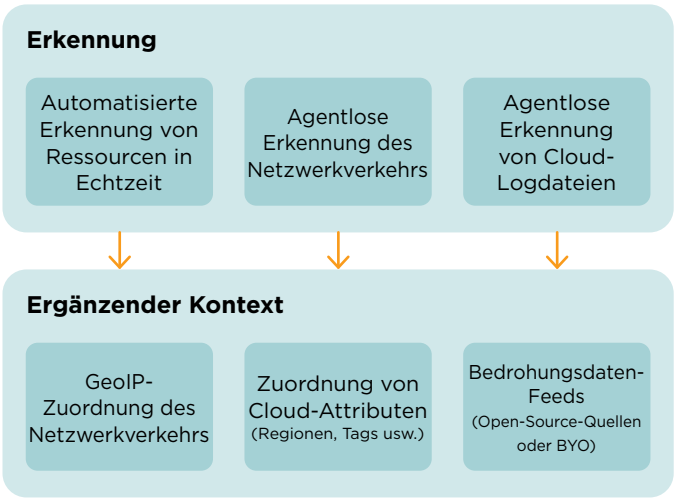
FIREEYE™

DATENBLATT

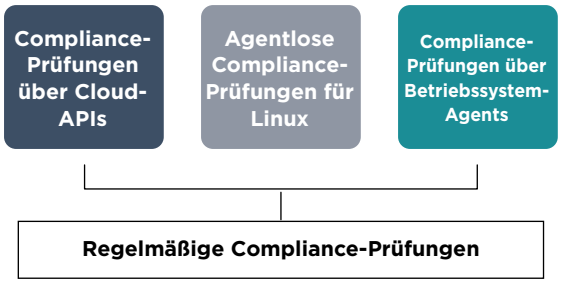
Cloudvisory

Zuverlässige Multi-Cloud-Sicherheit für Workloads durch Transparenz, kontinuierliche Compliance und intelligente Governance



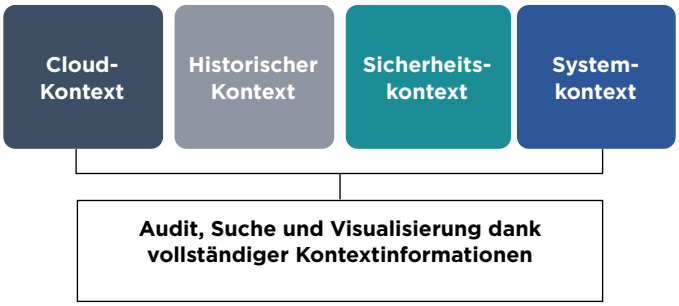
Compliance

Automatisierte Sicherheitsüberwachung mit mehr als 1.300 integrierten Prüfungen. Durchsetzung von Best Practices, individuellen Richtlinien und Vorschriften, zum Beispiel CIS, DSGVO, HIPAA, NIST und PCI DSS.



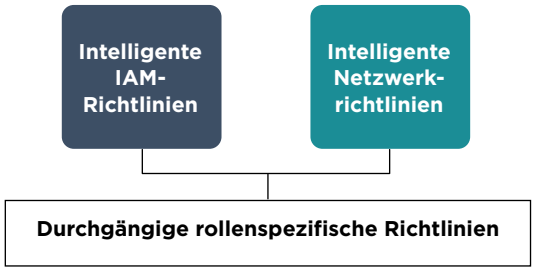
Transparenz

Kontinuierliche Erkennung und Zuordnung von Unternehmensressourcen, Sicherheitsfunktionen und -ereignissen in öffentlichen und privaten Clouds. Funktionen für maschinelles Lernen nutzen Kontextanalysen, um Risiken und Bedrohungen aufzudecken.



Governance

Ergänzende Governance-Richtlinien mit maschinell erfassten Bedrohungsdaten. Reduzierung der Angriffsfläche und Abwehr von Angriffen durch effizientes Lernen, Testen und Durchsetzen intelligenter rollenbasierter Richtlinien in Umgebungen aller Größen.



Öffentliche Cloud – Azure

Transparenz

Konten, IAM-Benutzer/-Gruppen/-Rollen, Regionen, Ressourcengruppen, Services, Abonnements, Subnetze

Erkannte Workloads

AKS-Pods, App-Services, App Service-Umgebungen, Cosmos, DB-Konten, DNS-Zonen, Funktionen, Load Balancer, Redis Caches, Service Fabric-Cluster, Speicherkonten, virtuelle Maschinen und viele mehr

Öffentliche Cloud – AWS

Transparenz

Konten, IAM-Benutzer/-Gruppen/-Rollen, Regionen, Services, Subnetze, VPCs

Erkannte Workloads

EC2-Instanzen, EFS (Elastic File Systems), EKS-Pods, Elastic Load Balancer, Kinesis-Streams, Lambda-Funktionen, NAT-Gateways, RDS-Cluster, gehostete Route 53-Zonen, S3-Buckets, SNS-Themen und viele mehr

Private Cloud – OpenStack

Transparenz

Cluster, Instanzen, Keystone, Netzwerk, Projekte (Mandanten), Regionen, Services

Erkennung, Analyse und Management der Network Security Groups for OpenStack-Instanzen (Nova) und Kubernetes-Pods. Überwachung des Netzwerkverkehrs zur Erkennung von Bedrohungen nahezu in Echtzeit.

Private Cloud – Kubernetes

Transparenz

Cluster, Bereitstellungen, Identität (Benutzer/Gruppen/Rollen), Namespaces, Netzwerke, Pods

Ältere Rechenzentren

Betriebssysteme

- Ubuntu Linux
- Red Hat
- CentOS

Integrationen für die Automatisierung

Externe Systeme (Drittanbieter)

Automatisierte, konfigurierbare Warnmeldungen, historische Analysen von Sicherheitsereignissen (z. B. SIEM und Elasticsearch), über die API ausgelöste/ereignisbasierte Compliance-Scans und -Berichte, Einspeisen von Logdateien als alternative Quellen von Sicherheitsereignissen (wie ältere Netzwerkgeräte und Identitätsanbieter)

Gartner Cool Vendor 2018

Cloudvisory wurde im Bericht „Cloud Security 2018“ als „Gartner Cool Vendor“ ausgezeichnet.

CIO APPLICATIONS – TOP 25 AMAZON SOLUTION PROVIDERS 2017

CIO Applications führt Cloudvisory unter den „Top 25 Amazon Solution Providers“ auf.

AICPA SOC

Cloudvisory-SaaS wurde von einer unabhängigen Stelle gemäß SOC-2 zertifiziert.

Weitere Informationen zu Cloudvisory erhalten Sie unter: **www.FireEye.de/cloudvisory**

FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE™