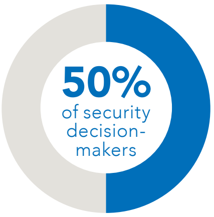
OPTIV

# Elasticsearch Maturity Service

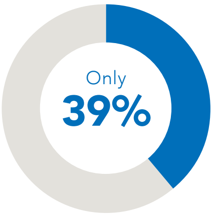
PARTNER SERVICE BRIEF elastic

## Mature and enhance Elasticsearch continually to keep up with the latest threats and opportunities.

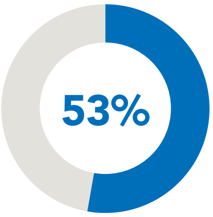
For security pros, it can sometimes feel like the only thing growing faster than the number of cyber threats is the complexity of tools to manage them. A state-of-the-art platform at purchase must continually be refreshed to stay effective.



say they don't use all the features in their security technologies.



say they're getting full value from their investments.



admit they don't know how well the tools they've deployed are working.

**Organizations must continuously mature their security environment if they want to stay ahead of hackers, who are as innovative as they are persistent.** The best way to keep pace? A strategic shift towards programmatic, iterative improvement.

**Source:** Ponemon Survey for AttackIQ, July 2019

### Optiv Elasticsearch maturity services sessions can include:

| SIEM Services | Enhancing and Scaling | Troubleshooting | Optimizing |
|---|---|---|---|
| • Use case creation and tuning<br>• Data source ingestion<br>• Custom parsing and dashboards | • Upgrade to latest version of Elasticsearch<br>• Cluster management and growth<br>• Onboard new features | • Resolve time-consuming problems<br>• Implement monitoring and system health checks<br>• Automate failure notifications | • Configure Elasticsearch to meet evolving requirements<br>• Innovation and Proof of Concept support |

Our maturity services extend well beyond basic implementation and optimization. We help you establish a proactive security mindset, reducing risk and getting you the most out of your Elasticsearch platform.

Regular tuning delivers you from the chaos of reaction mode and allows you to prioritize applying critical adjustments and best practices.

## How We Do It

Our Elasticsearch maturity program builds around a series of tailored weekly or bi-weekly fixed-fee sessions that begin with an extensive technology health check and use-case workshop or architectural review.

A regular cadence of optimization services rigorously assesses overall platform health and adjusts your current technology mix. This engagement matures your security footing, maximizes ROI and fortifies you against the environment's inevitable evolution.

## Why Clients Choose Optiv

Each of our engagements are customized to the client's distinct technical, business and cultural dynamics. Our consultants are seasoned and tech-agnostic, informing a deep, objective view of your challenges.

## Additional Technology Services

### Migration and Implementation

Configure baseline capabilities or get help migrating to a new security solution

### Authorized Support

Dedicated, 24/7/365 support from certified engineers with multiproduct expertise and industry best-practice savvy

### Health Check and Optimization

Ensure continued security technology effectiveness through review and remediation of identified issues so your security infrastructure is configured for optimal performance and protection

### Technology Management

Offload primary management responsibility for security devices or applications and ensure proactive, efficient upgrades and fault monitoring

## Case Study

A leading global retailer with over 12,000 employees

### Desired Outcomes

The client asked Optiv to review the health and maturity of its Elasticsearch platform, including hardware and software configurations, then upgrade to the latest version, all with the goal of improving overall data visibility and SIEM platform effectiveness.

### Solution

After a platform review workshop and health assessment, Optiv began frequent optimization and fine-tuning sessions to prepare, implement and assure quality throughout the upgrade. This included sessions to review and enhance data flows, parsing and index lifecycle management, as well as use case recommendations, implementations, and integrations of related tools into the platform.

### Client Benefits

Consistent methodology driven by best practices helps clients continually identify and document issues, as well as prioritize improvements that align with their evolving security, visibility and search requirements.

OPTIV

**Optiv Global Headquarters**
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com

**Secure greatness®**

Optiv is the cyber advisory and solutions leader, delivering strategic and technical expertise to nearly 6,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential. For more information, visit www.optiv.com.