FIREEYE™

SOLUTION BRIEF

Continuous Compliance Assurance for Cloud Security

Scenario for consideration

If (approved) System-A and System-B are both 100% in compliance right now, but there is no record of (rogue) System-C existing for long enough to act as a database replica for System-A and System-B, then there is no useful proof of due diligence in validating compliance for either System-A or System-B.

If (approved) System-D is 100% in compliance now, but there is no proof of the compliance state of System-D in the time since the last audit until now, then proof of due diligence for System-D is limited to only what can be proven "now."

Many types of compliance audits require ongoing (recurring or continuous) proof of due diligence as part of compliance certification.

If it needs to happen continuously and it needs to happen at scale, then it needs to be as automated as possible to reduce—rather than introduce— operational expenditures.

Achieving continuous compliance assurance

Compliance assurance means establishing proof of due-diligence, which provides the group, individual or organization with some form of protection from liability—legal or otherwise. Compliance assurance activities are cost-justified so long as they are effective in establishing due diligence, and security budgets are often allocated accordingly.

But if compliance assurance must dominate the security budgets of organizations, then compliance assurance must also be the cornerstone of any solution to advanced and persistent security threats. Even if an organization cannot stop all advanced threats with compliance checks alone, it can expect to filter out much of the noise by using recurring compliance checks to continuously validate that many basic things are always done right.

Automating compliance assurance is the best way to ensure that compliance activities are both thorough and efficient. What the modern enterprise needs is a genuinely useful compliance assurance solution which saves money through automation efficiency while providing greater coverage of assets and their respective states of compliance at multiple levels. This coverage should include configurations and patches for cloud applications (such as serverless functions), networks (such as virtual private networks), services and workloads, as well as traditional operating systems.

Core problems

Security teams face many challenges when trying to achieve continuous compliance assurance for public and private cloud environments—especially when various types of cloud assets span multiple cloud providers, cloud provider accounts, operating systems, regions, services and other logical groups.

In the absence of automated and comprehensive visibility into both asset states and compliance history of multi-cloud environments, organizations waste valuable personnel hours struggling through each and every periodic compliance audit. To many personnel, compliance assurance becomes a massive disruption with huge operational costs and no clear ongoing benefit.

Organizations struggle to integrate compliance activities into existing automation processes and tooling; it is difficult to bring greater efficiency to compliance assurance by leveraging the DevOps model.

Organizations also struggle to find useful technical solutions to common problems in compliance assurance, largely because legacy compliance tools lack at least one of several critical features, such as:

- Automatic discovery of the complete asset inventory via cloud provider APIs
- Built-in mechanism for enforcing compliance guardrails via inline risk remediation
- Comprehensive visibility into cloud- and operating system-level vulnerabilities
- Event-driven responses (such as alerts, reports, remediations) to detected compliance failures
- Handling for time-based exceptions to compliance rules according to business needs
- Group-level configuration of compliance settings for subsets of discovered assets
- On-demand (API-driven) compliance scanning of specified asset(s)
- Risk analytics which allow teams to triage risk remediation efforts
- Standardized support for many common compliance reporting standards

Solution requirements

Cloud environments are dynamic by nature. Cloud users can create the resources they need, when they need them, but this also allows resources to be created, altered or destroyed at any time.

Compromised cloud account credentials may allow hackers unfettered access to insecure, unauthorized resources which are out of scope for traditional monitoring tools. For continuous (ongoing) proof of due diligence for all in-scope infrastructure assets—continuous compliance assurance—cloud security solutions must:

- Continuously maintain the complete inventory of in-scope assets, including a detailed and searchable state record for each asset.
- Record the complete historical activity of security-related events for each and every asset, including compliance check results created by the solution.

Ideally, a single solution could assess compliance assurance across many logical and physical infrastructure boundaries. It would enable users to use pre-built and ad-hoc queries to aggregate risks (compliance failures) by logical attributes and allow DevOps and SecOps staff to prioritize risk remediation activities for vulnerable areas.

The compliance assurance solution should use context gleaned from cloud provider APIs to provide a context-rich data set, which can be queried and filtered by users via UI and API to create new custom compliance checks. It should be both powerful and easy to use for basic audits of asset inventory, compliance check results and compliance assurance reports. The solution's compliance engine must also be flexible enough to support more advanced and atypical forms of compliance checks to meet the unique organizational needs.

CONTINUOUS COMPLIANCE ASSURANCE REQUIREMENTS

- **Breadth**
  Ability to perform a wide array of compliance checks at various levels in the modern technology stack for cloud accounts, cloud services, identity objects (users, groups, roles), networks, operating systems and patches, and more.
- **Depth**
  Ability to gather deep contextual data regarding both the configuration and behavior of assets. Most security products sacrifice depth for breadth or vice versa. An ideal solution should provide deep coverage of compliance states across multiple layers (levels) in the modern technology stack.
- **Integration**
  Ability to work in concert with existing operational tooling. As early detection of compliance deficiencies becomes a growing concern, it becomes even more important to integrate automated compliance checks with existing DevOps deployment (CI/CD) pipelines. The solution should provide a RESTful API for integrating on-demand compliance features into agile testing environments, such that deployment teams may detect and correct compliance deficiencies in early stage testing environments (such as “Dev”, “Lab”, “QA”).

