Google Cloud

Building a Secure Data Platform with Google Cloud

CYDERES

Google Cloud

Thank you for interest in this eBook.

As a Google Cloud partner, we at Cyderes are committed to providing you with the resources and insights you need to make informed decisions about your cloud journey.

We believe that this eBook will provide valuable insights into the benefits and capabilities of Google Cloud. Cyderes is equipped to support you in expanding your Google Security Operations capabilities and data with comprehensive threat detection, investigation, triage workflows, rich reporting, and IAM.

If you have any questions or would like to discuss your specific requirements, please do not hesitate to contact us.

Sincerely,

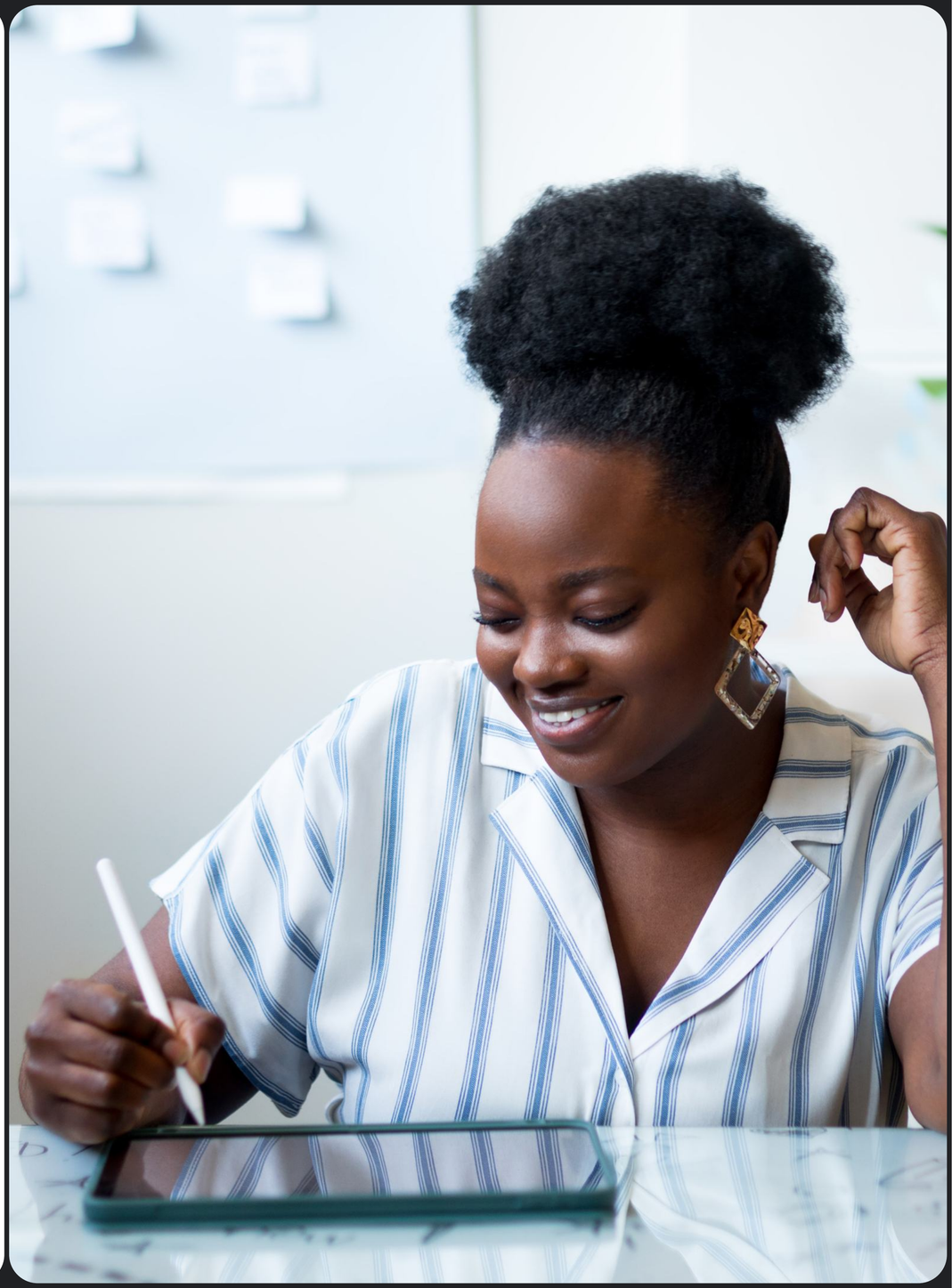
Cyderes

Google Cloud
Partner

Learn more about at cyderes.com

Google Cloud

Introduction



Organizations are faced with growing volumes of data that they need to be able to access, manage, and analyze, ranging from highly confidential business or customer data to behavioral and marketing analytics. Many are adopting cloud services to help them achieve more agility and innovate in the use of data across their business. Yet, understanding how best to secure cloud data remains an obstacle to overcome as part of these ongoing digital transformation efforts.

As more data and applications move out of on-premises data centers and away from traditional security mechanisms and infrastructure, new approaches are required. While many of the foundational elements of on-premises data security remain, they must be adapted to the cloud.

The evolving threat landscape presents additional challenges. Mandiant, in the 2024 M-Trends Report, notes that attackers have followed the growing adoption of cloud, pivoting to target cloud-hosted data and leverage cloud computing resources in their operations. As just one example, a recent high-profile threat campaign targeted a multi-cloud data warehousing SaaS platform with the intent of data theft and extortion. The attacker worked to systematically compromise customer instances using stolen credentials, advertised victim data for sale on cybercrime forums, and attempted to extort many of the victims.

At Google Cloud, we follow a shared fate model. That means we are active partners in ensuring our customers deploy workloads securely on our platform. We can help you implement best practices by offering secure-by-default configurations, blueprints, policy hierarchies, and advanced security features to help develop security consistency across your data platforms and tools.

This eBook provides data and security executives with a comprehensive overview of Google Cloud's data security capabilities. Read on to learn more about how Google Cloud enables companies to protect their sensitive data assets in the cloud and drive data-based innovation strategies with confidence.

Google Cloud

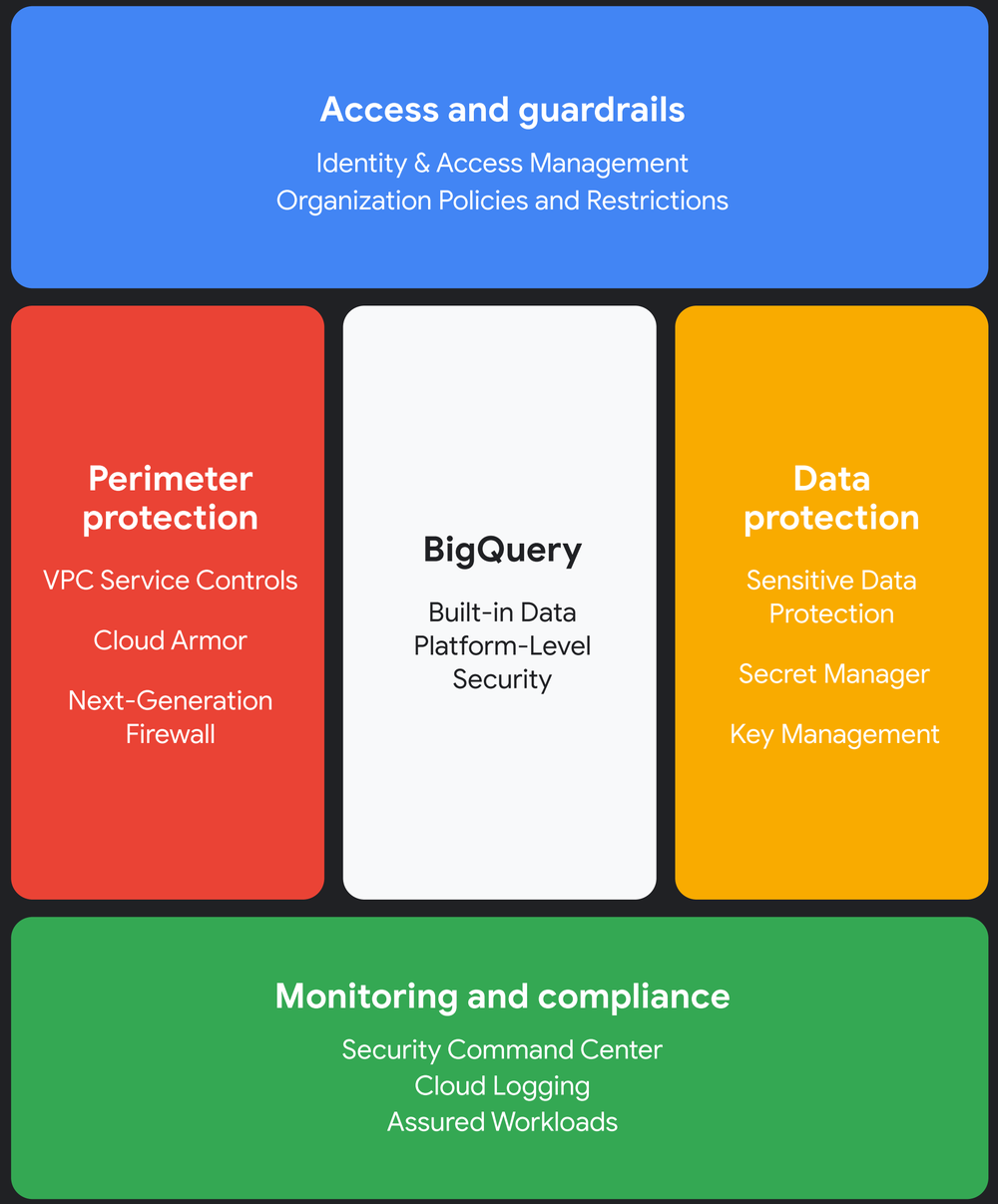
Table of contents

Fortify your data at every level

In the current digital age, the integrity and confidentiality of data are paramount. Google Cloud's multi-layered data security is designed to help you protect your critical data assets from internal and external threats.

