IRONCORE LABS

Cloaked Search Datasheet

Bringing the power of encrypted search to Elasticsearch and OpenSearch.

# HOW CLOAKED SEARCH GOT STARTED

Elasticsearch is the most commonly used search software. Solr comes next. And they're all underpinned by Lucene, which brings most of the search functionality. These products are packed with features for scalability, redundancy, customizable rankings, and expressive queries.

IronCore Labs built Cloaked Search as a **no-code encrypted search proxy** that sits in front of Elasticsearch or OpenSearch. Cloaked Search allows users to retain the performance, resiliency, scalability, and power of Elasticsearch while protecting their data from hackers, curious administrators, and service providers — without worrying about data breaches or liability.

# EXPANDING ACCESS TO ELASTICSEARCH AND OPENSEARCH

Before Cloaked Search, companies had to limit what data would be searchable from Elasticsearch or OpenSearch to protect sensitive customer data. But with Cloaked Search, you're able to store more data than ever before and still keep that data private and secure. **Here are three pain points where Cloaked Search makes an immediate impact.**

1 Many companies choose to not use Elasticsearch for sensitive customer data due to limited options for securing data.

2 If multiple customers have data stored in the same index, a programming error or exploit could return data to an unauthorized person.

3 Index terms extracted from your documents are stored in Elasticsearch in plaintext, and curious admins or hackers can use that to gain a lot of information.
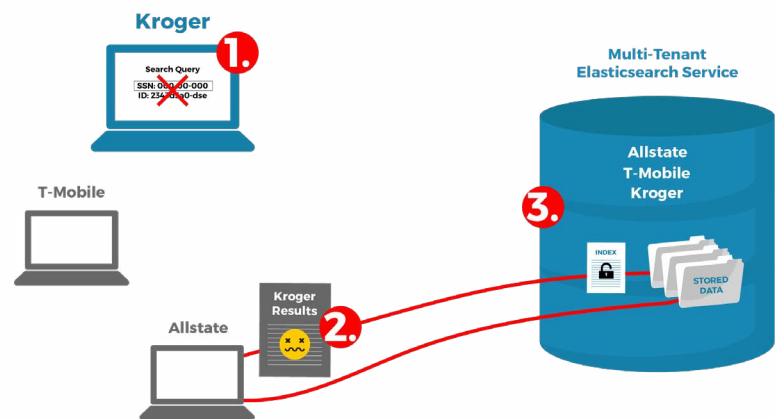
HOW CLOAKED SEARCH WORKS

The Cloaked Search proxy sits in front of Elasticsearch or OpenSearch. For most applications, all you need to do is point your code to the proxy and everything will work as it did before with similar rankings and results. You configure which fields should be encrypted in which indices along with per-field options. When indexing or searching documents, the proxy will automatically encrypt the documents and queries as needed.
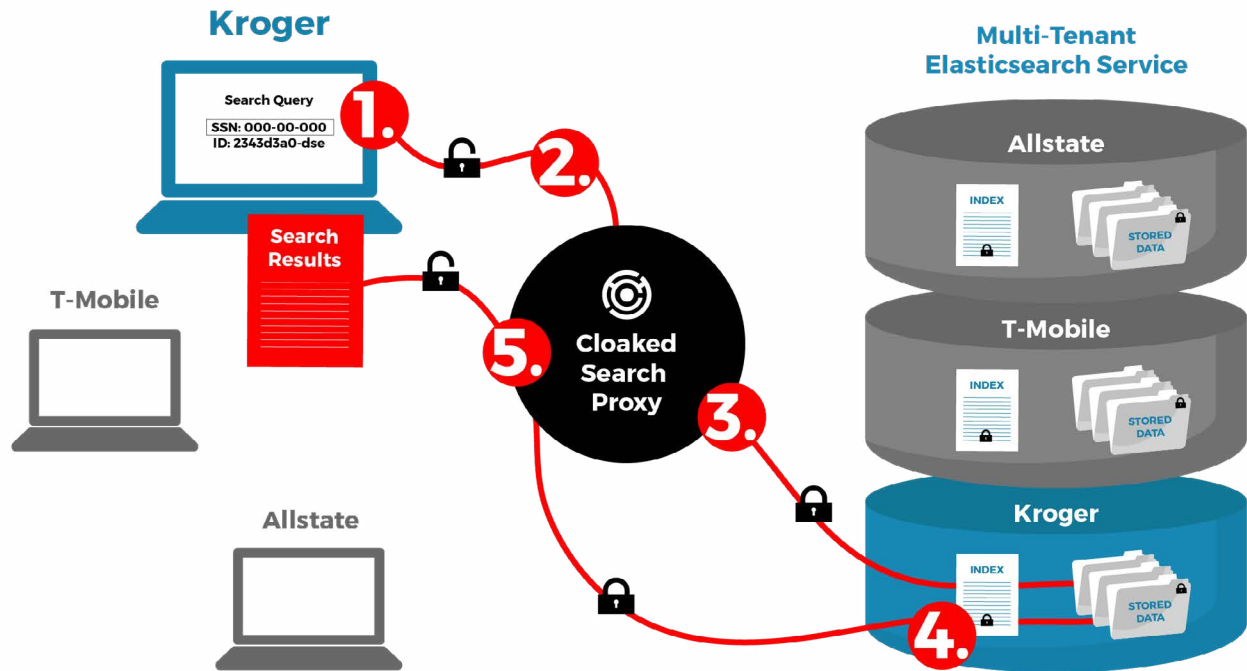
CLOAKED SEARCH SECURITY EXPLAINED IN 5 STEPS

1   A customer performs a search for a social security number, which you've pre-configured as a protected field.

2   The search query is sent with the customer's ID to the Cloaked Search Proxy.

3   Cloaked Search fetches the encryption key for the current customer, cryptographically secures the SSN with it, and sends the protected query to Elasticsearch.

4   Elasticsearch finds all results with SSNs that match the protected search query and returns their associated encrypted documents to Cloaked Search.

5   Cloaked Search uses the per-customer key to decrypt the data and returns the search results to the customer with low latency.

Get Started

IRONCORE LABS

ABOUT IRONCORE

We are a data privacy platform for application-layer encryption and customer managed keys (CMK). We enable software developers and businesses to rapidly build enterprise applications with strong data control. Data owners decide who can access their data, monitor how it's used, when, where, and by whom, and can revoke that access at any time. We are the fastest and easiest way to control data in multi-cloud and SaaS environments.

IronCore Labs
1750 30th Street #500
Boulder, CO 80301, USA

Inquiries
Email: info@ironcorelabs.com
Phone: +1.415.968.9607

CONNECT WITH US

blog.ironcorelabs.com

linkedin.com/company/ironcore-labs

twitter.com/ironcorelabs

ironcorelabs.com