The Cloudvisory solution

The Cloudvisory solution delivers continuous compliance assurance for multi-account, multi-cloud and multi-operating system environments. Compliance automatically detects risks via configurable checks against known assets, controls and events while providing options (alert, report, remediate) for manual and automated responses. Cloudvisory compliance provides over 1,300 built-in compliance checks and makes it easy to customize existing checks and add new checks.

A simple point-and-click user interface makes it easy to quickly convert findings from ad-hoc audits into continuous compliance guardrails (compliance checks that recur at some configurable interval). The solution tracks the complete history of compliance checks associated with discovered cloud assets and provides rich reporting capabilities to meet internal and external requirements for compliance assurance. It easily generates and exports compliance reports in various formats (such as PDF, XLS, CSV) for all compliance checks and any subset of compliance checks (for custom internal standard or compliance reports). It also offers built-in reports for supported compliance standards.

Why Cloudvisory?

Only Cloudvisory provides truly broad and deep integration of continuous compliance assurance for modern organizations. Other products may lack one or more critical capabilities:

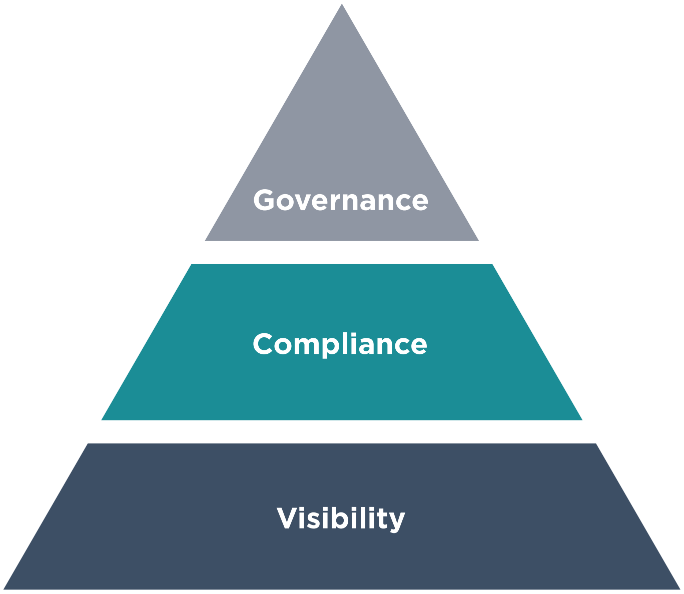
- Breadth of coverage across multiple cloud providers and operating systems
- Depth of coverage required to establish a useful level of due diligence at a given compliance layer (cloud, operating system)
- RESTful APIs required for integration of compliance automation into existing operational processes and tooling

Cloudvisory compliance builds on a strong foundation of comprehensive visibility to provide sufficient context for evaluating the various levels and states of compliance for a given asset. Cloudvisory compliance provides built-in support for essential features, such as configurable inline remediation, time-based handling of business-approved exceptions to compliance rules, on-demand compliance scanning of specified assets via Cloudvisory APIs, and drill-down risk aggregations which allow security analysts to assess risk across logical and physical infrastructure boundaries.

Competing products may provide limited compliance solutions (focused on one cloud provider or operating system) based off of limited visibility (logfiles only), which yield inconsistent results and limited value in an organization's compliance assurance practices. Cloudvisory couples a solid core of enterprise features with a market-leading extendable compliance framework. Cloudvisory makes it easy to automate compliance assurance activities in any environment, and helps organizations realize better security with lower costs.

Better together

Cloudvisory compliance is built on the foundation of deep context provided by Cloudvisory visibility. While Cloudvisory compliance is extendable for any compliance purpose, many basic custom compliance checks can be easily created from ad-hoc queries against data sets provided by Cloudvisory visibility. The distinct data sets which are provided by Cloudvisory visibility and used by Cloudvisory compliance include cloud resource configurations (such as VMs), cloud security control configurations (such as IAM Policies, Network Security Groups), cloud object logs, network flow logs, operating system configurations and operating system logs. Batches of custom compliance checks can be easily created to work with Cloudvisory and fulfill compliance assurance needs.



Supported Compliance Standards .

Cloud Provider

- AWS CIS Benchmark
- AWS GDPR
- AWS HIPAA
- AWS NIST 800-53 Revision 4
- AWS PCI DSS 3.2
- Azure CIS Benchmark
- Azure GDPR
- Azure HIPAA
- Azure NIST 800-53 Revision 4
- Azure PCI DSS 3.2
- Kubernetes CIS Benchmark
- OpenStack Security Checklist

Operating Systems

- CentOS CIS Benchmark
- Redhat CIS Benchmark
- Ubuntu 16.04 CIS Benchmark
- Ubuntu 18.04 CIS Benchmark

Supported Cloud Service Providers

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

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
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

Cloudvisory-SaaS independently SOC2 certified.

To learn more about FireEye, 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™