Google Cloud provides granular controls within BigQuery, its powerful data warehouse solution, enabling precise management of access and sharing. Access and guardrail mechanisms further enforce authorization protocols, ensuring that only approved individuals and data can interact with specific resources. Encryption protects sensitive information, both at rest, during use, and in transit safeguarding its confidentiality throughout its lifecycle.

Perimeter protection creates a robust outer layer of defense, proactively guarding against both accidental and malicious attempts to compromise your data. The platform's proactive monitoring capabilities offer ongoing visibility into potential vulnerabilities, ensuring that compliance and security requirements are upheld.



“With our invisible security solution, we haven’t just made Commerzbank more secure while saving a lot of time and resources, we’ve been able to rethink what security means in the cloud. Together with Google Cloud, we’ve developed new standards that increase the understanding of the cloud - not just for us, but for everyone."

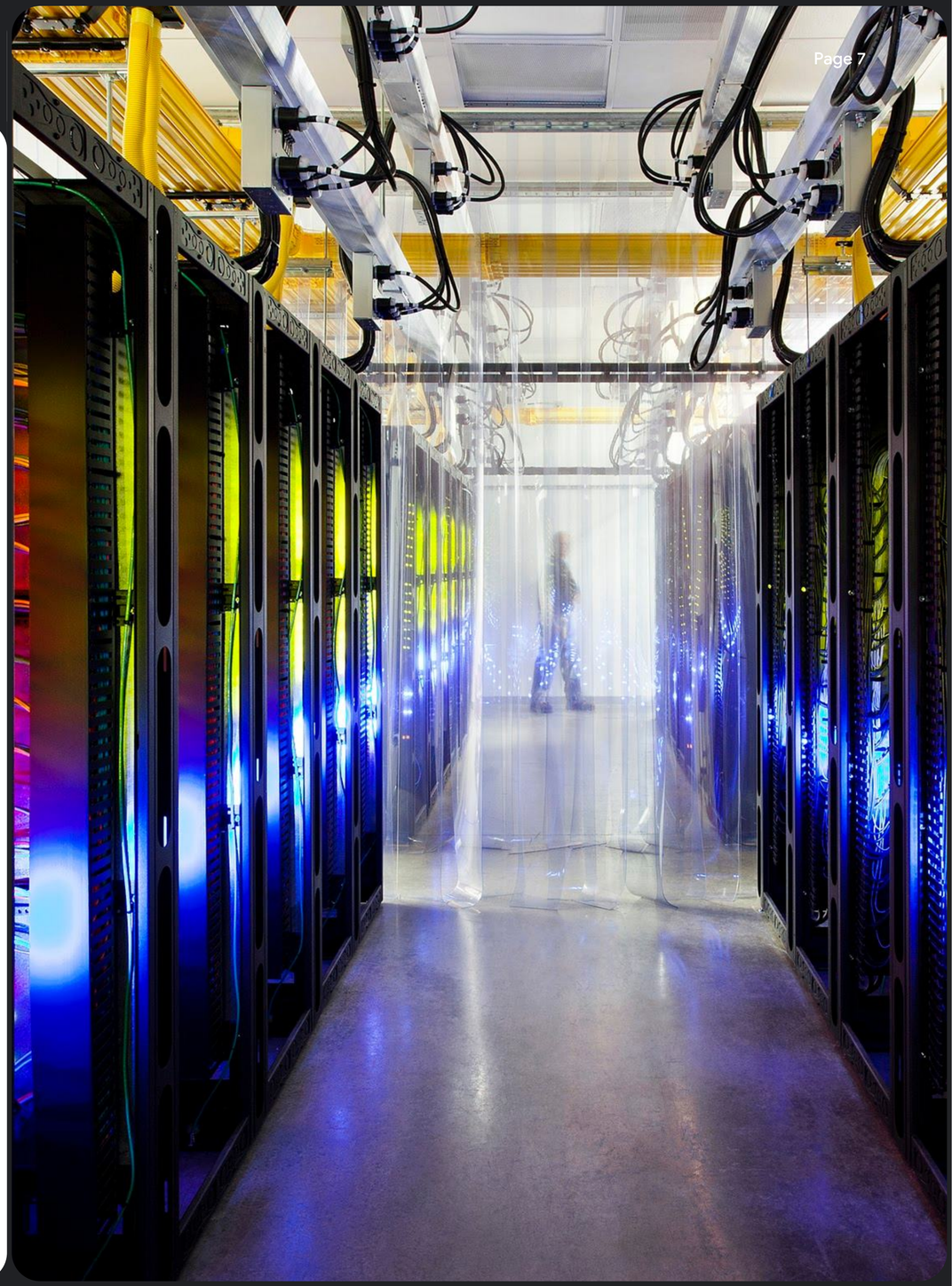
Christian Gorke

Vice President and Head of Commerzbank’s Cyber Center of Excellence

COMMERZBANK

Source: https://cloud.google.com/customers/commerzbankag

BigQuery platform-level security



Section 01

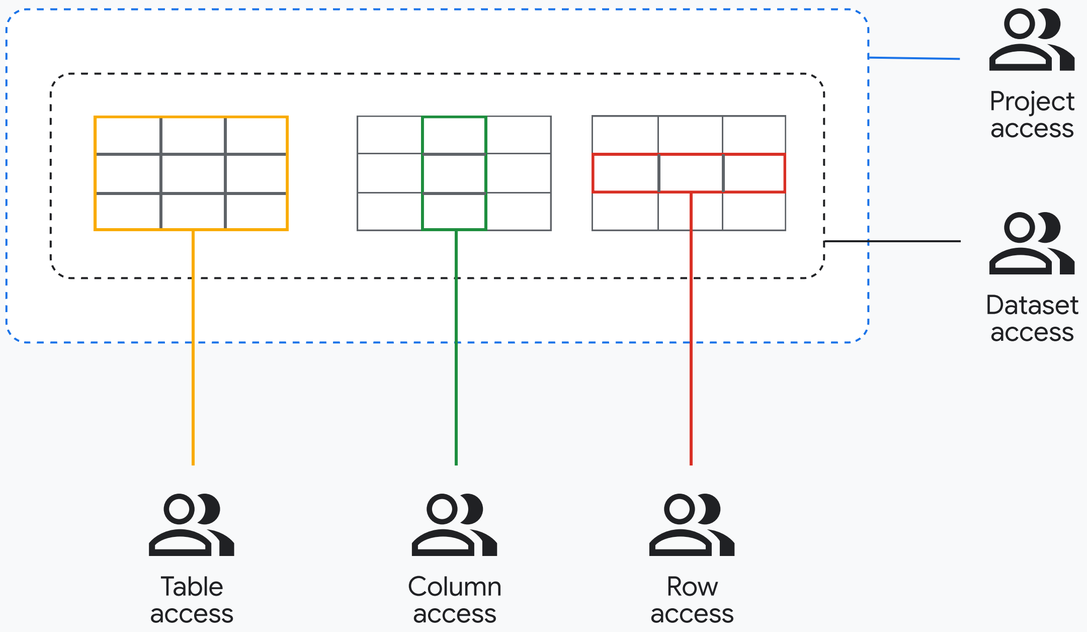
An introduction to data security in BigQuery

At the data platform level, BigQuery includes robust built-in security features, such as data encryption, masking, granular-level access controls to protect your data resources and to facilitate secure data sharing, and governance policy management.

BigQuery is tightly coupled with Cloud Identity and Access Management (IAM) to provide access control to your data and centralized management for all your cloud resources. With granular access controls, you can define resource policies in more depth, be that across projects, datasets, tables, rows and columns.

Learn more about BigQuery IAM roles and permissions →

BigQuery fine-grained access controls enable you to define resource policies at granular level



Protects your sensitive data with encryption and masking

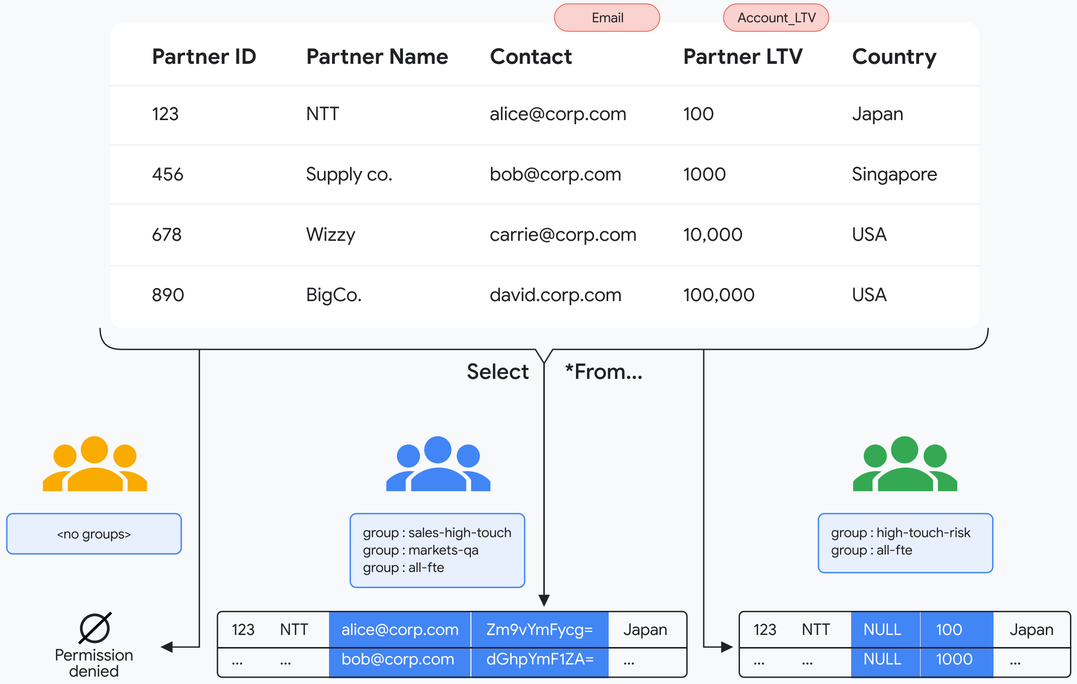
BigQuery automatically encrypts all data before it is written to disk. The data is then automatically decrypted when read by an authorized user. Using Cloud Key Management System, you'll have even more flexibility across encryption key management and storage.

