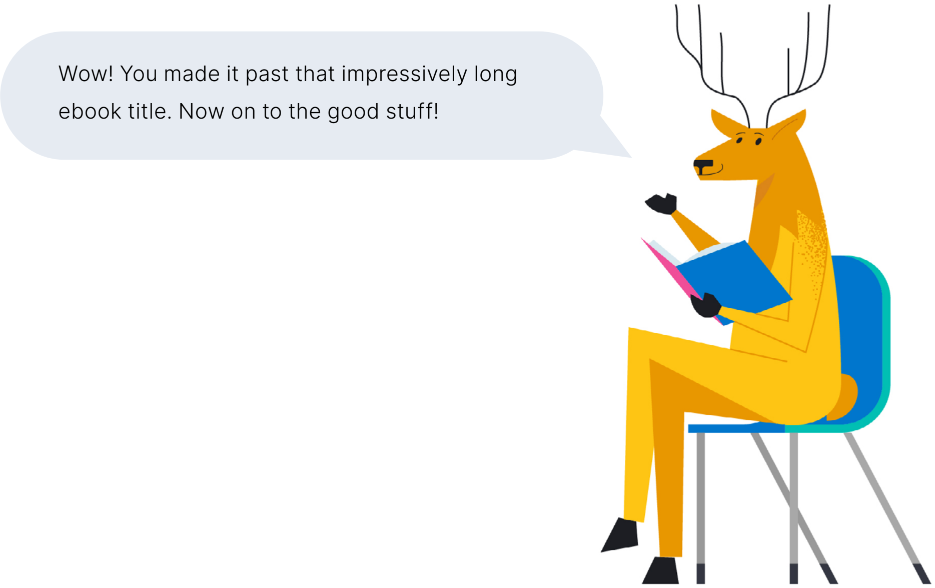
elastic

Real-world problems require real-time data:

A strategic guide to putting your data to work in public sector

How public sector IT leaders can improve digital customer experiences, increase operational resilience, and reduce cyber risk by putting existing, untapped data to work in real time

Table of contents


Wow! You made it past that impressively long ebook title. Now on to the good stuff!

Introduction

As a consumer and an employee, you expect nothing short of seamless, secure experiences across all of the applications, websites, emails, texts, and video calls that you interact with every day. As an IT leader, you're expected to keep all of these underlying systems running and secure to make your stakeholders happy, keep your employees empowered, and meet your mission goals.

And that's all coupled with unfavorable macroeconomic conditions that add pressure to find cost savings without compromising your IT performance or your larger missions. That's no easy task.

With the ongoing need to increase visibility into the performance of critical applications and infrastructure, dial-up cybersecurity, and improve the ability to surface relevant information, what if we told you there's an opportunity to condense your tech stack and save along the way?

Organizations that use real-time data for the right purpose are[1]:

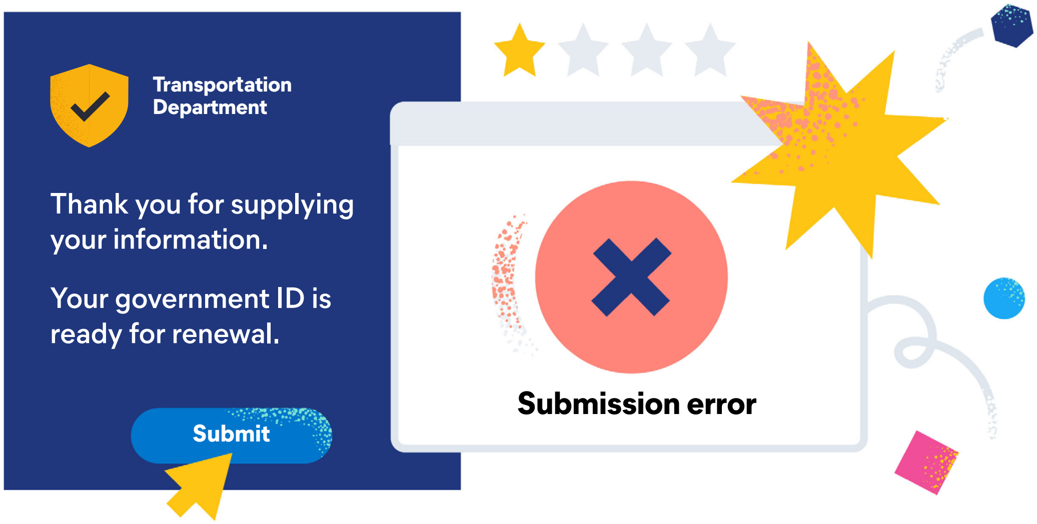
- 8x more likely to grow revenue by 20% or more
- 1.4x more likely to uncover new revenue streams
- 1.6x more likely to create data-driven experiences
- 1.8x more likely to commercialize their data

