

# elastic

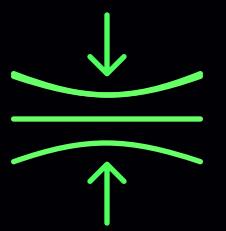


Zero Trust

# Elastic: elasticidad y visibilidad para operaciones críticas

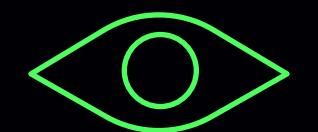
Elastic aporta la elasticidad operativa necesaria para escalar observabilidad y análisis en entornos tecnológicos complejos y dinámicos. Su plataforma unificada permite centralizar y analizar datos en tiempo real, brindando visibilidad continua, trazabilidad y capacidades avanzadas de detección.

## Elasticidad operativa



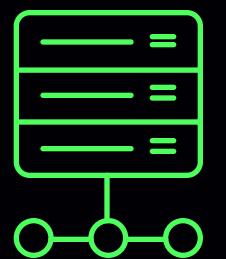
- 

## Visibilidad continua



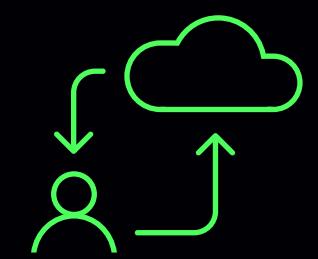
- 

## Centralización de datos



- 

## Análisis y correlación en tiempo real



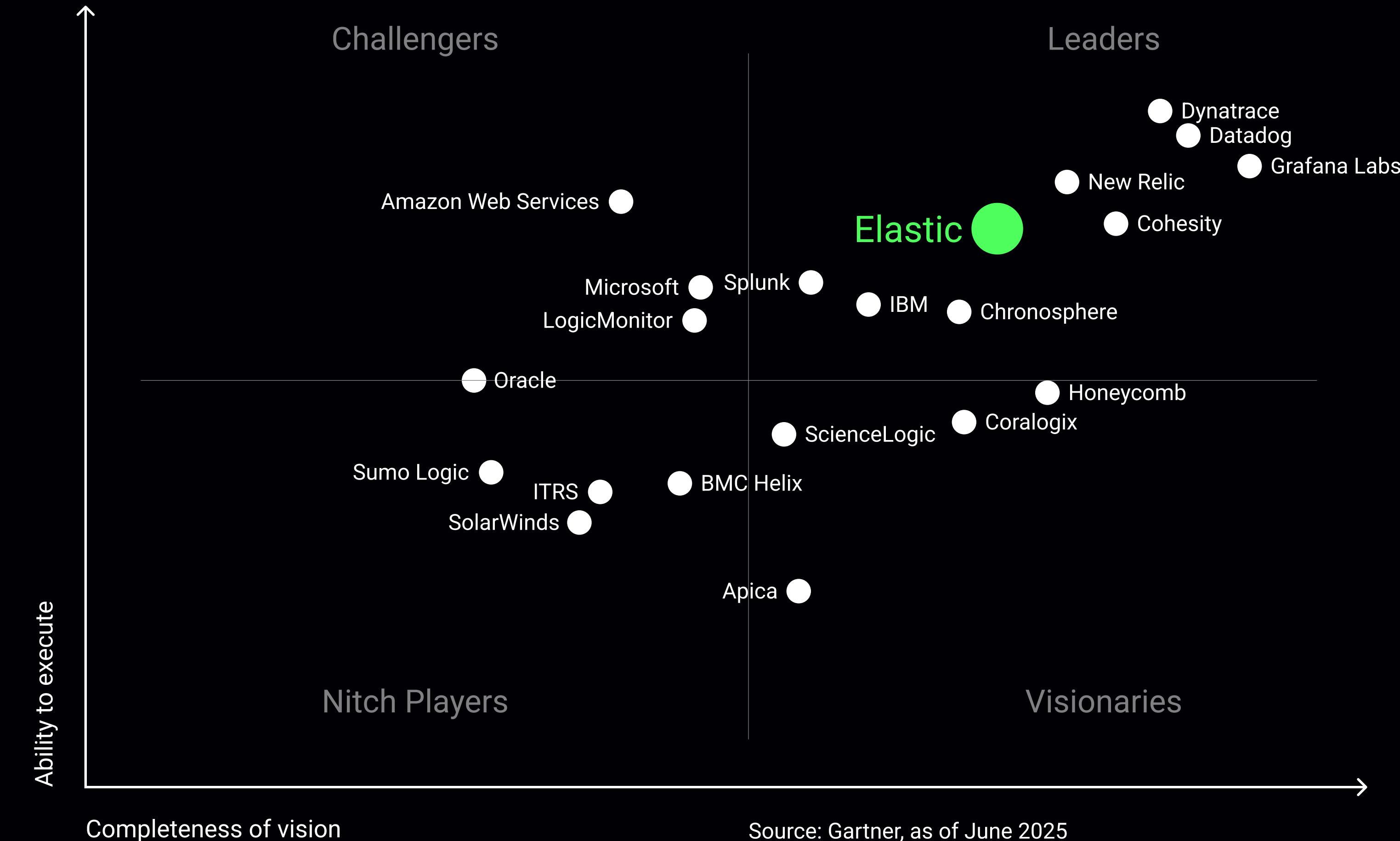
- 

## Trazabilidad completa



02 About Elastic  
03 Gartner  
04 Pilares  
07 ¡Gracias!

Elastic es reconocido por Gartner como Leader en Observability y Visionary en SIEM (2025).



# Pilares

[A]	Elastic SIEM (Elastic Security)	[F]	Elastic Security for Endpoint
[B]	Elastic Observability (Logs, Metrics, Traces)	[G]	Monitoreo Cloud (AWS / Azure / GCP Integrations)
[C]	Elastic APM	[H]	Machine Learning Jobs (Anomaly Detection)
[D]	Centralización de Logs	[I]	Elastic Enterprise Search
[E]	Elastic Agent + Beats	[J]	Dashboards Ejecutivos / Compliance Packs



## Elastic SIEM (Elastic Security)

---

SIEM unificado con correlación, detección de amenazas, reglas, machine learning y respuesta integrada.

## Elastic Observability (Logs, Metrics, Traces)

---

Plataforma completa de observabilidad para infraestructura, aplicaciones y servicios críticos.

## Elastic APM

---

Monitoreo de performance de aplicaciones, trazas, latencias, errores y dependencias en tiempo real.

## Centralización de Logs

---

Unificación de logs corporativos desde servidores, firewalls, contenedores, apps y cloud en un único stack.

## Elastic Agent + Beats

---

Ingesta y recolección masiva de eventos, telemetría, métricas y datos de endpoints/servers.



## Elastic Security for Endpoint (EDR)

Detección y respuesta en endpoints integrada al SIEM de Elastic.

## Elastic Enterprise Search

Búsqueda empresarial, indexación avanzada y motor de búsqueda interno/corporativo.

## Monitoreo Cloud (AWS / Azure / GCP Integrations)

Observabilidad y seguridad sobre workloads cloud, APIs, redes y servicios administrados.

## Dashboards Ejecutivos / Compliance Packs

Packs de visualización para auditorías, cumplimiento normativo y reporting ejecutivo.

## Machine Learning Jobs (Anomaly Detection)

Modelos automáticos para detectar anomalías, patrones inusuales y riesgos en datos operativos o de seguridad.



# ¡Gracias!