Learn more about data encryption →

BigQuery also supports data masking at the column level. You can use data masking to selectively obscure column data for user groups, while still allowing them access to the column. With Sensitive Data Protection you can automatically scan, discover, and classify data to set access policies with IAM.

Learn more about data masking →

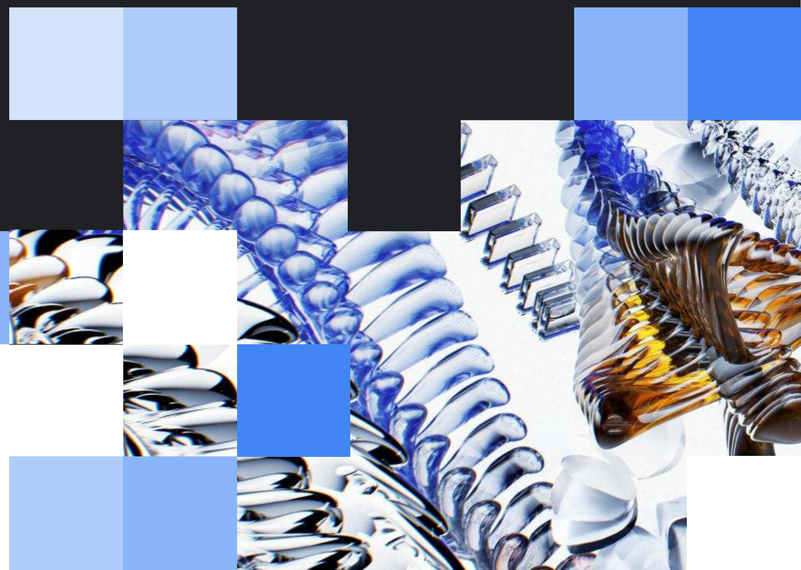
BigQuery data masking



“Enabling dynamic field level encryption is paramount for our data fabric platform to manage highly secure, regulated assets with rigorous security policies complying with several regulations including FedRAMP, PCI, GDPR, CCPA and more. BigQuery column-level encryption capability provides us with a secure path for decrypting externally encrypted data in BigQuery unblocking analytical use cases across more than 800+ analysts.”

Kumar Menon

CTO of Equifax



EQUIFAX

Source: https://cloud.google.com/blog/products/identity-security/announcing-new-bigquery-capabilities-to-help-secure-sensitive-data?e=48754805

Enables secure data sharing

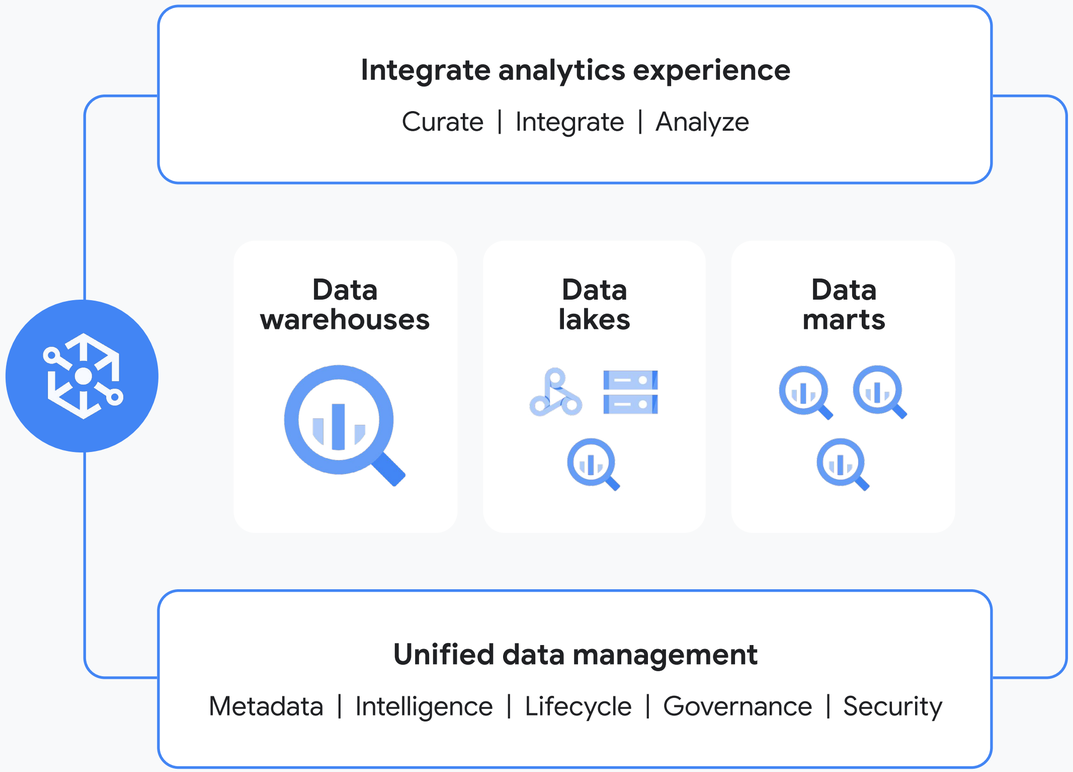
BigQuery Analytics Hub is a platform allows you to efficiently and securely exchange data assets across organizations. It makes the administration of sharing assets across any boundary easy and more scalable. For sharing data that may be subject to more stringent regulatory and privacy requirements, BigQuery data clean rooms provides extra layers of protection for privacy-centric data sharing, analysis, and collaboration.

Learn more about secure data sharing →

Assists with data governance at scale

BigQuery comes preloaded with Dataplex, an oversight layer that enables you to manage and govern data and AI artifacts across data lakes, warehouses and databases. This layer helps users establish data profiles, assess the data quality, determine lineage, classify and organize it into domains, all while monitoring its entire life cycle. Additionally, BigQuery supports disaster recovery scenarios in the case of a total region outage.

Learn more about data governance →

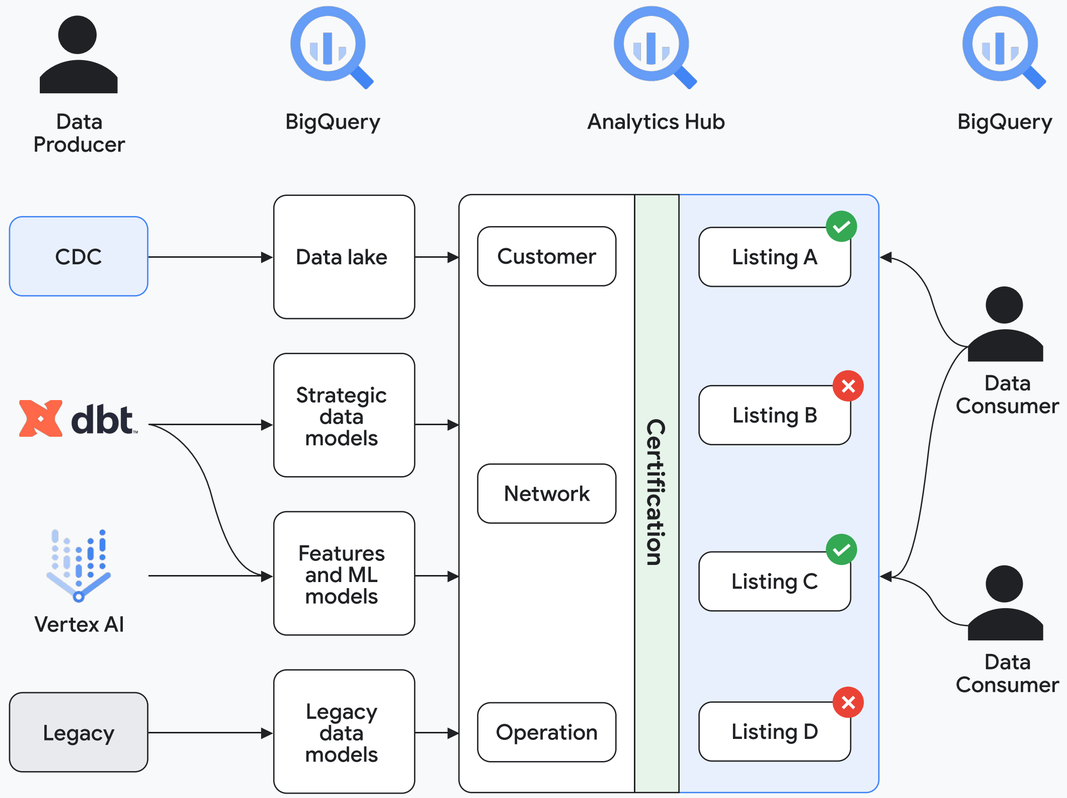


Virgin Media O2 simplifies data sharing with Analytics Hub

Virgin Media O2 is a media and telecommunications company that relies on data sharing across the organization to optimize operations, drive strategy, and empower decision makers.

The company's data platform team decided to pilot Analytics Hub after learning about its scalability, self-service capabilities, and simple governance model for data tags and quality.

