OVERVIEW AND ARCHITECTURE

# IN A NUTSHELL

▶ Search Guard is an Open Source security plugin for Elasticsearch

▶ Provides TLS encryption on the transport and REST layer

▶ Fine-grained access control for indices, types and fields

▶ Pluggable authentication methods

    ▶ LDAP, Active Directory, SPNEGO/Kerberos, Internal

▶ Document- and Field-level-security, audit logging

SECURING YOUR TRAFFIC

- ▶ Provided by Search Guard SSL

    - ▶ Responsible for TLS on REST- and transport layer

    - ▶ Encrypt inter-node and HTTP traffic

    - ▶ Make sure nobody tampers with your data

    - ▶ Make sure only trusted nodes join the cluster

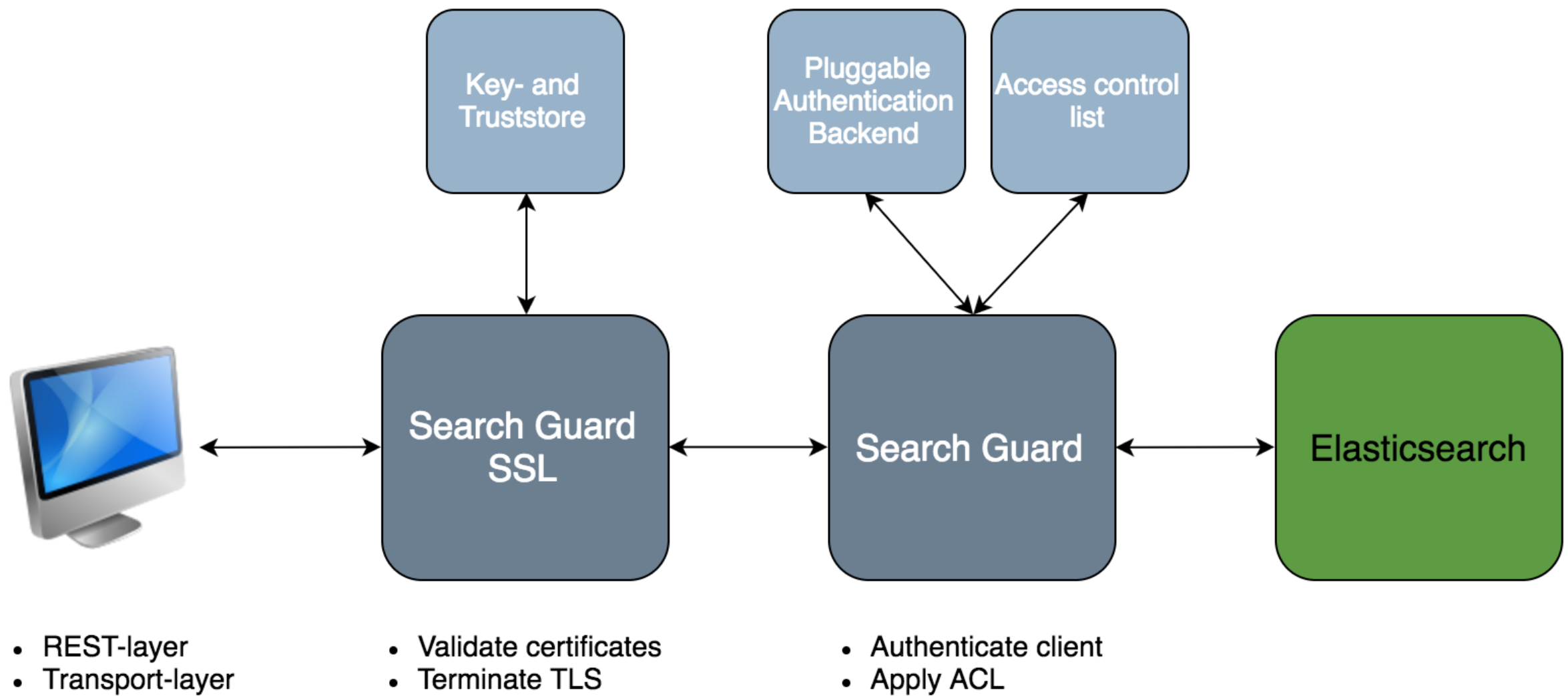- ▶ Supports OpenSSL for improved performance

