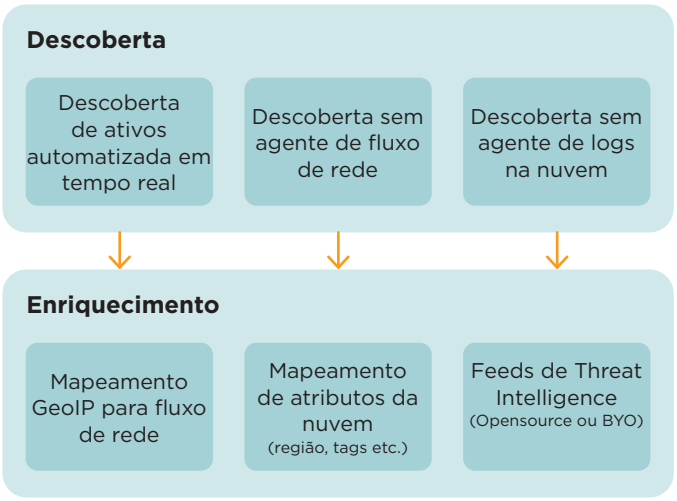
FIREEYE™

FICHA TÉCNICA

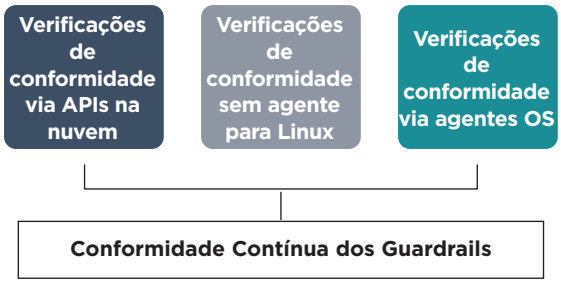
Cloudvisory

Segurança abrangente de workloads em várias nuvens por meio de visibilidade profunda, conformidade contínua e governança inteligente



Conformidade

Monitoramento automatizado de conformidade de segurança com mais de 1.300 verificações incorporadas. Governança de práticas recomendadas, políticas personalizadas e estruturas como CIS, GDPR, HIPAA, NIST, PCI DSS e outras.

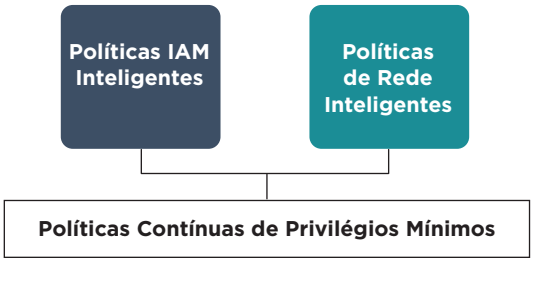


Visibilidade

Descoberta contínua e mapeamento de ativos da empresa, controles de segurança e eventos de segurança em nuvens públicas e privadas. O aprendizado de máquina aproveita o contexto para revelar riscos e ameaças.

Governança

Práticas de governança ampliadas com inteligência de máquina. Capacidade de reduzir superfícies de ataque e prevenir intrusão ao aprender, testar e implantar eficientemente políticas inteligentes com privilégios mínimos em qualquer escala.



Nuvem Pública—Azure

Visibilidade

Contas, usuários/grupos/funções IAM, regiões, grupos de recursos, serviços, assinaturas, Subnets.

Descoberta de Workloads

AKS Pods, App Services, App Service Environments, Cosmos, DB Accounts, DNS Zones, Functions, Load Balancers, Redis Caches, Service Fabric Clusters, Storage Accounts, Virtual Machines e mais...

Nuvem Pública—AWS

Visibilidade

Contas, usuários/grupos/funções IAM, regiões, serviços, Subnets, VPCs.

Descoberta de Workloads

EC2 Instances, EFS File Systems, EKS Pods, Elastic Load Balancers, Kineses Streams, Lambda Functions, NAT Gateways, RDS Clusters, Route53 Hosted Zones, S3 Buckets, SNS Topics e mais...

Nuvem Privada—OpenStack

Visibilidade

Clusters, Instances, Keystone, Network, Projects(Tenants), Regions Services.

Descubra, analise e gerencie grupos de segurança de rede para instâncias OpenStack(Nova) e Pods Kubernetes. Monitore fluxos de rede para detectar ameaças em tempo quase real.

Nuvem Privada—Kubernetes

Visibilidade

Clusters, Deployments, Identity Users/Groups/Roles, Namespaces, Networks, Pods.

Datacenter Legado

Sistemas Pperacionais

- Ubuntu Linux
- Redhat
- CentOS

Integrações Automatizadas

Sistemas externos (de terceiros)

Alerta configurável automatizado, análise histórica para eventos de segurança (tais como SIEM, Elasticsearch), geração de relatórios e varredura de conformidade baseados em eventos/acionados por API, ingestão de logs para fontes alternativas de eventos de segurança (tais como dispositivos de redes legados, provedores de identidade).

Gartner Cool Vendor 2018

Cloudvisory indicado Gartner Cool Vendor em Cloud Security 2018.

CIO APPLICATIONS — TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory reconhecido pela CIO Applications entre os 25 principais Provedores de Soluções Amazon.

AICPA SOC

Cloudvisory-SaaS independentemente certificado SOC2.

Para saber mais sobre Cloudvisory, acesse: **www.FireEye.com/cloudvisory**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035 EUA
1.408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2020 FireEye, Inc. Todos os direitos reservados. FireEye é uma marca registrada da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários. CS-EXT-DS-US-EN-000299-02

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e reagir a ataques cibernéticos.

FIREEYE™