After rolling out Analytics Hub to around 25 squads, the company saved up to 30 hours a week in time spent on training, support, pipelines issues with deployment, and communication overhead compared to their old solution. By building a dashboard, the team was able to democratize access to data for subscribers and their broader teams.



Platform Engineering - Governance, Privacy, Training, Observability

Learn more about Virgin Media's story

Access and guardrails

Section 02

Identity and access management

Secure your data, empower collaboration

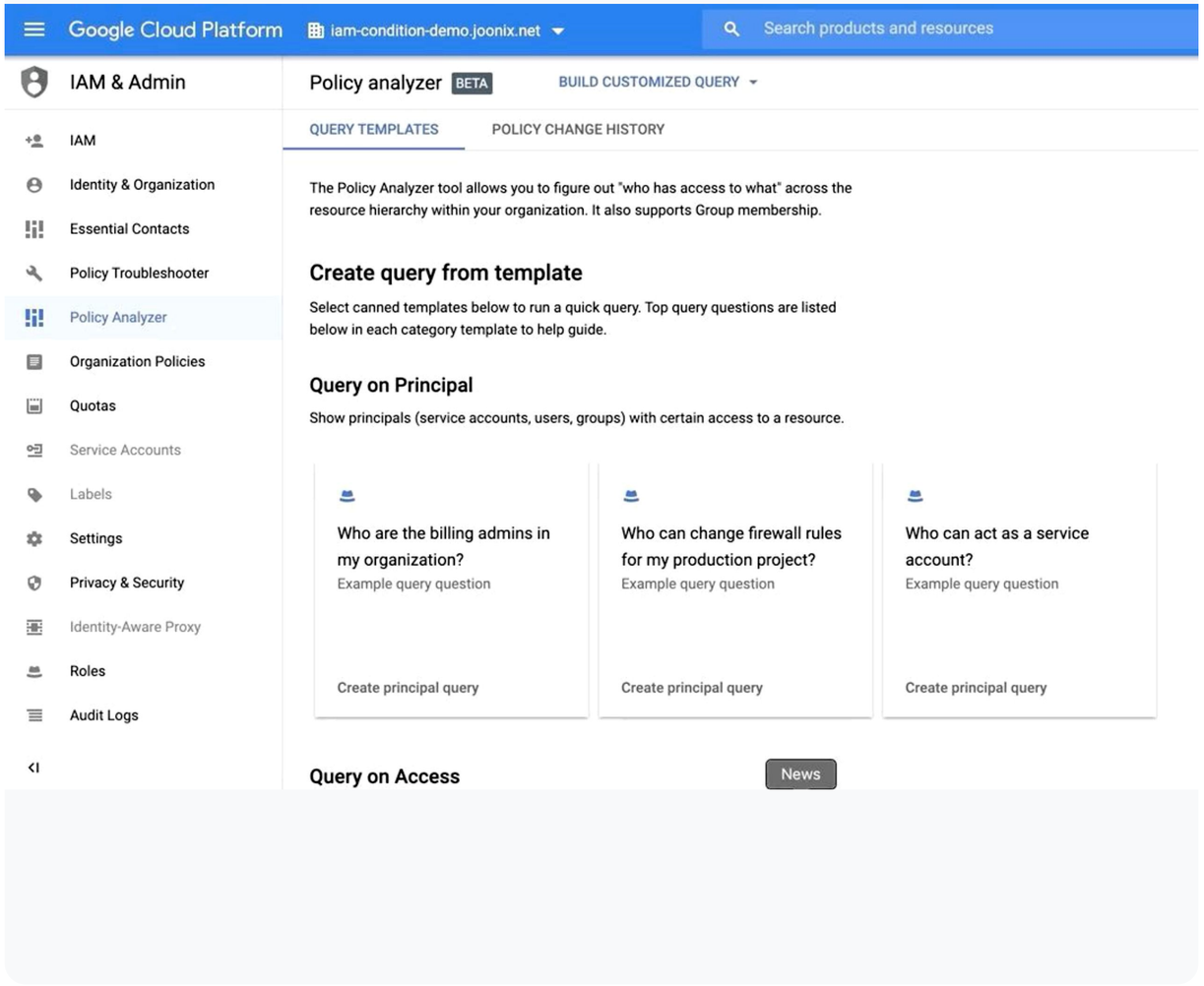
Google Cloud's Identity and Access Management (IAM) solutions provide precise control over who accesses your data.

With Cloud IAM, you have direct authority over not only your critical BigQuery data but also other key services like Cloud Run, Cloud Functions, and GKE resources. This ensures the right people have the right access, minimizing risks.

Worried about unauthorized logins?
Multi-factor Authentication adds another layer of defense, offering multiple verification methods—including Google Authenticator and phishing-resistant Titan Security Keys—to keep your data safe.

Need to collaborate externally?
Workforce Identity Federation lets you seamlessly integrate with third-party identity providers, ensuring secure and controlled access even when working with partners or contractors.

Learn more about IAM →



Access and organization policies

Precise control for cloud security

Google Cloud's Identity and Access Management (IAM), encompasses access and organization policies, and provides a robust framework for controlling who can interact with your cloud resources and what actions they can perform.

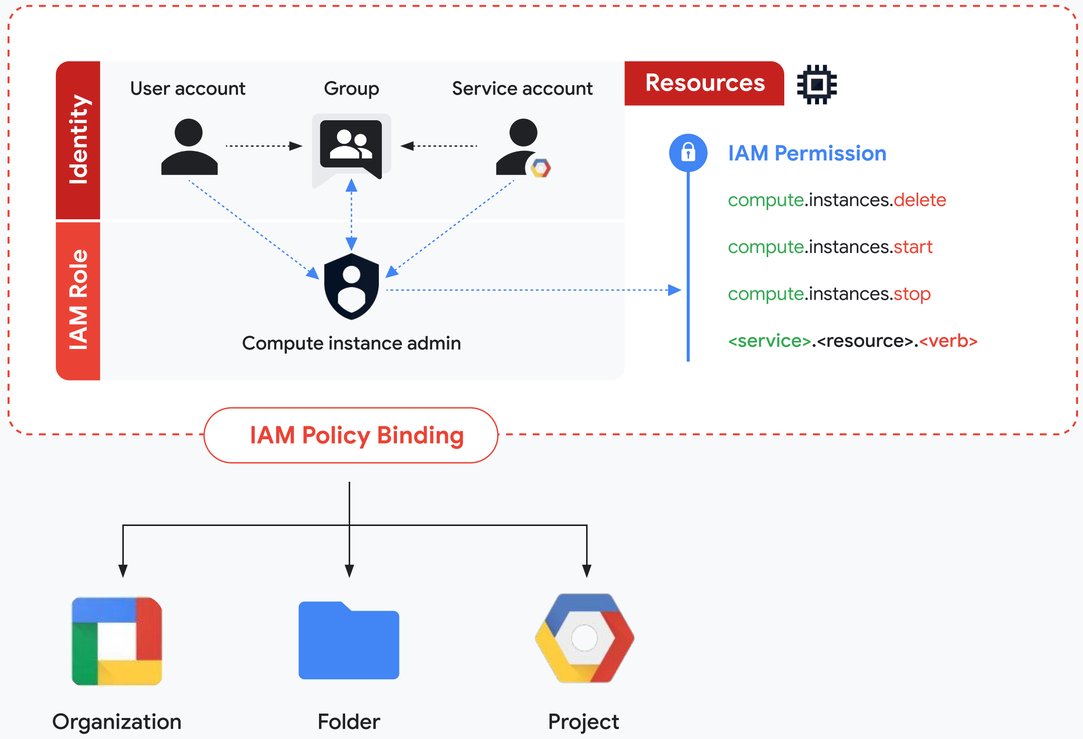
Organization policies offer a high-level way to govern resource usage and configurations across your Google Cloud projects. These policies consist of bindings that associate principals (users, groups, or service accounts) with specific roles. These roles, in turn, define the precise permissions granted to each principal on a given resource.

IAM access policies take this a step further, enabling extremely granular control. You can define both IAM Allow and IAM Deny policies, allowing you to explicitly permit or prohibit access to particular resources and actions. This level of granularity is essential for implementing the principle of least privilege, ensuring that users only have the access they need to perform their tasks.

Together, these capabilities give you the power to create a secure and well-managed cloud environment, where access is meticulously controlled to safeguard your sensitive data and critical operations.

Learn more about org policies →

IAM Policies bind identities, roles and resources



Organization restrictions

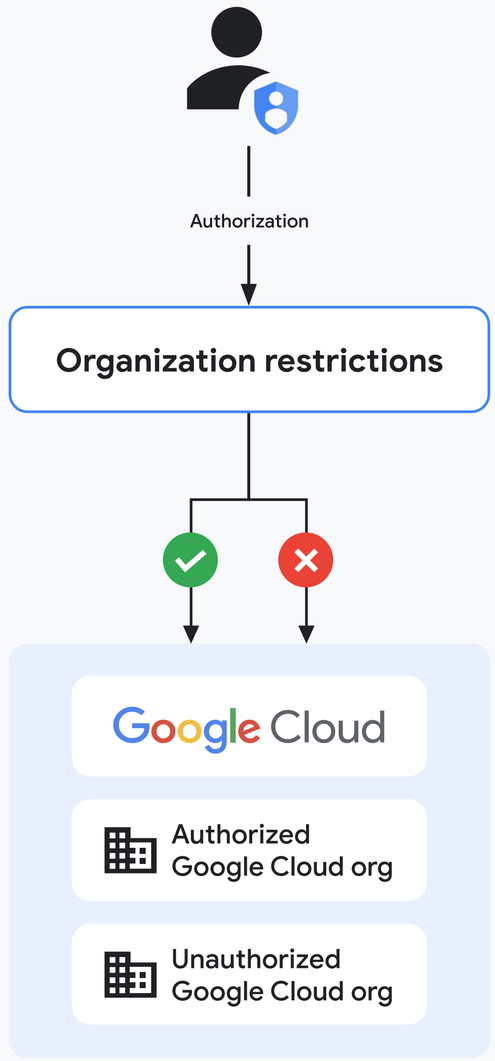
Reinforced protection against data exfiltration

Google Cloud Organization Restrictions add an extra layer of defense against data exfiltration by limiting access to only authorized Google Cloud organizations. This helps thwart threats like phishing attempts and insider attacks that aim to siphon off your valuable data.

