Honeycomb Secure Tenancy

Honeycomb Secure Tenancy provides two options to address your security/compliance requirements while delivering access to the fine-grained observability that you need.

Both options make use of a Honeycomb Secure Proxy running in your infrastructure. No plaintext data ever traverses Honeycomb's infrastructure and the Honeycomb UI presents complete transparency to authorized members of your team. You have complete control of key rotation and reissuance down to the columnar level from within your own infrastructure.

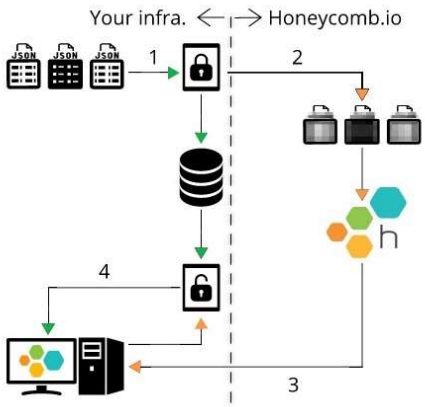
Option 1: Event Encryption

With Event Encryption, your datasets are encrypted and the keys are stored in a database on the Secure Proxy running in your infrastructure. When an authorized user accesses Honeycomb, their web browser connects to the Secure Proxy directly and the data is unencrypted for them. Honeycomb infrastructure never has access to the sensitive data in plaintext.

Option 2: Event Hashing

With Event Hashing, your datasets are hashed and the hash mappings are stored in a database on the Secure Proxy running in your infrastructure. When an authorized user accesses Honeycomb, their browser sends the hashed data to the Secure Proxy running in your environment and receives the unhashed data back. Again, no plaintext data reaches the Honeycomb infrastructure.

How the data flows

	1 Your data is masked by the Secure Proxy before it leaves your network.
	2 The masked data is sent to Honeycomb while the keys remain on-premises.
	3 An authorized user queries the data in Honeycomb via their browser.
	4 The user's browser sends the masked data to the Secure Proxy and receives unmasked data.