Section 1:

Your business problems are data problems

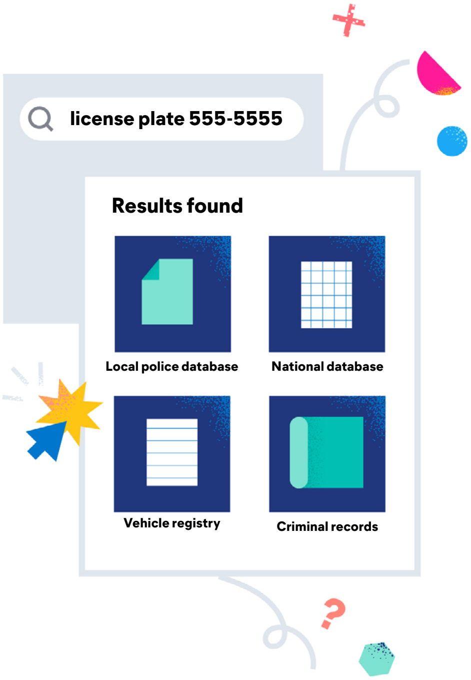
As an IT leader, you are expected **to optimize enterprise applications and infrastructure for availability and performance.** The average application, comprising of 50 to 100 services with multiple deployments, can generate more than 300 GB of data per hour during[1] an incident or outage. In the public sector, this data is often mission-critical. Unplanned downtime and system outages can mean major disruptions to transportation systems, military operations, and healthcare services – and can easily amount to millions of dollars lost.[2]

This is a data problem.


Transportation Department
Thank you for supplying your information.
Your government ID is ready for renewal.
Submit
Submission error

[1] AIOps: Unleashing the hidden insights in unstructured IT data for better IT operations management, 2021. IBM. https://community.ibm.com/
[2] What's new in the 2022 cost of a data breach report, 2022. IBM. https://securityintelligence.com/

As an IT leader, you're also expected to **prevent cyber threats and detect and resolve incidents quickly when they do occur.** The average cost of a public sector data breach is USD $2.07 million, which is no small amount, especially in a challenging economic climate. You and your team are always sifting through the exponential avalanches of security data, worried about the next threat and the impact it could have on your mission and the disruption it would have on your organization's day-to-day operations. This too is a data problem.



IT leaders are expected to **connect the right people and teams with the right information, at the right time** regardless of where the information is, or what format the data is in. For example, a law enforcement agency might be searching for information on an ongoing investigation, but data is categorized differently in disparate databases, and manually matching the data wastes critical hours or days in a time-sensitive operation.

This, again, is a data problem.

All of these challenges are fundamentally connected to data. In fact, the average enterprise stores more than 71PB of structured and unstructured data on-premises alone, not even including cloud.[3] A mountain of data could be hiding key insights to mission operations, indicators of compromise, and everything in between. This data shouldn't just be stored, but rather needs to be put to work.