SEARCH GUARD SSL
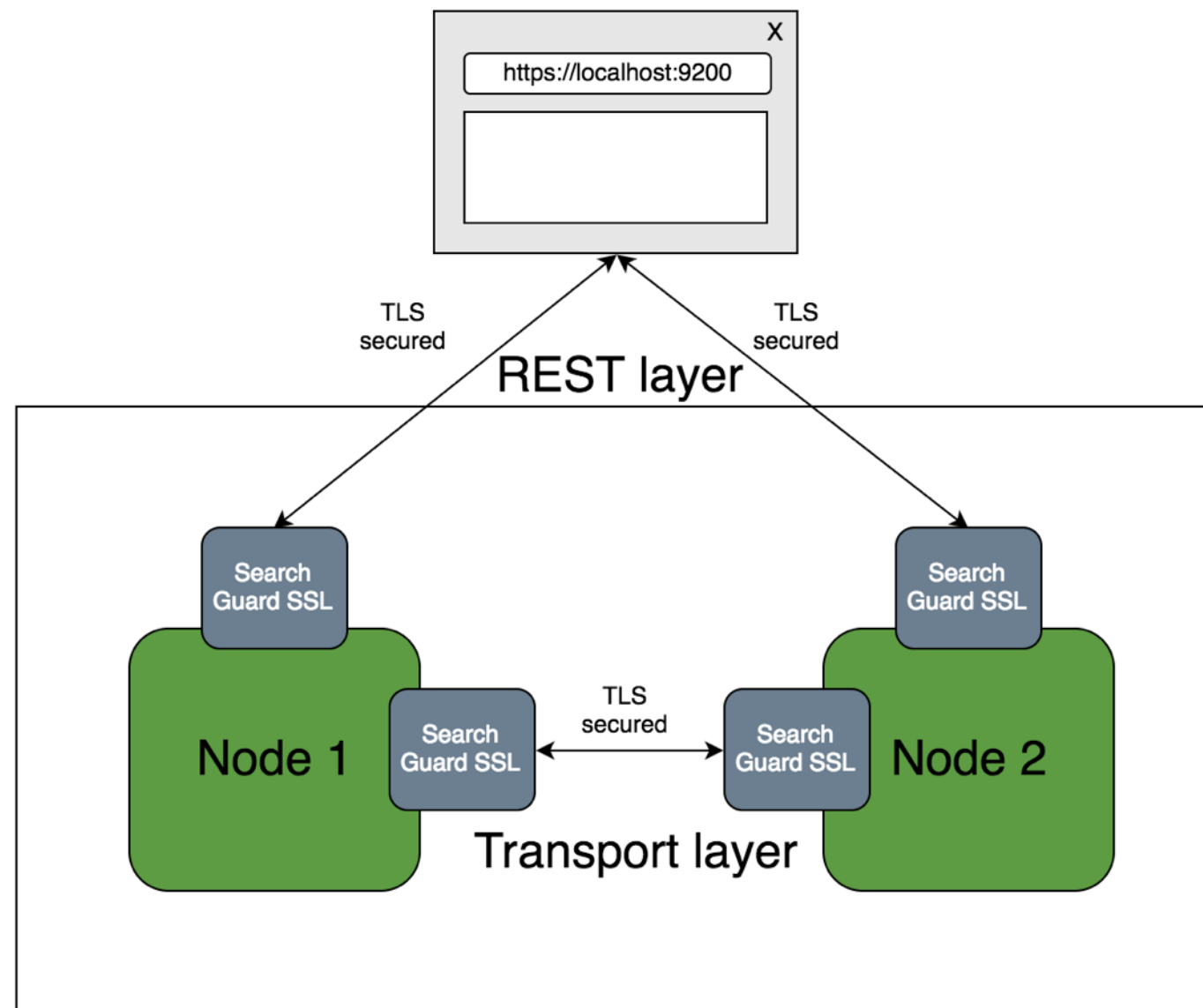
SEARCH GUARD SSL

▶ Runs stand-alone

▶ Completely free and Open Source

▶ Simple authentication by client certificate possible
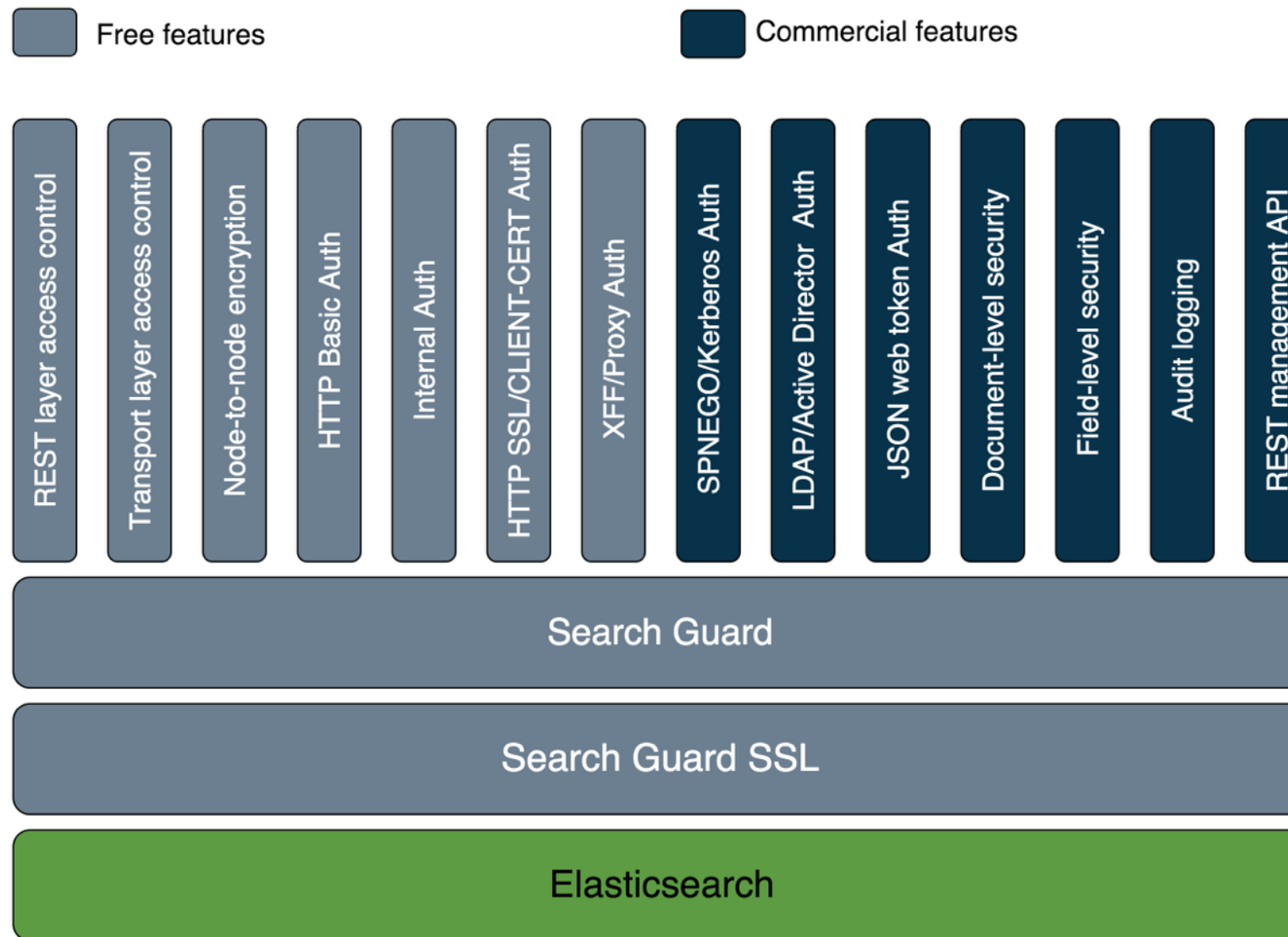
▶ Foundation for Search Guard

SEARCH GUARD

▶ Provides pluggable authentication and authorisation modules

    ▶ LDAP, Active Directory, Kerberos, JSON web token …

    ▶ Proxy and XFF support, User impersonation

▶ Fine grained access control on index and type level

    ▶ Wildcard support

    ▶ Full support for (filtered) index aliases

ARCHITECTURE

PLUGGABLE MODULES

Free features — Commercial features

| REST layer access control | Transport layer access control | Node-to-node encryption | HTTP Basic Auth | Internal Auth | HTTP SSL/CLIENT-CERT Auth | XFF/Proxy Auth | SPNEGO/Kerberos Auth | LDAP/Active Director Auth | JSON web token Auth | Document-level security | Field-level security | Audit logging | REST management API |

Search Guard

Search Guard SSL

Elasticsearch

ADVANCED FEATURES

▸ Document-level security (DLS)

  ▸ Restrict access to certain documents, based on regular queries