When combined with Cloud IAM (Identity and Access Management), Organization Restrictions become even more potent. While IAM controls access to specific resources within an organization, Organization Restrictions control access to the organization itself. This double layer of protection ensures that only trusted entities can interact with your data.

Google Cloud enforces your organization policies diligently by inspecting requests based on organization restriction headers. This proactive approach adds an additional safeguard against unauthorized access.

In essence, Organization Restrictions help you build a secure perimeter around your Google Cloud environment, ensuring that your data stays within the confines of your trusted network.



“Identity and Access Management is crucial for cloud security, in our industry often combined with least privilege. When additional just-in-time access to specific resources by certain identities is needed, time-bound conditional access elevation becomes essential. With Google Cloud’s Privileged Access Manager there exists now an efficient service providing the functionality we need, including approval process and audit logging. This not only simplifies security scenarios, but also enables new opportunities such as adhoc insights into data, infrastructure knowledge sharing, or penetration testing support.”

Christian Gorke

Vice President and Head of Commerzbank’s Cyber Center of Excellence

COMMERZBANK

Source: https://cloud.google.com/blog/products/identity-security/move-from-always-on-privileges-to-on-demand-access-with-privileged-access-manager?e=48754805

Perimeter protection

Section 03

VPC Service Controls

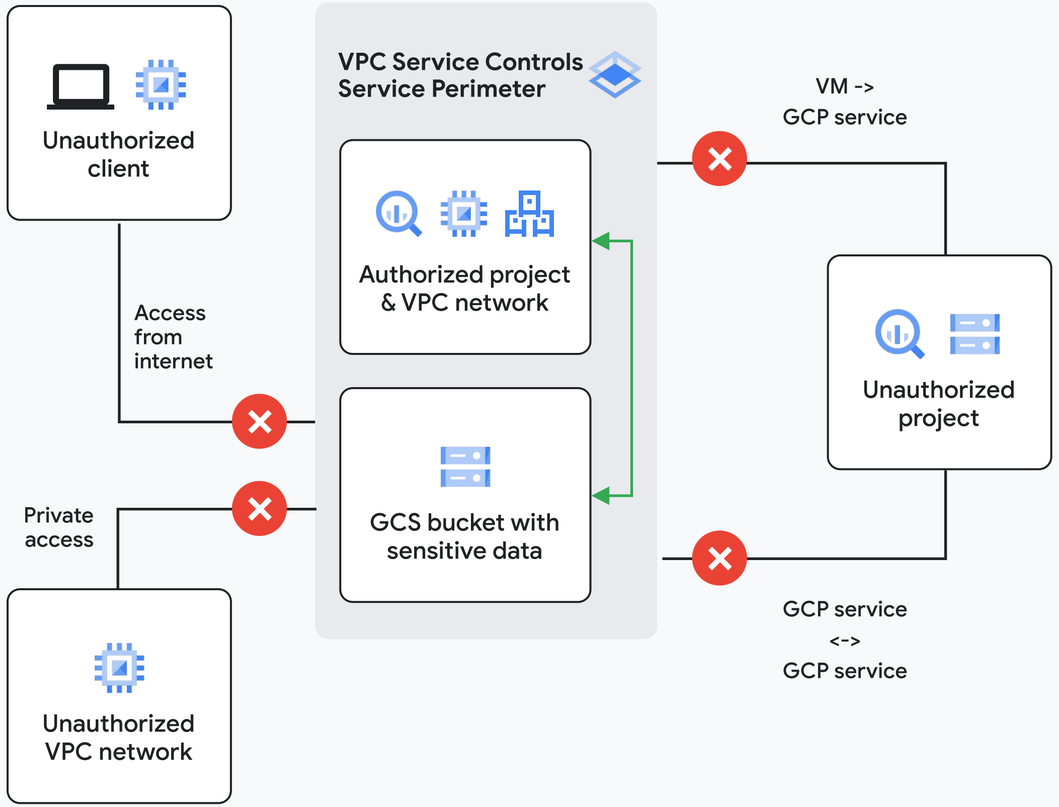
A virtual moat for your cloud data

VPC Service Controls help to prevent accidental leaks and thwart targeted attacks. This Google Cloud product establishes a protective perimeter around your valuable data, giving you fine-grained control over data access and movement.

Ingress policies let you define precisely which users or services can reach the data within your protected zone. Egress policies add another layer of security, restricting where that data can be sent.

VPC Service Controls acts as a robust complement to granular Cloud IAM policies and Organization Restrictions, providing a layered defense against data exfiltration. It ensures your sensitive information stays safe, allowing more time to focus on innovation, not data breaches.

Learn more about VPC Service Controls →



Cloud NGFW

Advanced network protection, simplified

Safeguard your valuable data with Cloud Next-Generation Firewall (NGFW), a powerful, cloud-native solution that simplifies network security without compromising on protection.

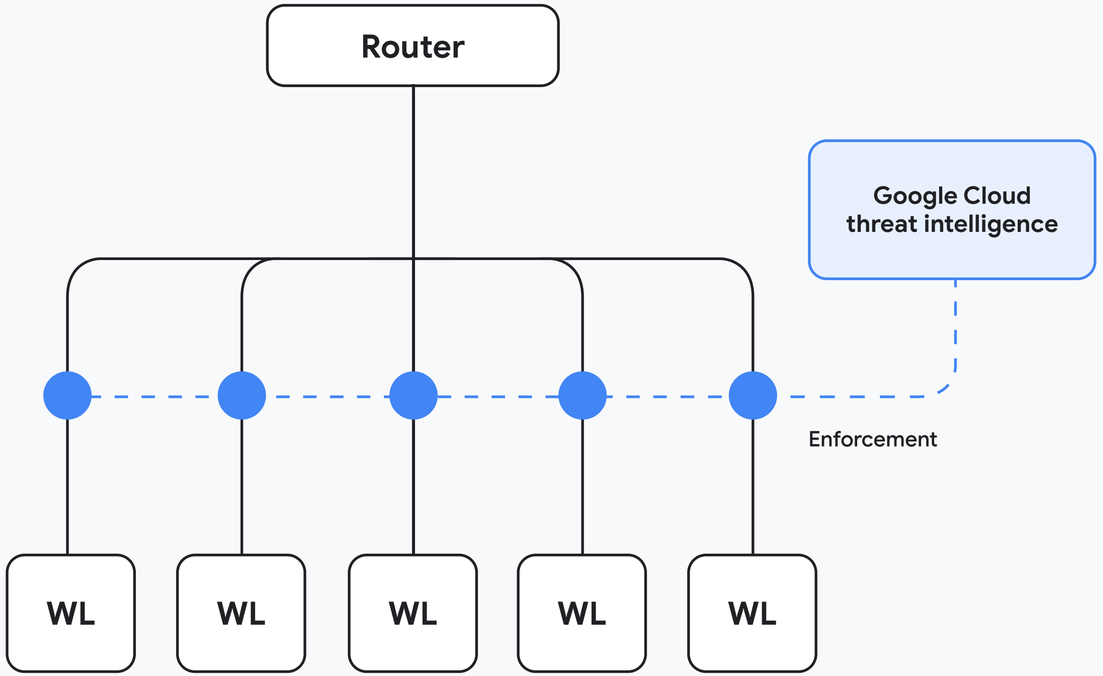
Designed for the cloud, it's quick and easy to deploy, delivering managed network threat detection and prevention that keeps your environment secure.

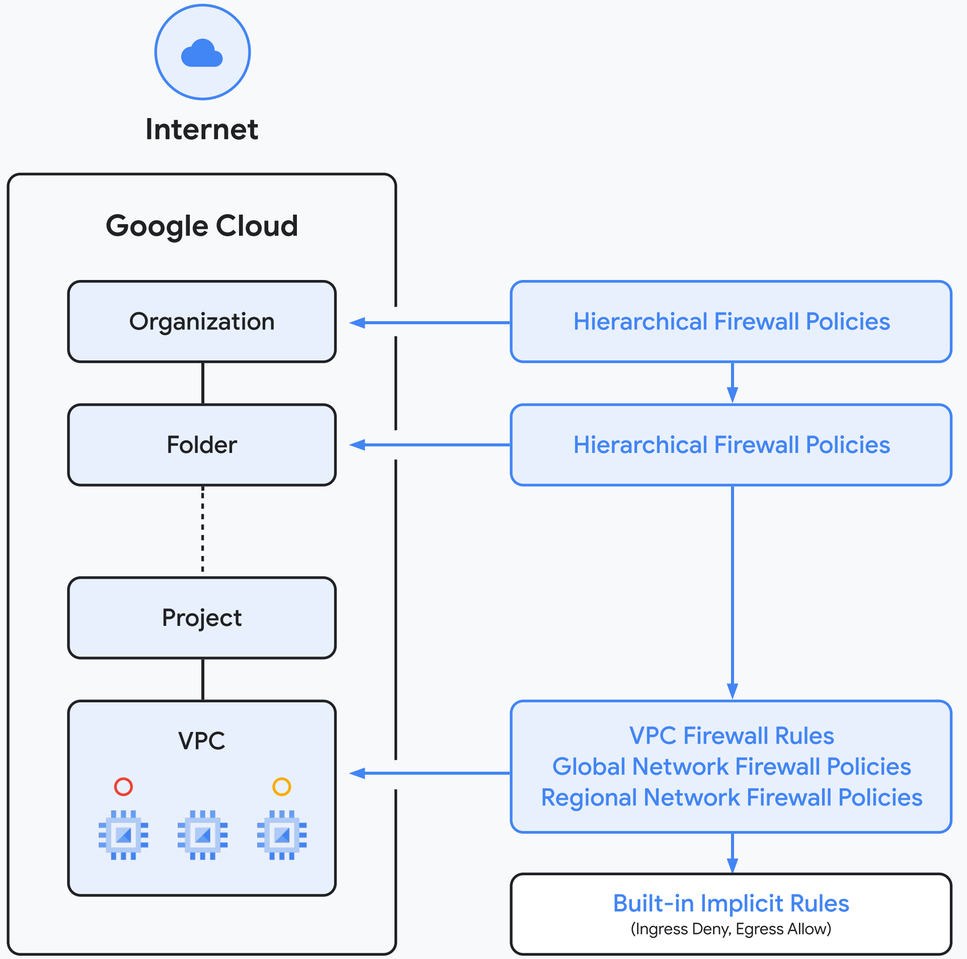
Cloud NGFW scales effortlessly to meet your needs, ensuring high performance and availability, even as your demands grow. The Enterprise tier takes protection further, offering industry-leading threat detection capabilities developed in partnership with Palo Alto Networks.

