SCHEDA TECNICA

Cloudvisory

Sicurezza completa del carico di lavoro multi-cloud grazie alla profonda visibilità, alla conformità continua e alla governance intelligente

Conformità

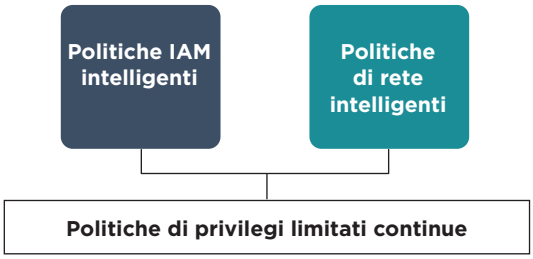
Monitoraggio automatico della conformità di sicurezza con oltre 1.300 controlli integrati. Governance delle migliori pratiche, politiche e quadri di riferimento personalizzati come CIS, GDPR, HIPAA, NIST, PCI DSS e altri.

Visibilità

Scoperte e mappature continue di asset aziendali, controlli di sicurezza ed eventi di sicurezza su cloud pubblici e privati. L'apprendimento automatico sfrutta il contesto per scoprire rischi e minacce.

Governance

Pratiche di governance potenziate con l'intelligenza artificiale. Capacità di ridurre gli attacchi e di prevenire le intrusioni attraverso l'apprendimento, test e implementazione di politiche intelligenti con privilegi limitati su qualsiasi scala.



Cloud pubblico—Azure

Visibilità

Account, Utenti/gruppi/ruoli IAM, Regioni, Gruppi di risorse, Servizi, Abbonamenti, Sottoreti.

Carichi di lavoro scoperti

AKS Pods, Servizi App, Ambienti di servizi App, Cosmos, Account DB, Zone DNS, Funzioni, Bilanciamenti del carico, Cache Redis, Cluster di Service Fabric, Account di archiviazione, Macchine virtuali e altro ancora...

Cloud pubblico—AWS

Visibilità

Account, Utenti/gruppi/ruoli IAM, Regioni, Servizi, Sottoreti, VPC.

Carichi di lavoro scoperti

Istanze EC2, File di sistema EFS, EKS Pods, Bilanciamenti del carico Elastic, Flussi Kineses, Funzioni Lambda, Gateway NAT, Cluster RDS, Zone ospitate Route53, Bucket S3, Argomento SNS e altro ancora...

Cloud privato—OpenStack

Visibilità

Cluster, Istanze, Keystone, Rete, Progetti (tenant), Servizi regioni.

Scopri, analizza e gestisci gruppi di sicurezza di rete per le istanze OpenStack(Nova) e Kubernetes Pods. Monitora i flussi di rete per rilevare le minacce in tempo quasi reale.

Cloud privato—Kubernetes

Visibilità

Cluster, Implementazioni, Identità Utenti/Gruppi/Ruoli, Spazio dei nomi, Reti, Pod.

Datacenter storico

Sistemi operativi

- Ubuntu Linux
- Redhat
- CentOS

Integrazioni di automazione

Sistemi esterni (di terzi)

Avviso automatico, configurabile, analisi storiche per eventi di sicurezza (come SIEM, Elasticsearch), scansione e reportistica della conformità basata su evento/innescata API, inserimento dati nei log per fonti alternative di eventi di sicurezza (come dispositivi di rete legacy, provider di identità).

Gartner Cool Vendor 2018

Cloudvisory è stato nominato Gartner Cool Vendor nel Cloud Security 2018.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory è inserito da CIO [Chief Information Officer (Direttore Informatico)] Applications fra i 25 migliori fornitori di soluzioni Amazon.

AICPA SOC

Cloudvisory-SaaS è certificato SOC 2.

Per ulteriori informazioni su Cloudvisory, visita: **www.FireEye.com/cloudvisory**

FireEye Italia Srl
Piazza IV Novembre, 7. 20124 Milano Italia
+39 0294750535
italy@FireEye.com

Informazioni su FireEye, Inc.

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.

FIREEYE™