PRÉSENTATION DE SOLUTION

FireEye

Sécurité du cloud

Surveillance et protection des infrastructures hybrides

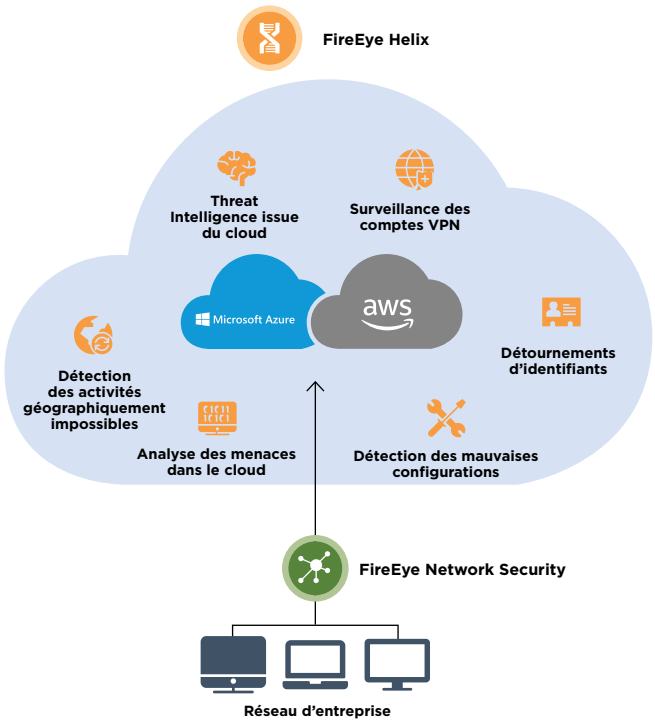
EN BREF

- Visibilité temps réel sur les menaces et vulnérabilités de l'infrastructure cloud
- Détection et prévention du vol d'identifiants et des erreurs de configuration susceptibles d'entrainer une violation de l'environnement cloud
- Centralisation du suivi et de la collecte des logs CloudTrail, S3 et ELB pour simplifier les opérations de sécurité

Les entreprises qui migrent leurs opérations vers le cloud font face à une multitude de problèmes de sécurité. Dispositifs d'authentification mal configurés, clés de cryptage mal gérées, API non sécurisées... ces exemples ne représentent qu'une poignée des nombreux vecteurs qu'utilisent les attaquants pour accéder aux infrastructures cloud. Une fois à l'intérieur, ils peuvent alors détourner des applications et se déplacer incognito dans l'environnement cloud pour s'emparer d'identifiants et exfiltrer des données confidentielles. En fait, le cloud est aussi vulnérable aux attaques que les technologies sur site, mais très peu d'entreprises disposent des outils de protection adéquats.

Les fournisseurs de solutions IaaS (Infrastructure as a Service) et PaaS (Platform as a Service) s'appuient sur un modèle de responsabilité partagée qui laisse aux clients la charge de protéger leurs propres données dans le cloud. Pour sécuriser leur infrastructure cloud, les entreprises doivent par conséquent protéger les identifiants des utilisateurs, identifier proactivement les vulnérabilités et centraliser la surveillance du dispositif de défense.

Seule solution pour y parvenir : FireEye Helix. Cette plateforme de sécurité opérationnelle assure une visibilité centralisée, un suivi des configurations et des analyses comportementales des utilisateurs pour détecter les menaces avancées dans le cloud.



Sécurité de l'infrastructure cloud avec FireEye

Points forts de la solution FireEye :

Visibilité et Threat Intelligence pour détecter les menaces cachées

Protection contre le détournement d'identifiants et les mauvaises configurations de l'environnement cloud

Suivi des ressources décentralisées

Détection des détournements d'identifiants

Identifie et signale les comptes compromis

Détection des activités géographiquement impossibles

Vérifie si les connexions observées sont physiquement impossibles pour le détenteur légitime des identifiants, compte tenu de l'éloignement géographique

Analytique, orchestration et règles de configuration du cloud

Détecte les mauvaises configurations des environnements cloud, puis y remédie et génère des rapports automatiquement

Identification des comptes VPN compromis

Identifie les éventuelles menaces par VPN en s'appuyant sur les connexions au data center, les impossibilités géographiques et les anomalies IP

Threat Intelligence issue du cloud

Complète les alertes Amazon GuardDuty par des données contextuelles pour améliorer les processus de détection et de réponse

Surveillance réseau

Détecte les activités suspectes sur les liaisons WAN pour empêcher les déplacements latéraux des attaquants entre les réseaux des entreprises et les environnements IaaS et PaaS

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France
Nextdoor Cœur Défense 110 Esplanade du Général de Gaulle 92931 Paris La Défense Cedex 92974 | +33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Threat Intelligence. Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de Cyber Threat Intelligence d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FireEye