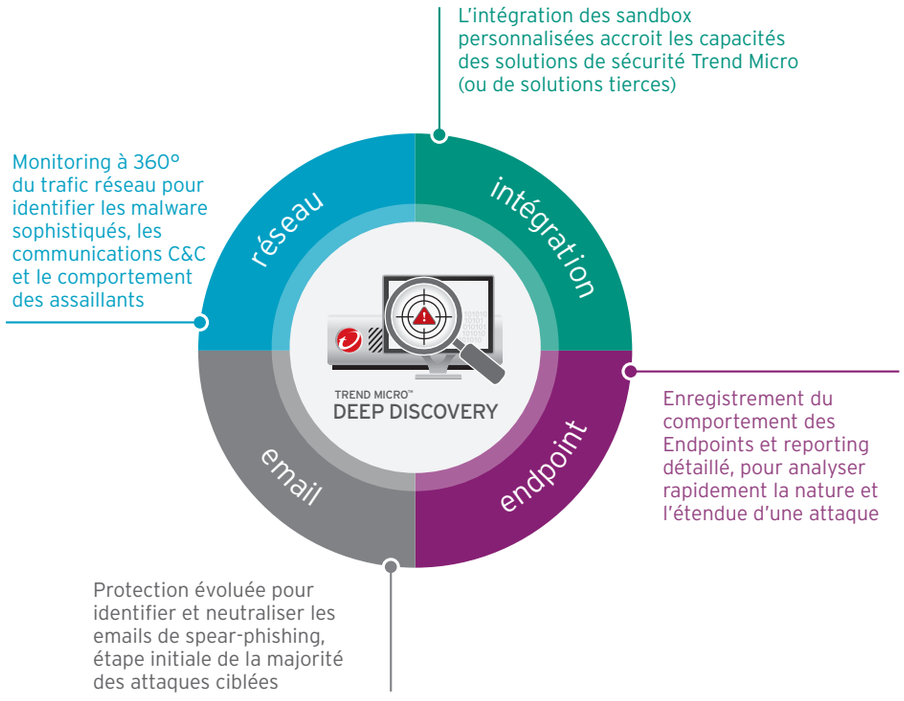
Trend Micro™

DEEP DISCOVERY

Une protection optimale contre les attaques ciblées

Trend Micro Deep Discovery est une plateforme de protection contre les menaces qui détecte, analyse et neutralise les attaques ciblées et furtives. À l'aide de moteurs de détection spécialisés, d'un sandboxing personnalisé et d'une veille sur les menaces proposée par l'infrastructure Trend Micro Smart Protection Network, Deep Discovery neutralise les attaques qui passent aujourd'hui inaperçues auprès des produits de sécurité traditionnels. Les solutions Deep Discovery dédiées à la sécurité des réseaux, de l'email et des Endpoints activent une protection évoluée contre les menaces sur les périmètres les plus critiques de votre réseau.



Deep Discovery en 3 avantages :

Protection contre les attaques
Des technologies de détection pour identifier les menaces avant tout dommage

Plateforme unique, multiples solutions
Une protection sophistiquée active sur tous les points critiques de l'infrastructure sécurisée

Veille et prise en charge rapide
Associé à Smart Protection Network, Deep Discovery offre une réactivité inégalée

Trend Micro Custom Defense

Trend Micro Custom Defense fédère l'ensemble de votre infrastructure de sécurité en une ligne de défense temps-réel contre les attaques ciblées. La détection qu'offre Deep Discovery et le partage des informations de veille, forment la pierre angulaire de l'offre Custom Defense, permettant aux organisations d'accélérer la détection, l'analyse et la prise en charge des attaques.

NSS LABS RECOMMENDED
Trend Micro™ Deep Discovery
MOST EFFECTIVE
Recommended Breach Detection System
2015 Breach Detection Tests

DEEP DISCOVERY : FONCTIONNALITÉS CLÉS

Détection évoluée des menaces
Des moteurs d'analyse de menaces, des règles de corrélation et un ensemble de sandbox personnalisées détectent les malware, les communications C&C et le comportement des assaillants.