  ▸ Queries can include user information, e.g. username

▸ Field-level security (FLS)

  ▸ Restrict access to certain fields in documents

▸ Audit logging

  ▸ Log malicious access attempts

INTEGRATIONS

- ▶ Search Guard integrates with

  - ▶ Kibana

  - ▶ Logstash

  - ▶ Beats

- ▶ More integrations will follow

FURTHER READINGS

▶ Overview

  ▶ https://floragunn.com/searchguard/

▶ Licensing and Support

  ▶ https://floragunn.com/searchguard/searchguard-license-support/

▶ Documentation

  ▶ https://github.com/floragunncom/search-guard-docs

LEGAL

floragunn GmbH
Tempelhofer Ufer 16
D-10963 Berlin, Germany
Managing Director: Claudia Kressin
Registergericht: Amtsgericht Charlottenburg
Registernummer: HRB 147010 B
E-Mail: info@floragunn.com

Search Guard is a trademark of floragunn GmbH, registered in the U.S. and in other countries.

Elasticsearch, Kibana, Logstash, and Beats are trademarks of Elasticsearch BV, registered in the U.S. and in other countries. floragunn GmbH is not affiliated with Elasticsearch BV.

Search Guard is an independent implementation of a security access layer for Elasticsearch. It is completely independent from Elasticsearch own products.