With Cloud NGFW, you gain complete visibility into your security posture. Any firewall violations are promptly surfaced through multiple channels, including a user-friendly interface, APIs, Cloud Logging, Google Security Operations, and even your preferred third-party SIEM/SOAR tools.

Learn more about Next-Generation Firewall →

Cloud NGFW


Router
Google Cloud threat intelligence
Enforcement
WL
WL
WL
WL
WL


Internet
Google Cloud
Organization
Folder
Project
VPC
Hierarchical Firewall Policies
Hierarchical Firewall Policies
VPC Firewall Rules
Global Network Firewall Policies
Regional Network Firewall Policies
Built-in Implicit Rules
(Ingress Deny, Egress Allow)

Cloud Armor

Shielding your web applications from cyber threats

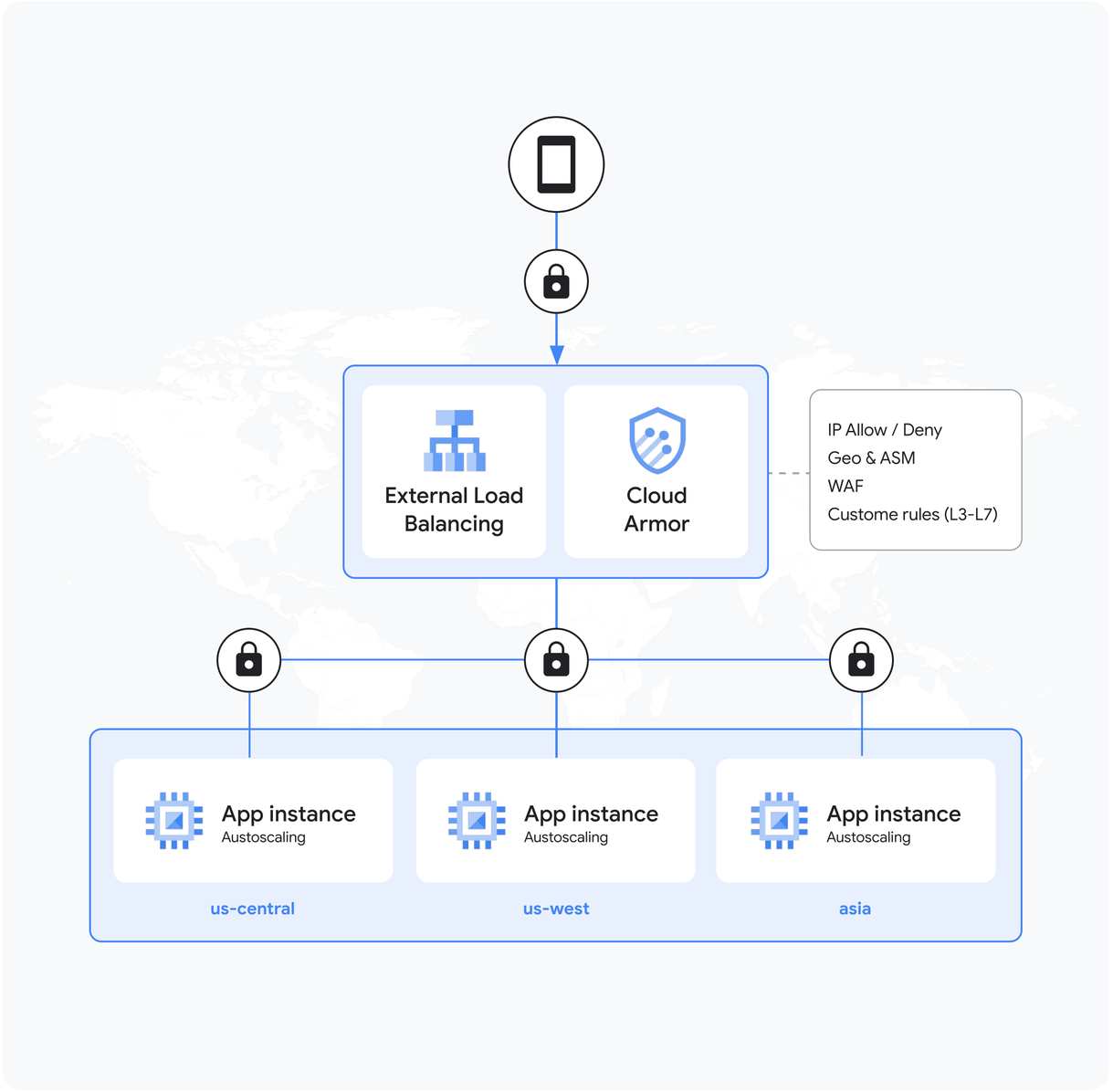
Cloud Armor provides a powerful, multi-level defense against a range of threats aimed at your web applications and services.

This robust solution stops not only large-scale Distributed Denial of Service (DDoS) attacks designed to overwhelm your systems but also defends against insidious threats, like cross-site scripting (XSS) and SQL injection (SQLi), that can compromise sensitive data.

Seamlessly integrated with Google Cloud Load Balancer, Cloud Armor gives you comprehensive control over your traffic while actively mitigating threats. You can define protection based on various factors such as geographic location, known threat intelligence, and specific IP addresses.

But Cloud Armor doesn't stop at static rules. Its Adaptive Protection feature employs machine learning to analyze traffic patterns, detect anomalies, and even suggest Web Application Firewall (WAF) rules to counter emerging attack vectors.

Learn more about Cloud Armor →



> Thanks to Cloud Armor, we have strengthened the security posture of the Symantec network security infrastructure that provides leading, enterprise-grade solutions for our customers. And as a bonus, this lowers operational overhead, freeing Broadcom internal resources to focus on developing cutting-edge software solutions that address many of the industry's greatest cybersecurity challenges."

Ben-Haroche

Platform Group Manager, Broadcom

BROADCOM®

Source: https://cloud.google.com/blog/products/identity-security/how-google-cloud-armor-helps-broadcom-block-ddos-attacks?e=48754805

Data protection

Section 04

Sensitive Data Protection

Safeguarding your valuable information

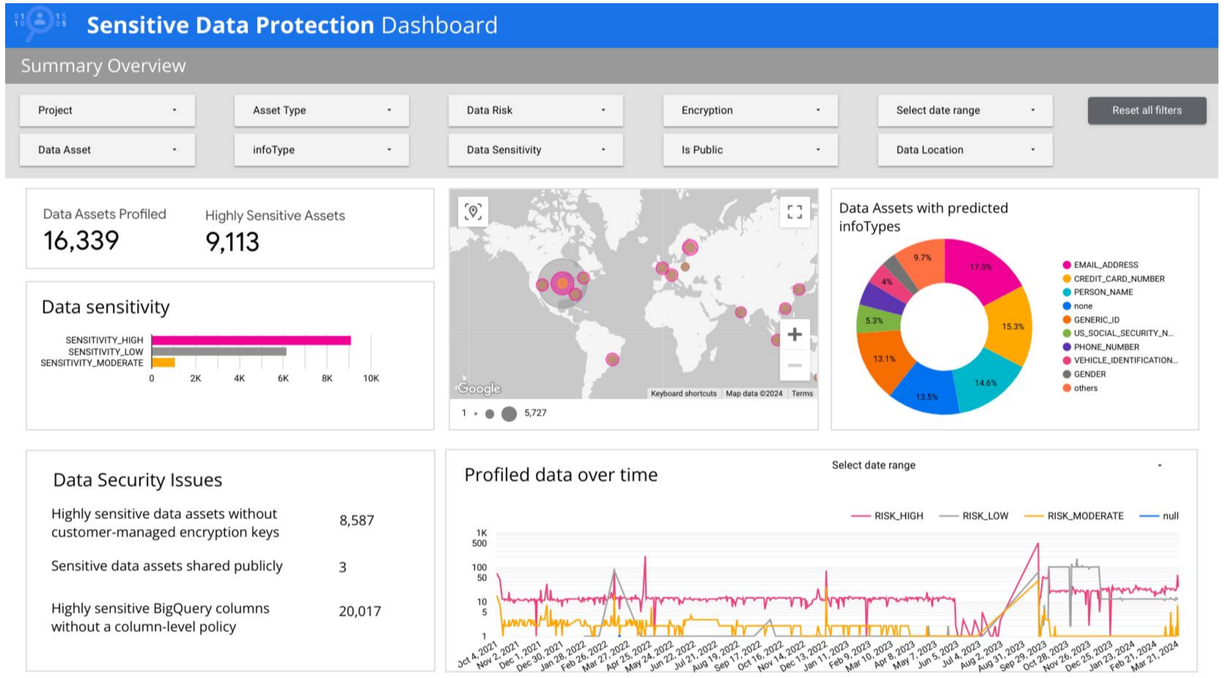
Google Cloud's Sensitive Data Protection offers a comprehensive suite of tools to help you not just identify sensitive data but actively protect it, mitigating risks and maintaining compliance within your BigQuery environment.

