PROTECTION MAIL

Pourquoi la protection mail
est-elle indispensable ?

L'évolution rapide du paysage numérique a profondément modifié la gestion des communications par email au sein des entreprises. Avec la prolifération des menaces sophistiquées ciblant directement les boîtes de réception, la protection des emails est devenue une priorité incontournable. Les entreprises font face à des défis croissants, notamment :

- La protection contre les **attaques ciblées** de plus en plus perfectionnées, dont le premier vecteur resteencore aujourd'hui l'email : spear phishing, fraude au président, malwares, etc.
- La sécurisation des **échanges de données sensibles** via des canaux de communication vulnérables.
- La nécessité de se conformer aux **réglementations en constante évolution**, en particulier en ce qui concerne la confidentialité des données dans les communications électroniques : ISO-27001, RGPD, etc.
- La garantie de **l'intégrité des données**, quelle que soit leur localisation, dans un environnement où les communications électroniques sont sujettes à des risques croissants de violation de la vie privée et de sécurité.

En résumé, la protection des emails est devenue une priorité absolue pour les entreprises, appelant à l'adoption de solutions de Secure Email Gateway afin d'assurer la sécurité, la confidentialité et la conformité des communications électroniques dans un environnement numérique en constante évolution et de plus en plus exposé aux menaces.

NOS SOLUTIONS DE PROTECTION MAIL

DEEP travaille avec CISCO et Hornet Security pour vous proposer une solution de protection mail.

- Cisco Secure Email Gateway (anciennement ESA)
- Cisco Secure Email Cloud Gateway (anciennement CES)
- Cisco Secure Email Threat Defense (anciennement CMD)

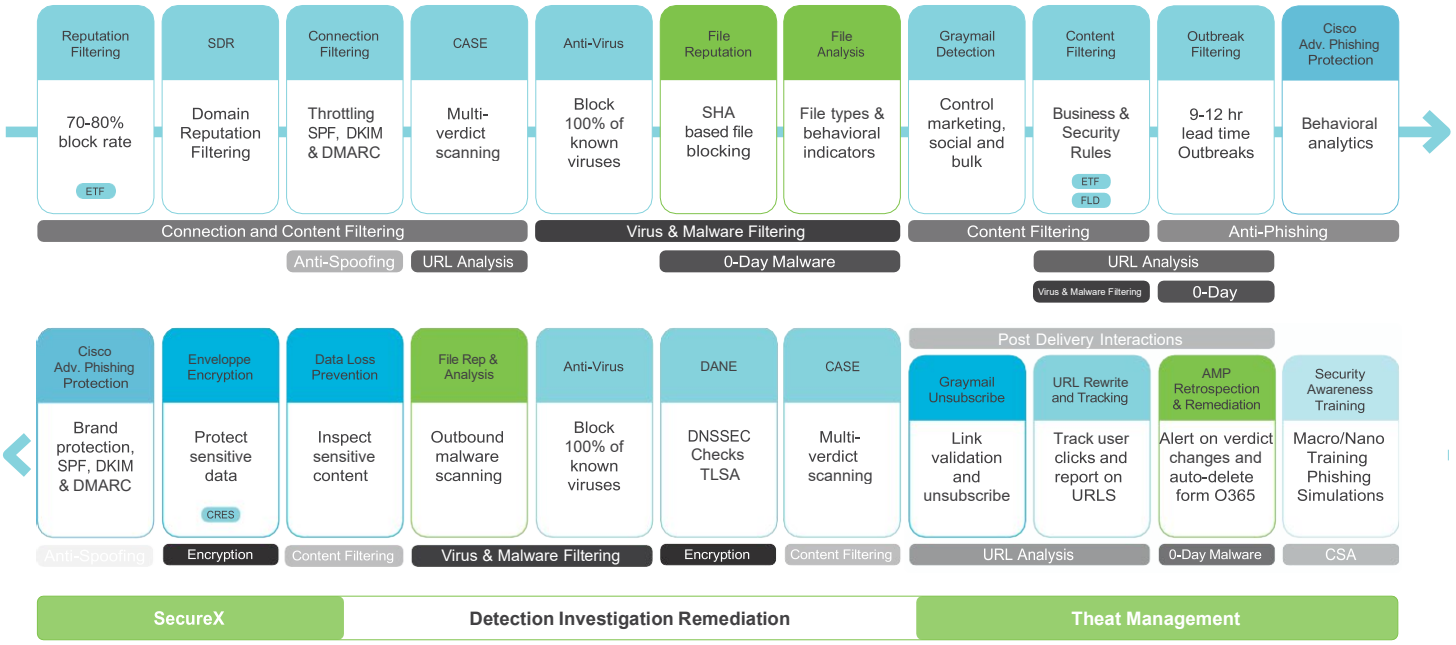
- Hornet Security : Vade pour M365 ou Google Workspace

