FIREEYE™

SOLUTION BRIEF

Minding the Visibility Gap for Cloud Security

43% of some 400,000 survey respondents listed “Visibility into infrastructure security” as a key pain point.

Cloud Security Report
Cybersecurity Insiders

Scenario for consideration
Most organizations get hacked at some point, though most data breaches go undetected.

Of the minority which do get detected, most data breaches go undetected for at least 6-12 months prior to being detected either by accident or by some external entity, such as a customer or security researcher.

A given organization is more likely to be notified of a given data breach by an external, well-meaning entity than they are to discover the same data breach via their internal operations.

These statistics are provided by organizations which were “in compliance” at the time of the data breach and does not take into account organizations which do not bother with compliance or data breach investigations.

All things being equal, it’s better to find hacks early using your own people, rather than be informed by your customer(s).

The visibility gap
Everything depends on visibility, the essential foundation for any cloud security strategy. It doesn’t matter whether your cloud security strategy revolves around compliance assurance, threat hunting, policy governance or risk remediation.

But visibility presents a hurdle which many organizations never clear. Every year, surveys of cyber security professionals show that visibility into infrastructure security is the most prevalent cyber security challenge.

Before tackling any more advanced security strategy or topic, you need to address the visibility gap.

Core problems
Security teams face many challenges that work against the maintainability of a centralized and context-rich security operations (SecOps) view of attack behavior moving laterally within an enterprise.

The visibility gap widens as organizations grow and different groups of people implement an increasingly diverse array of deployment processes and technologies spanning many cloud providers, accounts, geographies and services.

Self-service deployments have made businesses more efficient at the expense of the ability to centrally provision and monitor hardened infrastructure. Cloud technologies have, in various ways, allowed infrastructure deployments to become larger, more distributed, dynamic by nature and (sometimes) ephemeral, while traditional security tools fail at cloud scale and speed. Over the past decade, deployment automation technologies have also outpaced security automation technologies in aspects such as adoption, features and maturity.

Historically, SecOps focused on controls for prevention rather than detection. But prevention eventually fails. Traditional prevention focused on statically defined controls concentrated at the enterprise perimeter. In the cloud, however, the perimeter is dynamic rather than static in nature and logically rather than physically defined.

Legacy security tools (such as physical and virtual firewalls) are poorly suited for blocking and detecting attacks within distributed and dynamic cloud environments. And the rapid pace of change in the cloud, coupled with increasingly distributed and diverse enterprise deployments, makes it difficult to find a single security solution which can provide deep visibility into all deployment environments.

Solution requirements
Any solution to the visibility gap must provide comprehensive visibility, which requires broad and deep monitoring of current-state configurations and historical security events associated with assets.

Comprehensive visibility into infrastructure security requires multiple forms of visibility simultaneously, to ensure:

- **The complete inventory of all in-scope assets at all times**
  Without visibility into the complete inventory (both current and historical) of all in-scope assets, compliance audits and security analytics will yield incomplete and/or misleading results.
- **Contextual details are searchable for the current state of any and every asset**
  Without visibility into the current state of all in-scope assets, there is no context. Without context, there is no meaning and no validity to concepts such as compliance assurance and anomaly detection.
- **The complete historical record of in-scope security events for each asset**
  Without visibility into the actual behavior of workloads and users, there is no way to confirm that governance policies are working and no reason to expect that a given infrastructure is not already owned by some nefarious actor.

Merely deriving the asset-inventory and asset-state data from logs is insufficient. Data gaps remain as a result of warmup periods, service disruptions and other failure scenarios.

If the current configured state of assets is not known directly from the cloud provider APIs associated with the asset or service being discovered, then the inventory of assets cannot be considered complete and it may be possible for attackers to easily evade detection. Logs tell a good story, but APIs do not lie.