Start with continuous discovery which scans and classifies your data to understand its composition and pinpoint any associated risks. Then, you can take proactive measures to protect this information. Obfuscation and de-identification techniques mask sensitive elements, while redaction, masking, tokenization, and transformation provide further layers of security for both structured and unstructured data, including images.

With a library of over 150 pre-defined detectors and the option to create custom ones, Sensitive Data Protection is adaptable to your specific business requirements. The flexibility ensures you can address the unique nature of your data and potential threats.

To provide even deeper insights, Sensitive Data Protection findings can be integrated with Security Command Center (SCC). These findings along with virtual red team technology, allows you to analyze potential attack patterns and gain valuable context about the types of data that might be targeted.

Learn more about Sensitive Data Protection →



Secret Manager

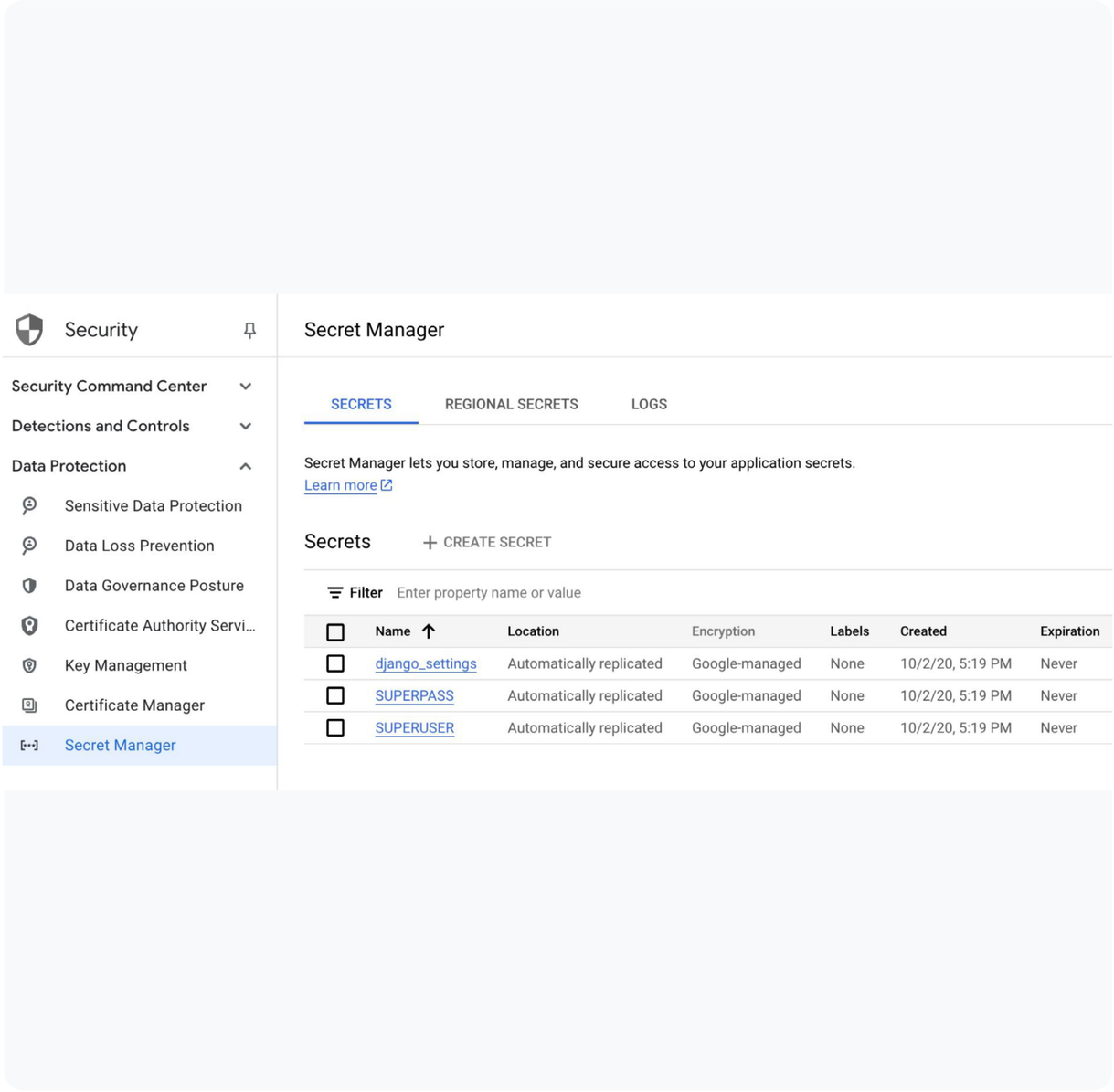
Protect your secrets

In the world of cloud computing, keeping sensitive data secure is paramount. Google Cloud Secret Manager provides a robust solution for protecting your most valuable secrets, such as API keys, passwords, certificates, and other credentials.

It's not just about storage. Secret Manager enforces strict access control policies, ensuring that only authorized users and services can access your secrets. Automatic secret versioning and comprehensive audit logging further enhance security and compliance.

Seamless integration with BigQuery enables a streamlined workflow. Grant users one-click access to data without the need to expose sensitive passwords, minimizing the risk of accidental leaks or misuse

Learn more about Secret Manager →



Cloud KMS and HSM

Take control of your data encryption in Google Cloud

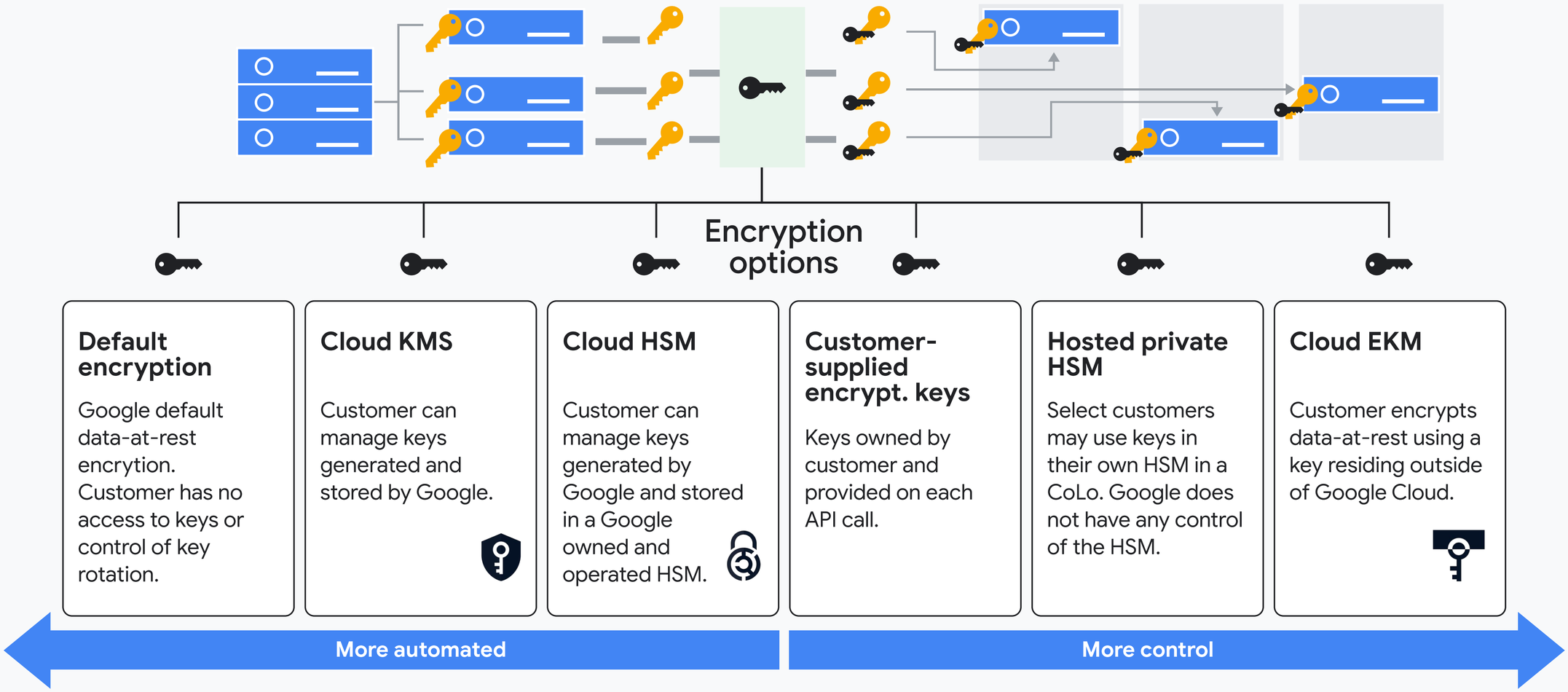
Google Cloud prioritizes data security. BigQuery encrypts your data at rest by default, but if you desire greater control over your encryption keys, Cloud KMS and HSM offer that flexibility.

With Customer-Managed Encryption Keys (CMEK) for BigQuery, you take ownership of the encryption keys that safeguard your data. This means you control key creation, rotation, tracking, and deletion within Cloud KMS, aligning encryption practices perfectly with your specific security and compliance requirements.

Cloud KMS simplifies key management, while Cloud HSM adds an extra layer of security with FIPS 140-2 Level 3 certified hardware. The familiar Cloud KMS API frontend makes it easy to integrate HSM into your existing workflows.

