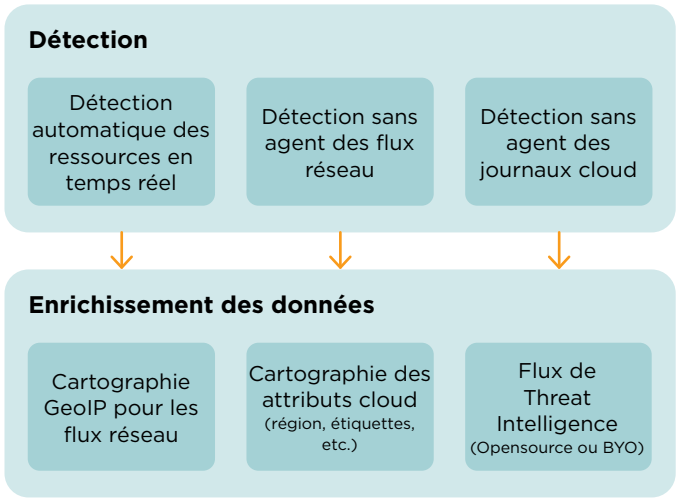
FIREEYE™

FICHE PRODUIT

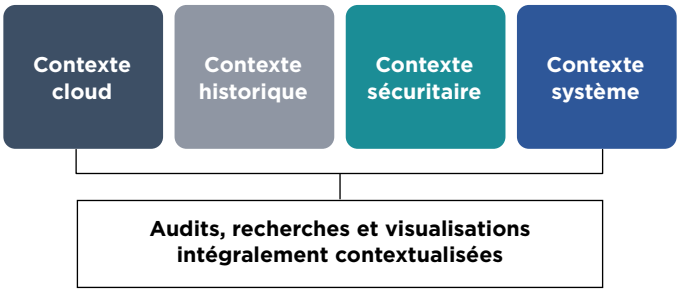
Cloudvisory

Visibilité approfondie, conformité continue et gouvernance intelligente au service d'une sécurité complète des environnements multi-cloud



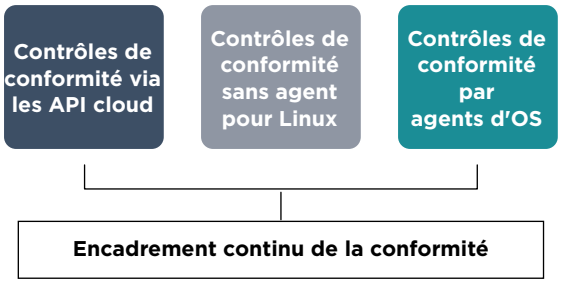
Visibilité

Détection et cartographie continue des ressources d'entreprise, des contrôles de sécurité et des événements de sécurité dans les clouds privés et publics. Le machine learning interprète les données contextuelles pour détecter les risques et les menaces.



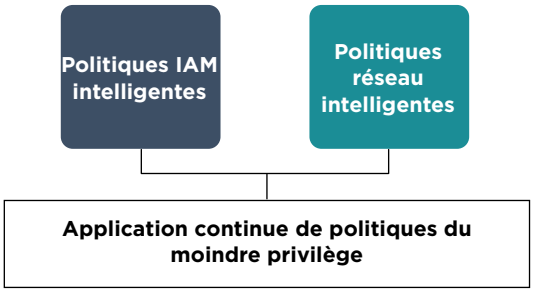
Conformité

Suivi de conformité automatisé avec plus de 1300 points de contrôle intégrés. Application des bonnes pratiques, des politiques personnalisées et des standards de sécurité tels que CIS, GDPR, HIPAA, NIST, PCI DSS et d'autres.



Gouvernance

Application des politiques de sécurité augmentée par machine learning. Réduction des surfaces d'attaque et prévention des intrusions par l'apprentissage, les tests et le déploiement de politiques du moindre privilège à n'importe quelle échelle.



Cloud public : Azure

Visibilité

Comptes, utilisateurs/groupes/rôles IAM, régions, groupes de ressources, services, abonnements, sous-réseaux

Workloads détectés

Pods AKS, services applicatifs, environnements de services applicatifs, Cosmos, comptes de bases de données, zones DNS, fonctions, équilibreurs de charge, caches Redis, clusters de fabrics de services, comptes de stockage, machines virtuelles et bien plus encore...

Cloud public : AWS

Visibilité

Comptes, utilisateurs/groupes/rôles IAM, régions, services, sous-réseaux, réseaux VPC

Workloads détectés

Instances EC2, systèmes de fichiers EFS, pods EKS, équilibreurs de charges élastiques, flux Kinesis, fonctions Lambda, passerelles NAT, clusters RDS, zones hébergées Route53, buckets S3, topics SNS et bien plus encore...

Cloud privé : OpenStack

Visibilité

Clusters, instances, keystone, réseau, projets (tenants), services de régions

Détection, analyse et gestion des groupes de sécurité réseau pour les instances OpenStack (nova) et les pods Kubernetes. Surveillance des flux réseau pour détecter les menaces en quasi temps réel.

Cloud privé : Kubernetes

Visibilité

Clusters, déploiements, utilisateurs/groupes/rôles d'identité, espaces de noms, réseaux, pods.

Data center historique

Systèmes d'exploitation

- Ubuntu Linux
- Redhat
- CentOS

Automatisations intégrées

Systèmes externes (tiers)

Alertes automatiques configurables, analyses d'historique des événements de sécurité (SIEM, Elasticsearch), scans et reporting de conformité déclenchés par API/événements, ingestion de journaux pour des sources alternatives d'événements de sécurité (équipements réseau d'ancienne génération, fournisseurs IAM...).

Gartner Cool Vendor 2018

Cloudvisory élu Gartner Cool Vendor dans la catégorie Sécurité cloud 2018.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory classé par CIO Applications dans le Top 25 des fournisseurs de solutions Amazon.

AICPA SOC

Cloudvisory : SaaS certifié SOC 2 par un audit indépendant.

Pour en savoir plus sur Cloudvisory, rendez-vous sur **www.FireEye.com/cloud**

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
FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035
+1 408 321 6300 | info@FireEye.com

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 CTI 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™