pour évaluer les fonctionnalités clés de CheckPoint :

- **Protection anti-spam (7/10)** : Bien que CheckPoint offre une protection efficace contre le spam, certains utilisateurs rapportent un manque de personnalisation des règles dans des environnements complexes.
- **Détection des malwares (9/10)** : Grâce à son service ThreatCloud et son sandboxing avancé, CheckPoint excelle dans la détection des malwares, même les plus sophistiqués.
- **Anti-phishing avancé (8/10)** : Les algorithmes d'analyse contextuelle de CheckPoint permettent une détection précise des emails de phishing, bien que la gestion des faux positifs puisse être optimisée.
- **Chiffrement des emails (8/10)** : CheckPoint prend en charge les standards de chiffrement comme TLS, offrant une sécurité robuste pour les communications sensibles.
- **Protection contre les BEC (8/10)** : CheckPoint utilise des techniques d'analyse comportementale pour détecter les compromissions de comptes professionnels, avec une efficacité respectable.
- **Gestion des données (DLP) (7/10)** : Les capacités DLP sont solides, mais nécessitent une configuration avancée pour répondre aux besoins spécifiques des entreprises.
- **Intégration SIEM/EDR (8/10)** : CheckPoint s'intègre facilement avec des solutions SIEM et EDR populaires, bien que certaines options d'automatisation soient limitées.
- **Facilité de déploiement (8/10)** : La solution est relativement simple à déployer, mais peut nécessiter des ressources techniques pour une personnalisation avancée.

Avantages de CheckPoint

- **Approche globale** : CheckPoint offre une suite complète pour la protection des emails, combinée à des solutions réseau et cloud.
- **Technologies avancées** : La prévention Zero-Day et le ThreatCloud assurent une protection proactive contre les menaces émergentes.
- **Intégration fluide** : CheckPoint s'intègre bien avec d'autres outils de sécurité, facilitant une gestion centralisée.

Inconvénients de CheckPoint

- **Coût élevé** : Les solutions CheckPoint, bien que performantes, sont souvent coûteuses, ce qui peut représenter un frein pour les PME.
- **Complexité des politiques** : Les configurations avancées, notamment pour le DLP et les règles anti-spam, peuvent être complexes à mettre en œuvre sans expertise technique.
- **Support technique perfectible** : Certains utilisateurs signalent des délais dans la résolution de problèmes via le support client.

Présentation de Proofpoint

Proofpoint est une entreprise américaine fondée en 2002, spécialisée dans la sécurité des emails, la protection des données et la prévention des menaces avancées. Elle appartient à Thoma Bravo, un fonds de capital-investissement. Proofpoint est largement reconnue pour sa capacité à détecter et bloquer des menaces sophistiquées comme le phishing, le ransomware et les attaques de type BEC (Business Email Compromise). Avec une présence mondiale, elle offre des solutions robustes adaptées aux grandes entreprises et aux organisations opérant dans des secteurs sensibles comme la santé et la finance.

Explication des notations

Nous avons évalué Proofpoint sur une échelle de 10 en nous basant sur ses principales fonctionnalités :

- **Protection anti-spam (9/10)** : Proofpoint se distingue par une excellente détection des spams et des messages malveillants grâce à des algorithmes basés sur l'IA. Quelques ajustements sont parfois nécessaires pour réduire les faux positifs dans des environnements complexes.
- **Détection des malwares (10/10)** : La solution intègre une sandbox avancée, permettant d'analyser les pièces jointes suspectes en profondeur et de neutraliser les menaces polymorphes.
- **Anti-phishing avancé (10/10)** : Proofpoint excelle dans la détection des attaques de phishing ciblées, notamment grâce à son intelligence artificielle et son apprentissage automatique, qui identifient les emails usurpant des identités.
- **Chiffrement des emails (9/10)** : Le chiffrement est intégré de manière fluide, offrant une sécurité renforcée pour les communications sensibles sans nécessiter de configurations complexes.
- **Protection contre les BEC (10/10)** : Proofpoint utilise une approche comportementale pour identifier efficacement les tentatives de fraude par compromission de compte professionnel.
- **Gestion des données (DLP) (10/10)** : Ses fonctionnalités DLP sont très complètes, avec une excellente capacité à identifier et protéger les données sensibles grâce à des politiques personnalisables.
- **Intégration SIEM/EDR (9/10)** : Proofpoint s'intègre facilement avec les solutions SIEM et EDR les plus courantes, bien que certaines intégrations avancées nécessitent un travail technique supplémentaire.

