Visibility and Context to Foster Security Confidence

As more organizations migrate more from the data center to the cloud and embrace multiple public cloud providers, security becomes a challenge. A basic question to answer is "Does your multi-cloud estate work like you think it does?" You may have one or more policies in place, but you need to take measures to ensure these policies are working as intended. This means relying on validation, not assumptions.

Kion brings visibility and context for key governance, security, and compliance functions across the three major cloud service providers — AWS, Azure, and Google Cloud — to provide the levels of validation that cloud security professionals need to gain confidence in the security posture of their environment.

Accelerate Account Provisioning & Compliance Baselines

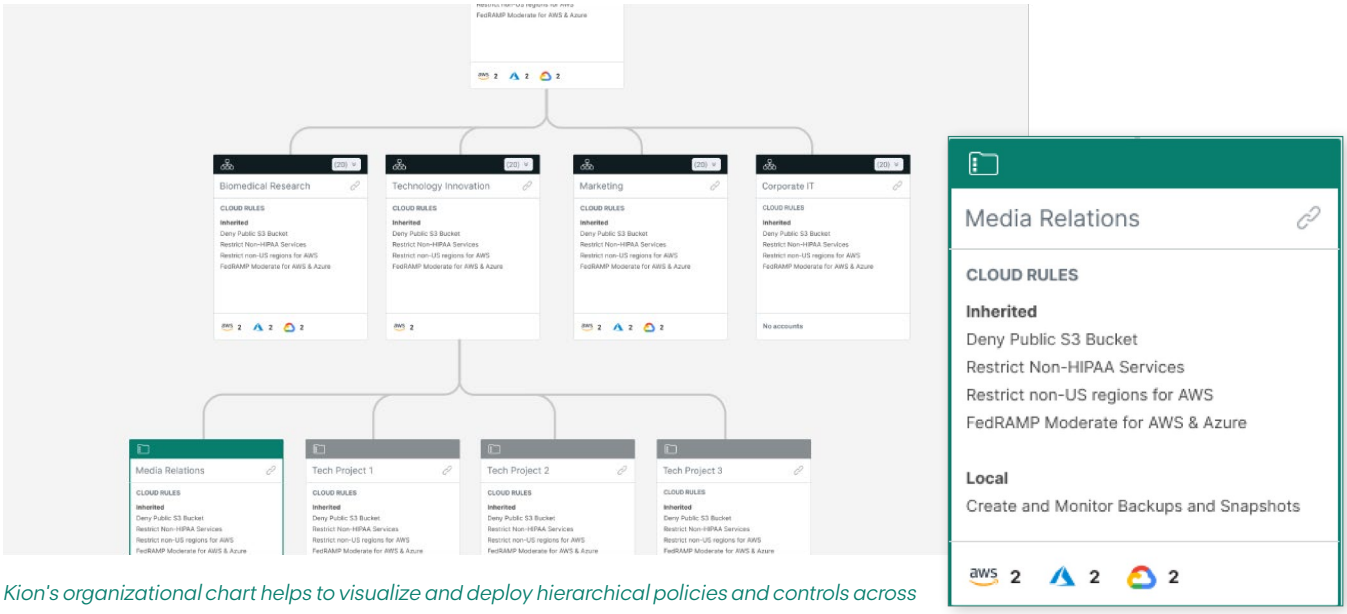
Your cloud service provider delivers you the cloud environment and secures and supports its underlying infrastructure, but your organization is responsible for properly implementing the policies and permissions for your cloud accounts and resources.

Kion bridges that gap by providing a single platform to automate governance, identity and access management, and compliance requirements for your cloud accounts. With Kion you can establish a secure, least-privileged blueprint for AWS, Azure, and Google Cloud accounts to increase your account provisioning exponentially and with confidence that users will only have access to what they need.

We do this by providing:

- Hierarchical controls for easy account provisioning
- Automated enforcements to uphold spending limits
- Pre-built security checks for out-of-the-box compliance

Wherever you are on your journey in the cloud, we can help you optimize the entire cloud account lifecycle, enabling your organization to scale confidently.

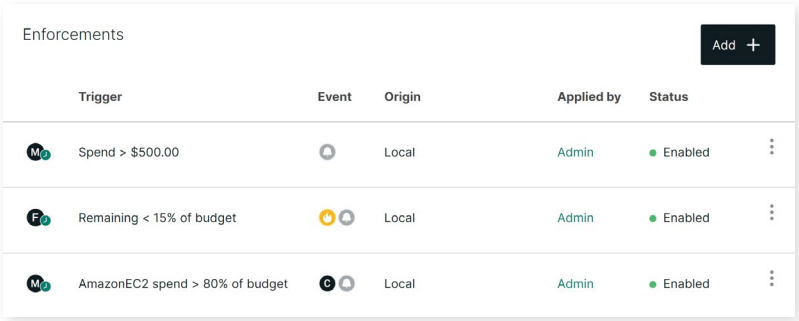


Kion's organizational chart helps to visualize and deploy hierarchical policies and controls across cloud providers.