Unfortunately, only 32% of data within organizations is actively being put to work[4] today, which leaves an undesirable amount of data taking up space and costing money to store without adding any value. Using this untapped data will enable you to facilitate better digital experiences, keep your systems up and running, and help your critical systems and information stay protected.

> **To address these data challenges, organizations need a way to derive value from data continuously, in real time.**

So, how do you do that?

With **a unified and flexible data analytics platform powered by search technology** that enables users to find, share, protect, and visualize data across multiple data sources and environments in real time.

Search-powered technology consists of tools that enable the searching of data across multiple sources like websites, applications, databases, hybrid cloud environments, and other enterprise-type sources. It delivers data and insights to stakeholders in the moment they're needed, regardless of where the data is located.

[3] Meeting the new unstructured storage requirements for digitally transforming enterprises, 2022. IDC. https://www.delltechnologies.com/
[4] Rethink data put more of your business data to work—from edge to cloud, 2020. Seagate. https://www.seagate.com/

According to a survey conducted by Forrester Consulting and commissioned by Elastic, more than 4 in 5 data leaders agree that search-powered technology helps[5] them:

83%

Reduce costs for their business, when deployed as an integrated platform.

81%

Give time back to their teams to do meaningful work.

83%

Improve their customer and employee experiences.

84%

Work faster with an increase in speed and productivity of their organizations.

83%

Deliver important insights that speed up decision-making.

84%

Implement successful digital transformations.

How do you put this search-powered technology to work? **With search-powered solutions.** Read on to find out everything you need to know in order to analyze your data, extract insights, and continuously derive value in real time. But first, a bit of insight into the challenges organizations are facing.

[5] Search-powered technologies: A mission-critical enabler for the digital future of business, 2022. Forrester Consulting. https://www.elastic.co/

Section 2:

Data challenges and digital environments continue to accelerate

Public sector organizations of all sizes are experiencing exponential growth of unstructured data, and digital business complexities are soaring to new heights. You're most likely dealing with at least one of the challenges below.

Stakeholder expectations are higher than ever. According to McKinsey, public sector is ranked lowest of 10 industries for customer satisfaction. Public sector organizations have an opportunity to better serve their stakeholders through fast, efficient, and secure digital service delivery. And when it comes to employees, they need their technology stack to work for them and integrate disparate systems across the organization in order to feel empowered to do their best work. Many organizations also need to share data and insights with other agencies, but lack the ability to do so in a quick and seamless manner. Plus, IT teams must monitor all systems to ensure problems are diagnosed and fixed quickly, which leads to a huge amount of data that must be monitored.

Digital transformation initiatives continue to influence government IT strategies as organizations move their processes to more digitized environments and workflows. With the goal of aligning growing data in real time across environments and platforms, organizations have a lot more data to manage, process, and extract insight from to transform their business and meet employee and stakeholder expectations.