- **Facilité de déploiement (8/10)** : La solution est relativement simple à déployer dans des environnements d'entreprise, mais cela peut être un défi pour les petites organisations disposant de ressources limitées.

Avantages de Proofpoint

- **Efficacité exceptionnelle** : Proofpoint offre des performances supérieures dans la détection des menaces sophistiquées, notamment les attaques ciblées et les malwares avancés.
- **Conformité réglementaire** : Idéal pour les secteurs sensibles, Proofpoint répond aux exigences des cadres légaux comme le RGPD et HIPAA.
- **Écosystème intégré** : La solution s'intègre bien avec d'autres outils de sécurité, facilitant une gestion unifiée des menaces.

Inconvénients de Proofpoint

- **Coût élevé** : Comme pour d'autres solutions haut de gamme, les prix peuvent être prohibitifs pour les petites et moyennes entreprises.
- **Complexité pour les petites structures** : Le déploiement et la gestion nécessitent des compétences techniques avancées, ce qui peut représenter une barrière pour des équipes moins expérimentées.
- **Dépendance au cloud** : Bien que flexible, la dépendance au SaaS peut poser problème pour certaines organisations nécessitant des solutions entièrement on-premise.

Présentation de Mimecast

Mimecast est une entreprise mondiale spécialisée dans la sécurité des emails et la gestion des communications en ligne. Fondée en 2003 et basée à Londres, elle se positionne comme un leader dans la prévention des menaces avancées liées aux emails. Mimecast appartient à Permira, une société de capital-investissement. Sa plateforme cloud propose des solutions complètes couvrant la sécurité des emails, la continuité des services et la gestion des archives. Elle est largement adoptée par des entreprises de toutes tailles pour protéger leurs infrastructures contre les cyberattaques.

Explication des notations

Nous avons attribué des notes sur 10 pour évaluer les principales fonctionnalités de Mimecast :

- **Protection anti-spam (9/10)** : Mimecast offre une excellente protection contre le spam grâce à des algorithmes avancés et un apprentissage automatique.

Cependant, des ajustements manuels sont parfois nécessaires pour éviter les faux positifs.

- **Détection des malwares (8/10)** : La solution intègre des outils robustes de détection et utilise des analyses dynamiques, bien que certaines menaces complexes, comme les malwares polymorphes, puissent nécessiter des couches de protection supplémentaires.
- **Anti-phishing avancé (9/10)** : Mimecast excelle dans l'identification des attaques sophistiquées, y compris les tentatives de spear-phishing, grâce à des analyses comportementales et une surveillance en temps réel.
- **Chiffrement des emails (8/10)** : Mimecast propose des options de chiffrement solides, mais leur utilisation nécessite souvent des configurations avancées, ce qui peut être un frein pour les petites équipes.
- **Protection BEC (9/10)** : La solution est efficace contre les compromissions de comptes professionnels (BEC) grâce à une détection basée sur les anomalies dans les schémas de communication.
- **Gestion des données (DLP) (8/10)** : Mimecast intègre des outils de prévention des pertes de données performants, bien que leur configuration optimale demande une expertise technique.
- **Intégration SIEM/EDR (9/10)** : Mimecast offre une intégration fluide avec les principales solutions SIEM et EDR, ce qui améliore la centralisation des données et la détection des menaces.
- **Facilité de déploiement (9/10)** : La solution SaaS est simple à déployer et bénéficie d'un excellent support client, bien que certaines entreprises puissent rencontrer des défis dans la migration initiale.

Avantages de Mimecast

- **Solution complète** : Mimecast combine sécurité des emails, continuité des services et gestion des archives sur une plateforme unique.
- **Efficacité contre les menaces ciblées** : Les technologies avancées de détection des attaques ciblées en font un choix idéal pour les entreprises exposées à des menaces complexes.
- **Simplicité d'utilisation** : L'interface utilisateur intuitive et le support technique dédié facilitent l'adoption par les équipes.

Inconvénients de Mimecast

- **Coût élevé** : Les solutions Mimecast sont premium et peuvent représenter un investissement significatif, particulièrement pour les PME.
- **Complexité de configuration avancée** : Certaines fonctionnalités, comme la gestion DLP ou le chiffrement, nécessitent une expertise technique pour une configuration optimale.
- **Dépendance cloud** : Mimecast étant basé sur une architecture SaaS, des interruptions de connexion peuvent affecter l'accès aux services.