Ces solutions offrent les fonctionnalités de sécurité suivantes :

CISCO SECURE EMAIL GATEWAY (ON-PREMISES)

- Filtrage des connexions entrantes sur base de la réputation (IP, domaine)
- Filtrage anti-spam
- Filtrage des URLs dans les mails
- Scan antivirus et analyse en sandbox
- Protection contre les menaces émergentes
- Contrôle du graymail (marketing, réseaux sociaux, etc.)
- Signature et chiffrement des mails
- Politiques de filtrage sur base de groupes d'utilisateurs
- Gestion de quarantaines
- Traçabilité de l'ensemble des mails entrants et sortants
- Génération de rapports détaillés
- Fonctionnalités avancées : DLP (Data Loss Prevention), MAR (Mailbox Auto-Remediation)

CISCO EMAIL SECURITY: STRENGTHENING THE EMAIL PIPELIN

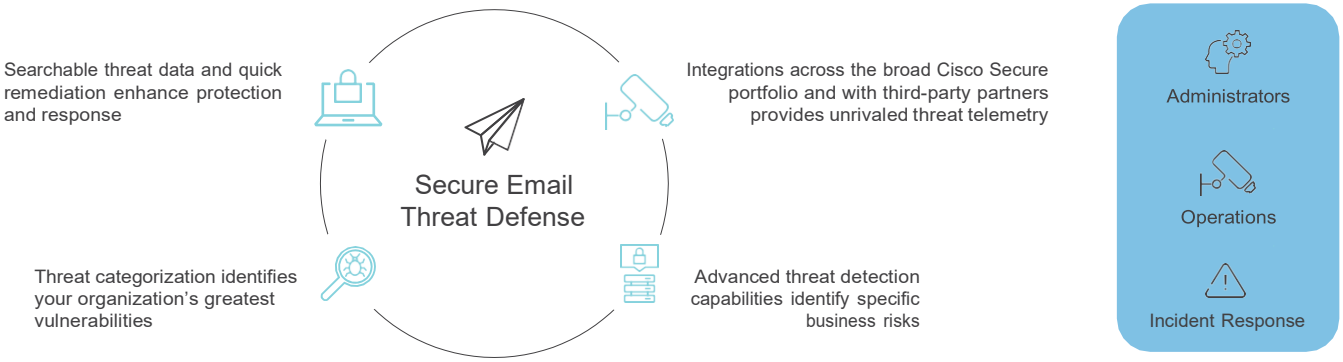


CISCO SECURE EMAIL CLOUD GATEWAY (CLOUD)

- Mêmes fonctionnalités que Secure Email Gateway mais hébergé dans le Cloud de Cisco