AUTOMATED MULTI-CLOUD GOVERNANCE & POLICY ENFORCEMENT

Establish and maintain a unified governance framework for your organization through our multi-cloud governance platform. Gain visibility and power automation across AWS, Azure, and Google Cloud to manage the full account lifecycle aligning with key focus areas:

- Financial Transparency and Control
- Account Provisioning and Baselining
- Standardized, Least Privileged Access
- Security and Compliance for Cloud Accounts and Resources



Cloud rules power automatic financial, access, and compliance enforcements across cloud providers.

Without financial and compliance guard-rails in place at account creation, every new AWS account, Azure subscription, and Google Cloud project becomes a new opportunity for potential compliance violations and cost overruns. That's why Kion lets you do more than merely see violations; Kion enforces policies and financial controls automatically to build confidence that as you scale, you will do so in line with your policies, compliance requirements, and best practices.

GRANULAR MULTI-CLOUD IAM

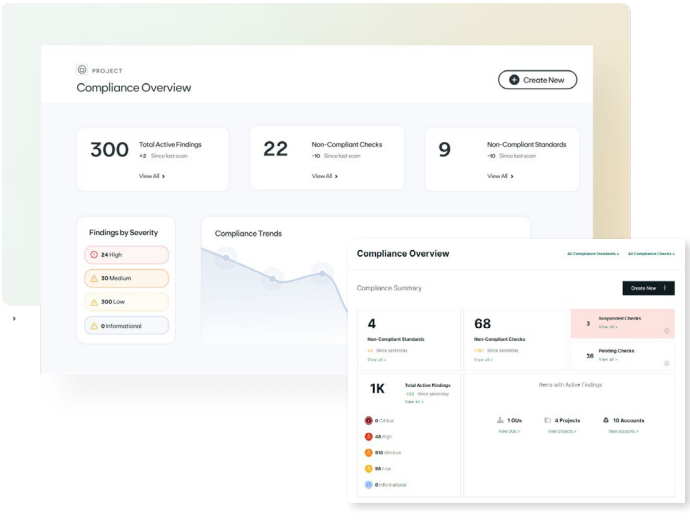
Many organizations lack visibility and control over their roles and permissions and don't have an easy way of managing their permission sets across their multi-cloud environments.

Cloud Access Roles (CARs) are the powerful, easy-to-use vehicle for granting users the right type and level of access to the cloud service providers to accomplish their work. CARs are used to define user roles that are assumed upon federation into the cloud environment. The parameters that can be defined within a CAR include access type, users/user groups associated to the role, cloud accounts the role has access to, associated IAM policies, Azure Role Definitions, or Google Cloud IAM Roles. CARs can be associated at any level of the organization structure and are automatically inherited allowing you to disseminate properly configured access across the entire organization without duplicate work.

Enhance Multi-Cloud Visibility with Powerful Context

Our compliance dashboard, spanning AWS, Azure, and Google Cloud, shows how many of your compliance checks were found non-compliant, gives insight at-a-glance into compliance violations, and lets you fix them easily. Using this dashboard, you can:

- Find the hot spots. You can view findings by resource to see which areas have the most compliance issues.
- See the impact of automation. You'll get information on how many non-compliant checks were automatically remediated, so you'll know the impact of the automation you've put in place.



- Let your team take action. Allow your security team to view active findings, intervening manually or suppressing the finding if it's not relevant, and build in automatic remediation wherever you need it.
- Keep your fingers on the pulse of your cloud compliance: Managers can easily learn how many compliance checks failed and exactly how they were handled by your team (whether ignored, addressed, or suppressed).

COMPLETE VISIBILITY THROUGHOUT YOUR SECURITY STACK

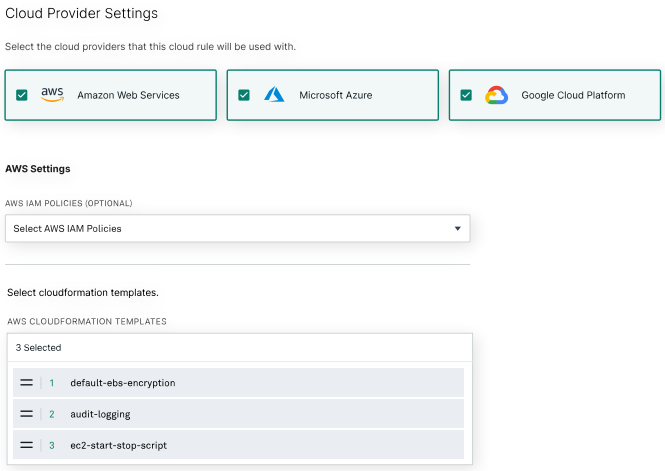
Kion integrates with and enhances many popular security platforms that you may already be using, including those across the three main cloud providers. These integrations mean that you can ingest findings from other sources higher up in the stack to make Kion your one-stop source for insight into OS-level and cloud service misconfigurations for AWS, Azure, and Google Cloud.