Learn more about key management →

Cloud KMS and HSM



“Google Cloud Sensitive Data Protection (SDP) provides us a way to scan the entirety of our BigQuery data and apply business-specific rules and edge cases to tune the performance of data profiling. This has significantly increased our understanding of our PII footprint, not just within our data warehouse but across the business.”

Anthony Tsoi

DataOps Lead Engineer at Charlotte Tilbury Beauty

CharlotteTilbury

Source: https://cloud.google.com/blog/topics/customers/how-charlotte-tilbury-beauty-responds-to-customer-data-requests?e=48754805

Monitoring and compliance

Section 05

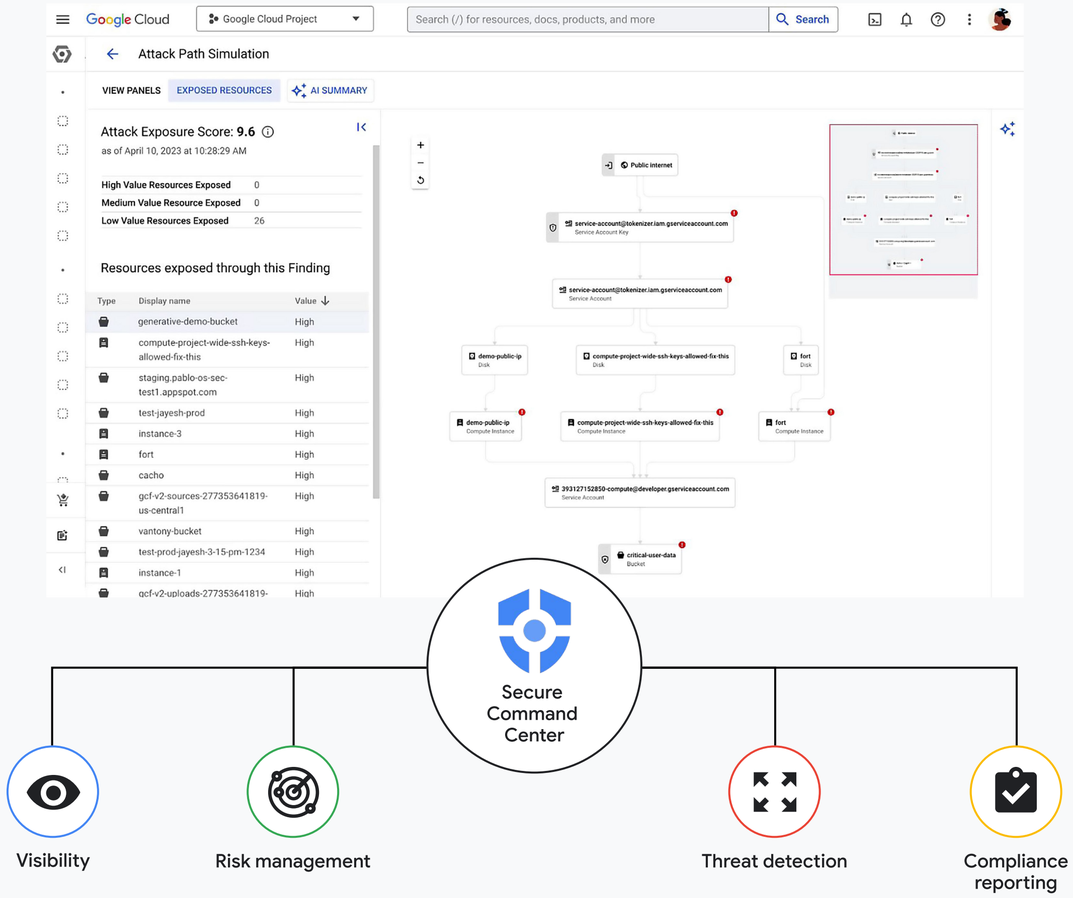
Security Command Center

Security Command Center helps to bolster your security posture, actively manages cloud risk, and ensures your organization's most valuable asset—its data—remains protected and compliant.

Through seamless integration with BigQuery, Security Command Center offers direct visibility into your datasets, allowing you to identify and address potential vulnerabilities and misconfigurations within your data warehouse.

With the Security Command Center's watchful eye on BigQuery, you can prevent unauthorized access and data exfiltration attempts before they cause damage.

Automated compliance reporting makes it easier for data leaders to maintain compliance with data protection regulations. When coupled with the proactive recommendations powered by Gemini AI, your team can continuously refine your BigQuery security strategy, ensuring it evolves alongside the ever-changing threat landscape.



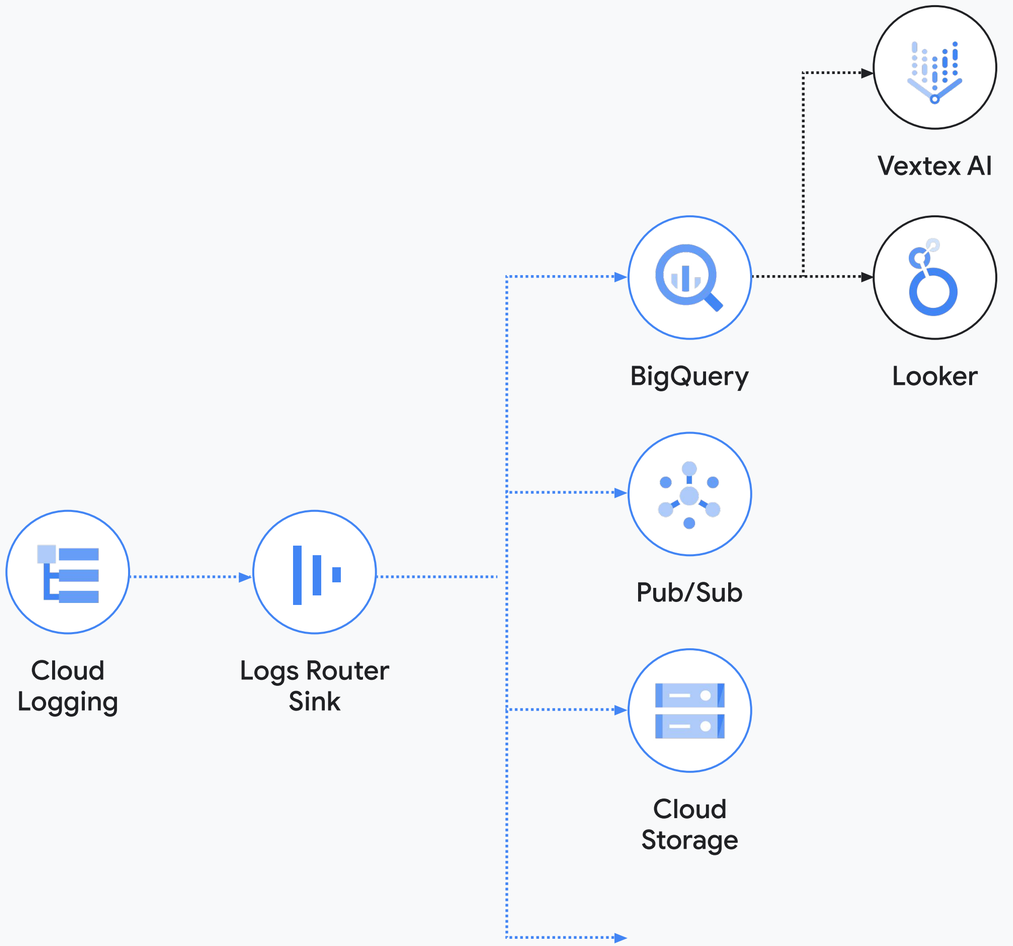
[Learn more about Security Command Center](#)

Cloud Logging

Google Cloud Logging offers comprehensive log collection, storage, and analysis capabilities to enhance your data security posture.

With logging across crucial Google Cloud services like BigQuery, App Engine, Cloud Run, GKE, and Compute Engine VMs, you gain complete visibility into system activities and data access patterns. This real-time insight empowers you to detect anomalies, investigate potential threats, and respond swiftly to security incidents.

The flexibility of Cloud Logging's storage options, ranging from default retention to long-term archival, ensures that you have access to historical log data for compliance audits and forensic investigations. Moreover, the ability to export logs to BigQuery allows for in-depth analysis and correlation with other data sources, enabling you to uncover hidden patterns and potential vulnerabilities.



Learn more about Google Cloud Logging

Assured Workloads

Simplified compliance and security in the cloud

Managing sensitive data and workloads in the cloud can be complex, especially when juggling compliance and security requirements. Assured Workloads offers a streamlined solution.

With Assured Workloads, you confidently secure and configure your sensitive resources to align with your organization's specific needs. It's about taking the guesswork out of cloud security. Simply choose your desired security settings – think data location, access controls, encryption levels – and Google Cloud implements the necessary controls for you.

This approach helps you to maintain regulatory compliance while protecting your critical assets. Assured Workloads eliminates the complexity, so you can focus on leveraging the cloud's full potential with peace of mind.

Learn more about Assured Workloads →

Compliance

- Data location
- Personnel access
- Inherited controls

Assured workloads

1. Select regulated access needs
2. Set the location of data at rest
3. Configure key management
4. Create the regulatory boundary

Compliance with confidence

Repeatable deployments

Confidently secure and configure sensitive workloads in alignment with your compliance needs.

Compliance made simple

Repeatable enforcement

Enforce restriction of resources, personnel, and data location to a selection region of your choice.

> We chose to deploy with Google Cloud Assured Workloads because it provides us with the security controls we need and helps address a wide range of compliance requirements. Our ability to meet requirements around the globe enables us to grow our business while reducing the overhead and complexities of the multinational compliance process.”

David Williams

Cloud Manager, Iron Mountain

IRON MOUNTAIN®

Source: https://cloud.google.com/blog/products/identity-security/how-iron-mountain-uses-assured-workloads-to-serve-customer-compliance-needs

Google Cloud

Learn more about Cyderes and Cloud Security