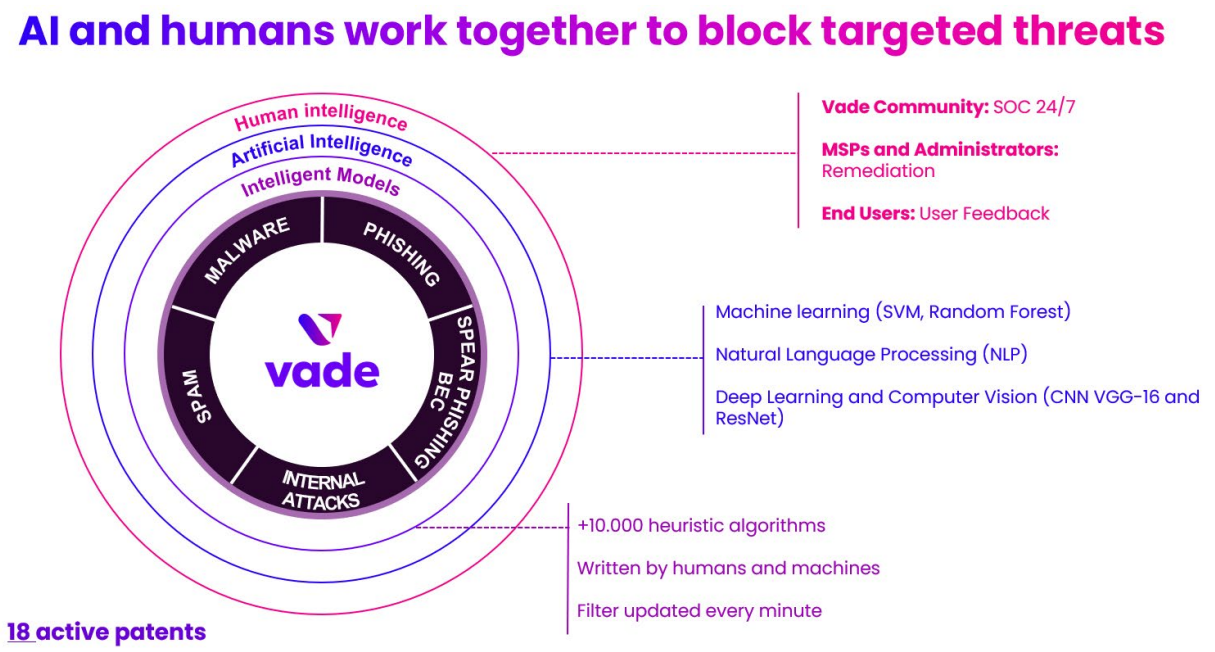
CISCO SECURE EMAIL THREAT DEFENSE (M365)

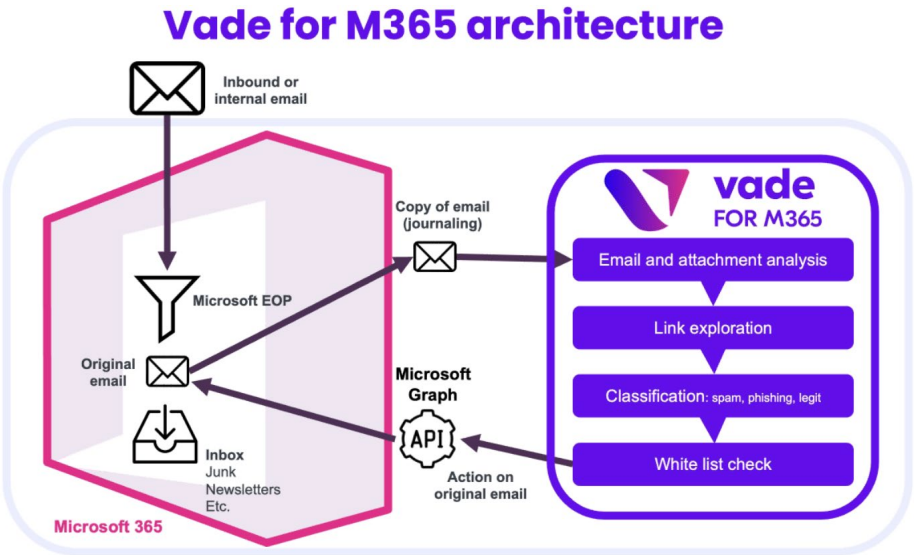
- Protection du flux mail entrant et sortant
- Protection du flux mail interne (intra-tenant M365)
- Console de gestion unique



HORNET SECURITY – VADE POUR M365 OU GOOGLE WORKSPACE

- Protection du flux mail entrant et sortant
- Protection du flux mail interne (intra-tenant M365/Google Workspace)
- Console de gestion unique





Services fournis par DEEP autour de la protection mail :

- Projets de design et implémentation
- Audits et conseil
- Maintien en condition opérationnelle
- Support

Intéressé(e) ?

Nos équipes, certifiées sur les produits Cisco et Hornet Security, vous accompagnent dans vos réflexions, dans la mise en œuvre et dans l'intégration de solutions de protection mail.

Contactez-nous :
cyberforce.sps@deep.eu