Shield

Security for Elasticsearch

Secure and protect your data in Elasticsearch, Logstash, and Kibana.

Security is increasingly top-of-mind for organizations today. Whether you are a Fortune 500 powerhouse, or a lean startup preparing to change the world, the ability to protect data from unauthorized access, secure network communications, share hardware and management overhead through multitenancy, and stay ahead of complex regulatory and reputational risks is crucial.

Shield makes it easy to add enterprise-grade security to Elasticsearch, Logstash, and Kibana. Designed to address the growing security needs of global enterprises using Elastic today, Shield provides peace of mind when it comes to protecting your data in Elasticsearch.

Shield protects Elasticsearch with:

Role-Based Access Control
Set index, alias, and cluster-level permissions (e.g., read, write, delete, update) for each user of your Elasticsearch cluster. For example, allow the marketing department to freely search and analyze social media data with read-only permissions, while preventing all access to sensitive financial data.

Field- and Document-Level Security
Get granular with your role-based access control by restricting access to individual fields in Elasticsearch and preventing users from accessing sensitive documents with true document-level security.

LDAP-Based Authentication System Support
Shield integrates with LDAP and Active Directory, so your users don't need to remember yet another password. We also provide a native authentication system for those who prefer to manage all access within Elasticsearch.

Encrypted Communications
Node-to-node encryption protects your data from intruders. With certificate-based SSL/TLS encryption and secure client communications with HTTPS, Shield keeps data traveling over the wire protected.

Audit Logging
Ensure compliance and keep a pulse on security-related activity happening in your Elasticsearch deployment; record login failures and attempts to access unauthorized information.

IP Filtering
Easily configure Elasticsearch to accept connections only from approved IP addresses. Filter connections at the network level, without the complexity of configuring iptables or other OS-level firewalls.

Experts agree that tightly-coupled, multilevel protection is significantly more secure than simply securing the perimeter of your network or application. That's why we engineered Shield to integrate into Elasticsearch at a very low level — intercepting and securing each individual API call while protecting network traffic. Shield also provides integration with LDAP and Active Directory, so you can leverage your existing infrastructure.

Shield is designed as a commercial plugin for Elasticsearch and uses only public APIs for the integration. This means that you can easily add Shield to immediately protect any Elasticsearch cluster. Of course, Logstash, Kibana, Marvel, Elasticsearch for Apache Hadoop, and all of our language clients also support Shield.

And, as always, Elasticsearch, Logstash, and Kibana remain the open source products you know and love: free to download and make data exploration easy and accessible to anyone.

We're redefining what's possible with Elasticsearch.

Shield makes it easier than ever to create secure applications that take advantage of the advanced search and discovery capabilities of Elasticsearch.

Run Elasticsearch in the cloud with confidence:
Protect and encrypt all Elasticsearch traffic, to prevent snooping or tampering.

Efficiently manage multitenant Elasticsearch clusters:
Ensure complete separation between multiple tenants of a single Elasticsearch cluster with role-based access control.

Simplify your architecture:
Shield provides multilevel security, with IP filtering, authentication, and role-based access control, so you can manage and protect Elasticsearch without complex proxies or application-level changes.

Simplify user management and authentication:
Use existing authentication systems with Active Directory and LDAP support.

Meet and exceed security regulations:
With encrypted communications and detailed auditing, Shield makes it easy to fulfill complex regulations.

Separate cluster management from data management:
Allow the operations team to manage and monitor the cluster, without granting access to application data.

Shield 2.0+ is compatible with: Elasticsearch 2.0+, Marvel 2.0+, Watcher 2.0+, Kibana 4.2+, Logstash 2.0+
Shield 1.x is compatible with: Elasticsearch 1.4 +, Marvel 1.3 +, Logstash 1.5 +, Kibana 3.1.1 - 4.1.x

Shield is included with our Development, Gold, and Platinum subscriptions. With a simple installation, you can get started in minutes.

watcher download
elastic.co/products/watcher

contact
sales@elastic.co