A true solution must, therefore, provide comprehensive visibility into complex and distributed deployment environments, including hybrid cloud and multi-cloud deployments which may be massive, ephemeral or serverless. The solution not only requires comprehensive visibility, but also must provide a consolidated and searchable view of all forms of the context available for each asset. The visibility solution should allow users to perform ad-hoc queries—via UI or API—against the recorded context of any and all in-scope assets, through a single interface for performing security analytics and compliance audits across cloud boundaries.

An ideal solution would make it easy for users to convert ad-hoc audit queries into recurring compliance checks to not only close the visibility gap, but also start using comprehensive visibility as a foundation for more advanced security practices such as compliance assurance, policy governance and threat hunting.

CLOUDVISORY VISIBILITY

The Cloudvisory solution provides comprehensive visibility into the security of any infrastructure, all from a single solution. Asset discovery is completely automated and Cloudvisory maintains the complete inventory of all in-scope assets in real-time. Automated discovery via cloud provider APIs yields deep context, because Cloudvisory stores details on the last-known state of every asset which has ever existed in any monitored environment. The state of a given asset contains details from multiple layers of deep context, including information about each asset's:

- **Cloud Context:** details about the asset's associated cloud-provider/account/region/group/role/etc.
- **Historical Context:** analytics derived from the historical record of security events created during the lifecycle of an asset
- **Security Context:** current-state configurations of an asset's security controls
- **System Context:** current-state information recorded directly from the asset's operating system

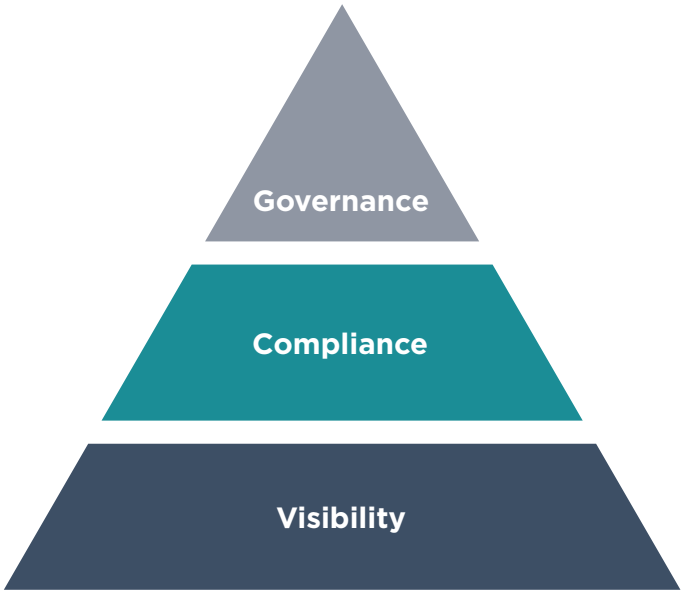
Why Cloudvisory?

The Cloudvisory solution provides the best coverage of all your multi-cloud, multi-operating system environments. In addition to providing broad and deep coverage, Cloudvisory is a complete solution which has been engineered so that its component parts (visibility, compliance and governance) work better together.

Many products can quickly assess your security posture across several deployments and accounts within the same cloud provider. Most organizations are aligned with a hybrid cloud or multi-cloud strategy and only have a few cloud security options. But there is only one multi-cloud security solution that provides an immediate return on investment (via comprehensive visibility) and future-proofed to drive efficiency and security improvements for years to come: Cloudvisory.

Better together

Visibility creates a foundation for compliance, but recurring compliance checks also create visibility data. This synergistic relationship creates additional security and historical context, which feeds into governance where machine learning algorithms take context as input and generate output in the form of intelligent least-privilege policies for augmented governance.



Supported Cloud Service Providers

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Supported Operating Systems

- CentOS
- Redhat
- Ubuntu Linux

Gartner Cool Vendor 2018

Cloudvisory named Gartner Cool Vendor in Cloud Security 2018.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

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

AICPA SOC

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.

FIREEYE™