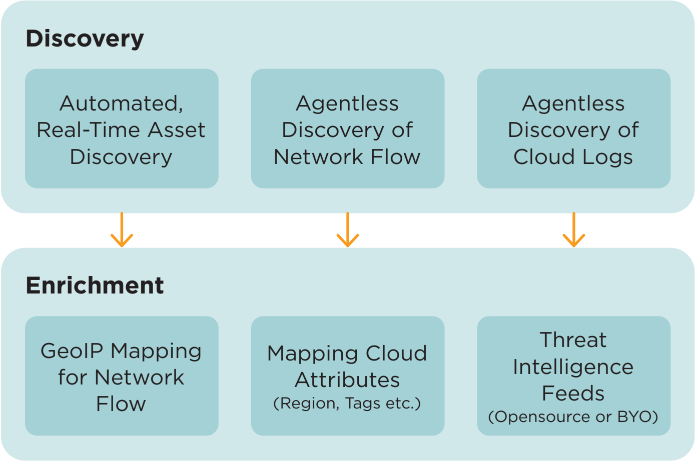
FIREEYE™

DATA SHEET

Cloudvisory

Comprehensive multi-cloud workload security through deep visibility, continuous compliance and intelligent governance



Discovery

Automated, Real-Time Asset Discovery

Agentless Discovery of Network Flow

Agentless Discovery of Cloud Logs

↓

Enrichment

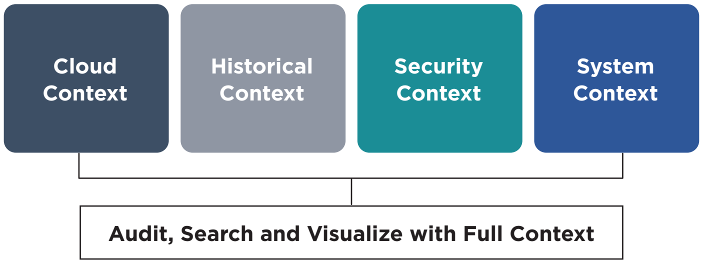
GeoIP Mapping for Network Flow

Mapping Cloud Attributes (Region, Tags etc.)

Threat Intelligence Feeds (Opensource or BYO)

Visibility

Continuous discovery and mapping of enterprise assets, security controls and security events across public and private clouds. Machine learning leverages context to uncover risks and threats.



Cloud Context

Historical Context

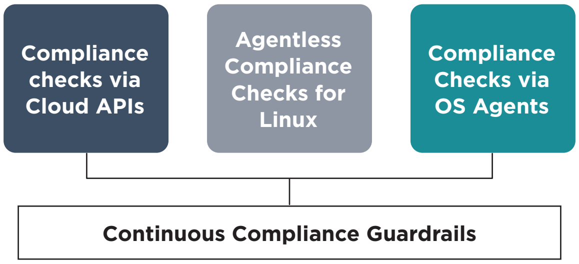
Security Context

System Context

Audit, Search and Visualize with Full Context

Compliance

Automated security compliance monitoring with over 1,300 built-in checks. Governance of best practices, custom policies and frameworks such as CIS, GDPR, HIPAA, NIST, PCI DSS and others.



Compliance checks via Cloud APIs

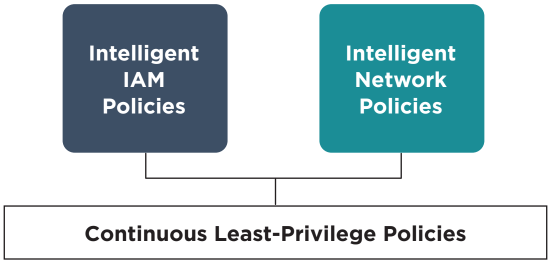
Agentless Compliance Checks for Linux

Compliance Checks via OS Agents

Continuous Compliance Guardrails

Governance

Augmented governance practices with machine intelligence. Ability to reduce attack surfaces and prevent intrusions by efficiently learning, testing and deploying intelligent least-privilege policies at any scale.



Intelligent IAM Policies

Intelligent Network Policies

Continuous Least-Privilege Policies

Public Cloud—Azure

Visibility

Accounts, IAM Users/Groups/Roles, Regions, Resource Groups, Services, Subscriptions, Subnets

Discovered 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 and more...

Public Cloud—AWS

Visibility

Accounts, IAM Users/Groups/Roles, Regions, Services, Subnets, VPCs

Discovered 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 and more...

Private Cloud—OpenStack

Visibility

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

Discover, analyze and manage Network Security Groups for OpenStack(Nova) Instances and Kubernetes Pods. Monitor network flows to detect threats in near-real-time.

Private Cloud—Kubernetes

Visibility

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

Legacy Datacenter

Operating Systems

- Ubuntu Linux
- Redhat
- CentOS

Automation Integrations

External (third-party) systems

Automated, configurable alerting, Historical analytics for security events (such as SIEM, Elasticsearch), API-triggered/event-based compliance scanning and reporting, log ingestion for alternative sources of security events (such as legacy network devices, identity providers).

Cloudvisory named Gartner Cool Vendor in Cloud Security 2018.

Cloudvisory recognized by CIO Applications in top 25 Amazon Solution Providers.

Cloudvisory-SaaS independently SOC2 certified.

To learn more about Cloudvisory, visit: **www.FireEye.com/cloudvisory**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.