

IDENTITY & SECURITY

Advancing control and visibility in the cloud

Sunil Potti

VP/GM, Google Cloud

November 20, 2019



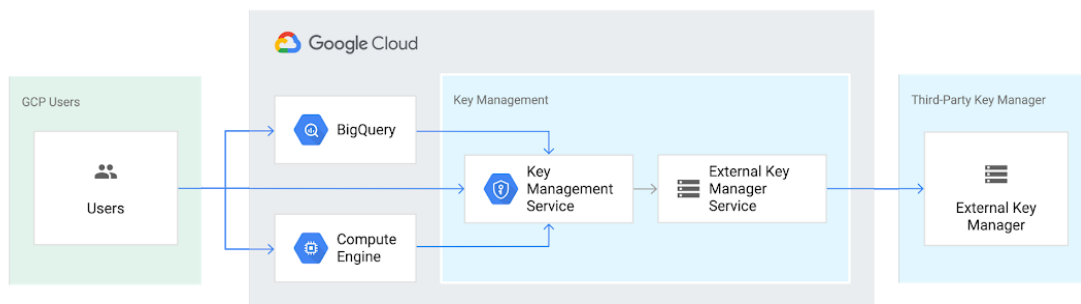
At Google Cloud, we work tirelessly to give our customers increasing levels of control and visibility over their data. Today in London at Next UK, we're announcing new capabilities for data encryption, network security, security analytics, and user protection designed to deliver on that promise.

External Key Manager: Store and manage encryption keys outside of Google Cloud



Find an article...

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)



To make this new service easy to implement, we are working with five industry-leading key management vendors: [Equinix](#), [Fortanix](#), [Ionic](#), [Thales](#) and [Unbound](#).

Key Access Justifications: Decide when and why your data can be decrypted

We believe that trust in the cloud is created through transparency. Google Cloud led the industry in providing meaningful transparency into [provider access to customer data](#), and now we're extending that transparency to use of encryption keys. [Key Access Justifications](#) is a new feature that will work with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set.

🔍 Find an article...

[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)



- Cloud HSM availability in all Google Cloud regions and multi-regions (with the exception of global multi-region)

All these updates offer you more control over how your data is protected.

Defend against internet threats

When you stand up applications on Google Cloud, you benefit from DDoS and web attack protection at Google scale. [Google Cloud Armor](#) works with our global [Cloud Load Balancing](#) infrastructure and provides always-on attack detection and mitigation so you can run your business without interruption.

Today, we're pleased to announce the beta of Cloud Armor's new web application firewall (WAF) capabilities to help protect applications against targeted and distributed internet threats. You can now configure Cloud Armor policies with geo-based access controls, pre-configured WAF application protection rules to mitigate [OWASP Top 10](#) risks, and a custom rules language to create custom Layer-7 filtering policies.

Cloud Armor also now integrates with [Cloud Security Command Center](#) (Cloud SCC), notifying customers of suspicious application traffic patterns directly in the Cloud SCC dashboard.

Cloud Armor: DDoS Protection & WAF



[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)



Our new [Packet Mirroring](#) service, now in beta, allows you to collect and inspect network traffic for Compute Engine and GKE; it's available for all machine types in all of our regions. With this service, you can use third-party tools to more proactively detect threats, better respond to intrusions with signature-based attack detection, and better identify zero-day attacks with anomaly detection. For more, watch this [video](#).

We've built an ecosystem of partners so you can use Packet Mirroring with third-party tools of your choice, including products from [Awake Security](#), [Check Point](#), [Cisco](#), [Corelight](#), [cPacket Networks](#), [ExtraHop Networks](#), [Flowmon](#), [Ixia by Keysight](#), [Netscout](#), and [Palo Alto Networks](#).

Protect G Suite and Cloud Identity users

Google's [Advanced Protection Program](#) is our strongest protection for users at risk of targeted attacks. In the enterprise, this includes IT administrators and executives. Today, the Advanced Protection Program is starting to roll out to G Suite and Cloud Identity customers. With the Advanced Protection Program for the enterprise, we'll enforce a specific set of policies for enrolled users including [security key](#) enforcement, blocking access to untrusted apps and enhanced scanning for email threats. [Learn more](#).

We're also introducing app access control, helping you reduce the risk of data loss by limiting access to G Suite APIs to third-party apps you trust. You can also more easily manage and restrict which Google APIs are available for use by third-party and

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)

Google threat intelligence to help you spot and stop threats before they result in



As we continue to innovate and simplify security management on GCP, Event Threat Detection and Security Health Analytics will be bundled in a Premium Edition of Cloud Security Command Center with other new capabilities that help you meet industry compliance requirements, catch web application vulnerabilities, detect compromised VMs, and discover other threats. The Premium Edition will give you a comprehensive, easy-to-deploy set of tools to protect your cloud resources. To learn more about how to use Cloud Security Command Center, check out our recent [video series](#).

Chronicle: security analytics wherever your apps are deployed

Chronicle's Backstory product was designed by former Google security professionals to enable anyone to use the types of techniques we use to detect threats and investigate security incidents. It brings world-class strengths in data analytics to your security data, privately and easily.


Many organizations leverage a mix of on-prem environments and multiple clouds to run their applications, making it difficult to collect and store security telemetry from various systems and tie individual events together for analysis. Backstory, our flagship offering for hybrid security analytics, offers you this level of intelligence. With just a few clicks, in minutes, you can aggregate and analyze your security telemetry wherever your apps may run, and where they might run in the future.

Be sure to check out the Chronicle booth during Next UK to learn more!

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)



Blog

Menu 

Follow Us




Google

[Privacy](#)

[Terms](#)

[About Google](#)

[Google Cloud Products](#)

Language 



[Help](#)