Sandboxing personnalisé
Vos configurations systèmes sont reproduites à la lettre au sein d'environnements virtuels pour détecter les menaces qui vous ciblent spécifiquement, et notamment les malware capables de contourner les sandbox génériques.

Veille via le Smart Protection Network
Une veille de sécurité sur les menaces, accessible depuis une plateforme Cloud, détecte les menaces et alimente la solution Threat Connect, qui fournit l'information nécessaire aux analyses post-incidents.

Custom Defense (défense personnalisée)
La mise à disposition d'indicateurs de compromission permet la mise à jour automatique des différents produits de sécurité existants et déploie une protection étendue et efficace contre les attaques futures.

DÉTECTION DES ATTAQUES RÉSEAU

Défense contre les attaques non détectées par les outils de sécurité traditionnels

TREND MICRO™ DEEP DISCOVERY INSPECTOR est une appliance qui surveille le trafic réseau sur tous les ports et 80 protocoles et applications. À l'aide de moteurs de détection évolués et d'un sandboxing personnalisé, la solution identifie les malware, les communications C&C et les signaux caractéristiques des tentatives d'intrusions. Les informations de détection permettent d'accélérer la prise en charge des menaces. Elles sont également partagées avec les autres solutions de sécurité afin de bloquer les prochaines attaques.

PROTECTION CONTRE LES ATTAQUES PAR EMAIL

Neutralisation de l'étape préliminaire d'un piratage de données : le spear-phishing

TREND MICRO™ DEEP DISCOVERY EMAIL INSPECTOR, appliance dédiée à la sécurité des emails, utilise des techniques sophistiquées de détection de malware et un sandboxing personnalisé pour identifier et stopper les emails de spear-phishing (souvent la phase initiale d'une attaque ciblée). La solution met en œuvre un système d'inspection des emails pour analyser les contenus de messages, les fichiers joints et les liens URL malveillants qui ne sont pas détectés par les systèmes traditionnels de sécurité.

DÉTECTION DES ATTAQUES SUR LES ENDPOINTS

Analyse et réponse aux attaques sur les serveurs et Endpoints

TREND MICRO™ DEEP DISCOVERY ENDPOINT SENSOR est une plateforme de type *context-aware* qui surveille l'activité des endpoints, enregistre les activités systèmes et définit un reporting permettant aux équipes de sécurité d'évaluer rapidement la nature et l'étendue d'une attaque. Les indicateurs de compromissions offerts par Deep Discovery et des sources tierces peuvent être utilisés pour rechercher sur un Endpoint d'éventuelles infiltrations et ainsi repérer une attaque dans sa globalité.

PROTECTION INTÉGRÉE CONTRE LES ATTAQUES

Dopez l'efficacité de votre infrastructure de sécurité existante

TREND MICRO™ DEEP DISCOVERY ANALYZER est un serveur d'analyse en sandbox qui améliore les capacités de détection des malware de l'ensemble des solutions de sécurité. Analyzer s'intègre nativement avec la plupart des produits Trend Micro et il est possible de soumettre manuellement un élément suspect. Un Web Service permet à tout produit ou processus de soumettre un échantillon pour analyse.

RECHERCHES ET ADMINISTRATION CENTRALISÉES

Évaluer, hiérarchiser et analyser les attaques avec Deep Discovery ou un SIEM

TREND MICRO CONTROL MANAGER offre une visibilité centralisée, des moyens d'investigation sur les menaces et un reporting sur l'ensemble des modules Inspector actifs, ainsi que des fonctions centralisées pour administrer l'ensemble des produits de Trend Micro, dont Deep Discovery notamment. La majorité des produits de la gamme Deep Discovery s'intègre avec les solutions SIEM du marché que constituent HP ArcSight, IBM QRadar et Splunk.

TREND MICRO™

http://www.trendmicro.com