



# LOOKOUT CLOUD KEY SECURITY

MANAGE AND SECURE YOUR ENCRYPTION KEYS FOR THE LOOKOUT SECURITY GRAPH

## Customer Problem

In a cloud-centric world, you need to stay ahead of evolving threats to secure the cloud services you use and remain compliant with government and industry regulations. Your data in cloud services must be protected from all threats to cloud infrastructure, including insider threats.

We encrypt your organization's personally identifiable information (PII) data end-to-end across cloud infrastructure of the Lookout Security Graph. But if you're an organization that holds particularly valuable data and is continuously targeted by internal and external attacks, you require an extra level of security.

## Case Study in Cloud Security

A former employee of a cloud infrastructure provider used their knowledge of the provider's operations to steal more than 1.2 million data records that included sensitive personally identifiable information (PII). The former employee may also have had access to multiple regional instances, collecting tens of gigabytes of data from multiple customers. While they did not sell the stolen data, it is likely that this threat actor shared processes to enable others to leverage vulnerabilities in cloud infrastructure.

## BENEFITS OF CLOUD KEY SECURITY

- Securely controls and manages encryption keys for cloud infrastructure
- Stops unauthorized access to your encryption keys
- Detects and prevents tampering of keys from insider threats
- Meets FIPS 140-2 Level 3 certification
- Delivers security while limiting latency for cloud infrastructure

## Customer Challenge

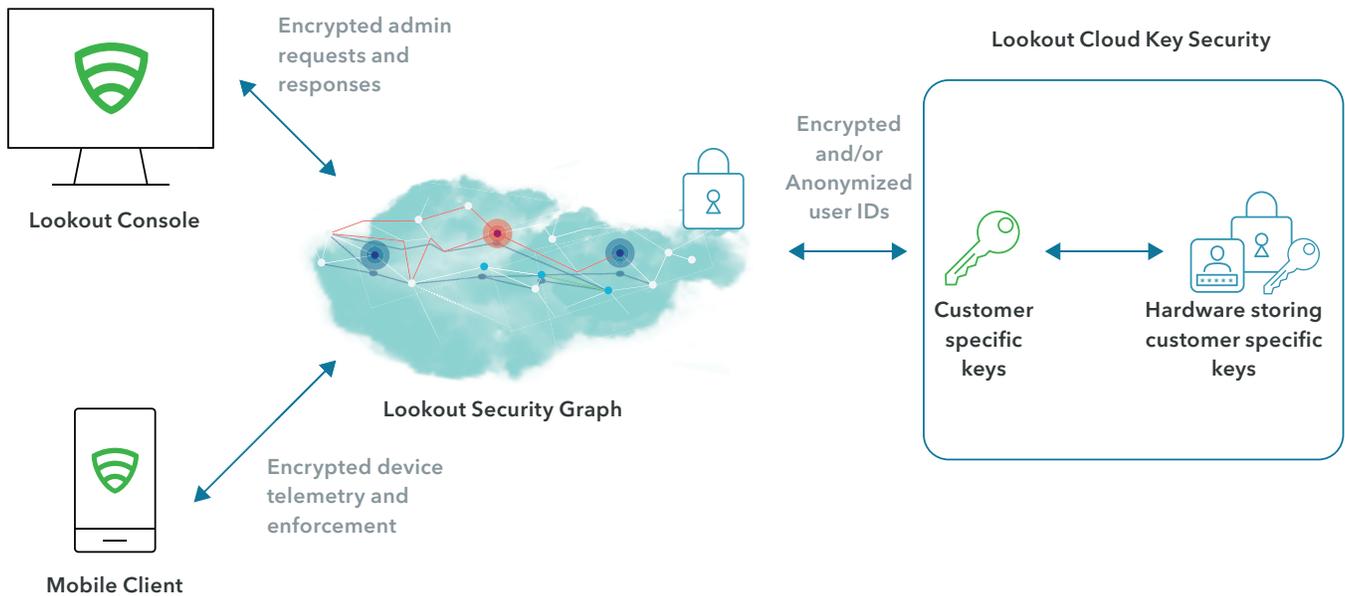
To protect your data as it moves through cloud infrastructure, you have to control and manage the storage, rotation, and deletion of your encryption keys. It is critical to limit encryption key access rights to the absolute minimum number of administrators required and prevent your keys from leaving tamper-resistant storage. At the same time, secure storage of your encryption keys should not slow down your critical cloud operations.

These encryption controls for cloud infrastructure should extend to all data that supports your infrastructure for mobile security, across the Lookout security platform, as well as your mobile device management (MDM) and Security information and event management (SIEM).

## The Solution

Lookout Cloud Key Security offers single-tenant access to tamper resistant FIPS 140-2 Level 3 Hardware Security Modules (HSMs). This gives you control over the management and storage of encryption keys that protects your mobile infrastructure connections across multiple virtual instances. In addition to providing you with greater security controls for Lookout cloud infrastructure, we use our HSM to secure and manage all external connections between Lookout and any MDM and SIEM platforms you use.

## How Lookout Cloud Key Security works: separation of duties



- Lookout monitors the health and network availability of Cloud Key Security.
- You manage the key material stored in the HSM used to deliver Cloud Key Security.

To complement the encryption of data-at-rest and data-in-transit within our infrastructure, we ensure that each datastore is deployed in its own virtual private cloud instance to provide additional isolation for your data.

## About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

For more information visit  
[lookout.com](https://lookout.com)

Request a demo at  
[lookout.com/request-a-demo](https://lookout.com/request-a-demo)

---

© 2021 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20210108-Lookout-USv1.0