Security teams love the context and visibility inside of our platform, but Kion can also enhance the information in other security event management platforms. You can also send the findings collected in Kion to other tools through our integration with native solutions like Azure Security Center or AWS Security Hub to create a more complete picture of your compliance posture.

Prevent, Detect, Report, and Remediate Cloud Misconfigurations

PREVENT DRIFT ACROSS CLOUD PROVIDERS

The easiest problem to fix is the one that never happens. To prevent drift, Kion uses a construct known as "Cloud Rules" that can be configured to effect security policy as well as cost and spending constraints across cloud providers. Cloud Rules conform to cloud provider constructs like CloudFormation, IAM, YAML, ARM Templates, Terraform (through webhooks) etc., meaning users spend less time writing policy across clouds and retain the assurance that their environment is properly configured.



Kion's cloud rules prevent drift by effecting security policy as well as cost and spending constraints across cloud providers.

THOUSANDS OF BUILT-IN COMPLIANCE CHECKS & AUTOMATIC REMEDIATIONS

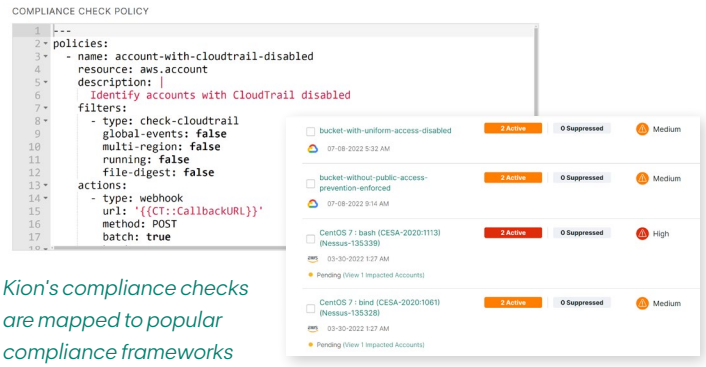
The compliance engine within Kion provides a very easy rule language as well as cloud platform agnostic remediations that don't require deploying Lambda functions or similar services. Kion has over 6,000 checks across many popular compliance regimes, including CIS, PCI DSS, NIST, ISO 27001, SOC 2, FedRAMP, HIPAA, and more.

Many of our checks include automatic remediation steps that leverage your configuration files. You don't need to write code but, rather, you can leverage simple YAML configuration files and comment in a line or two to remediate across findings and across accounts.

Kion's compliance engine is fully customizable, so you can:

- Apply checks only where you need them. Compliance standards are attached to inheritable cloud rules, which apply only where you specify. Resources can also be exempted from checks.

- Run checks on your own timeline. You can set the compliance check frequency, running scheduled checks automatically or running ad hoc manual scans whenever you need them.
- Write your own rules and checks. We provide a form to enter your own code for compliance checks, so you can craft custom checks using YAML.
- Go beyond the built-in engine. You can connect with an external compliance engine to pull those findings into Kion.



Kion's compliance checks are mapped to popular compliance frameworks and many have automatic remediations that can be customized using YAML

Streamline Audits Using Turnkey Jumpstarts

Kion not only provides you with reactive alerts and findings that identify gaps in your compliance posture; the solution also helps you to achieve compliance. To expedite your journey to compliance, Kion includes turnkey compliance jumpstarts to apply needed controls and guardrails mapped directly to a given standard or framework in just a few clicks.

These jumpstarts allow you to quickly satisfy requirements to the given compliance standard not only by helping apply the needed guardrails and policies but also showing you exactly where your gaps are — meaning you can start applying permissions and deploying resources out of the box to get compliant faster. We provide you with our own reference library, which includes many common compliance resources, as well as complete sets of resources for established compliance frameworks.

One of the most time intensive tasks for security professionals is documenting security controls in the form of a security control matrix. Kion saves you weeks or even months of time when preparing for an audit by including a security controls matrix for every supported compliance standard.

Kion provides the proactive boundaries and reactive detection and reporting to ensure compliance — and the auto-remediation to give you confidence in your cloud security posture. By providing easy to use, cross-cloud provider guardrails and IAM Kion helps you answer the question "Does my multi-cloud estate work like I think it does?". You can scale with confidence knowing that your policies are being enforced and least privileged access has been granted. You can achieve and maintain compliance with real-time monitoring and enforcements mapped to your desired standards and frameworks. This level of confidence makes your security and compliance posture an accelerator in the cloud, enabling you to accomplish meaningful innovations and move your business forward.

If you'd like to learn more about how Kion can help deliver multi-cloud security confidence, please get in contact with one of our experts at **info@kion.io** or visit **kion.io/product/request-a-demo**.

© Kion 2023. All rights reserved.