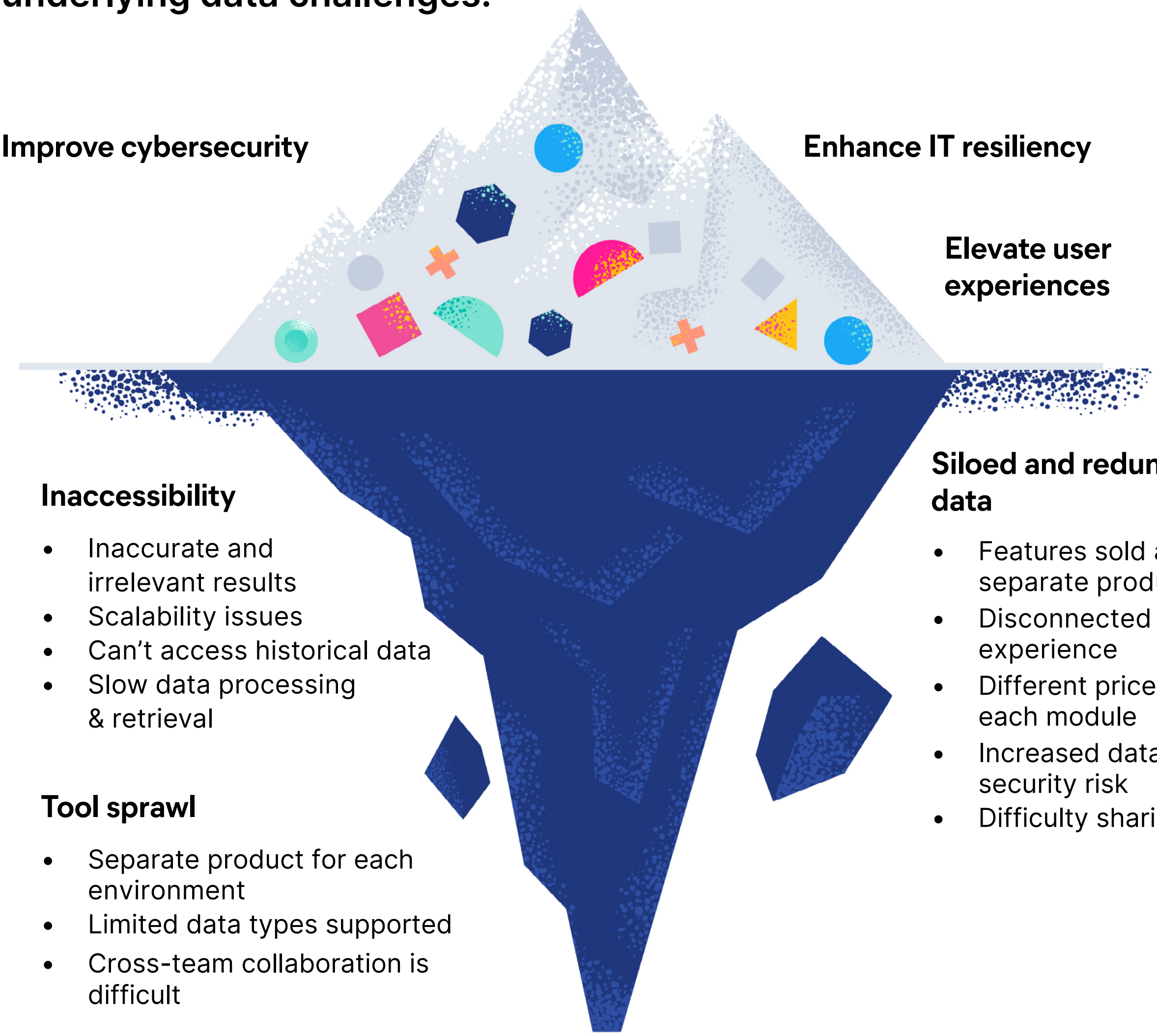
Cloud migration is the next step (or current step) for many public sector organizations on their digital transformation journeys. The cloud holds the key to enabling mission agility, reducing operational overhead, and more. But, moving to the cloud means more environments, systems, and complexity, not to mention more attack surfaces that need to be monitored.

With these complexities, come challenges:

1. **The need to elevate stakeholder and employee experiences**
2. **The need to improve operational resilience to keep critical systems up and running**
3. **The need to reduce security risks**

The ability to derive value from all of your data is more important than ever due to these challenges. Unfortunately, most public sector organizations are faced with a mountain (or an iceberg in this case) of underlying data problems that continuously compound until you're just overwhelmed with data that doesn't work for you.

Unfortunately, most organizations are impeded by myriad underlying data challenges.



Improve cybersecurity

Enhance IT resiliency

Elevate user experiences

Inaccessibility

- Inaccurate and irrelevant results
- Scalability issues
- Can't access historical data
- Slow data processing & retrieval

Tool sprawl

- Separate product for each environment
- Limited data types supported
- Cross-team collaboration is difficult

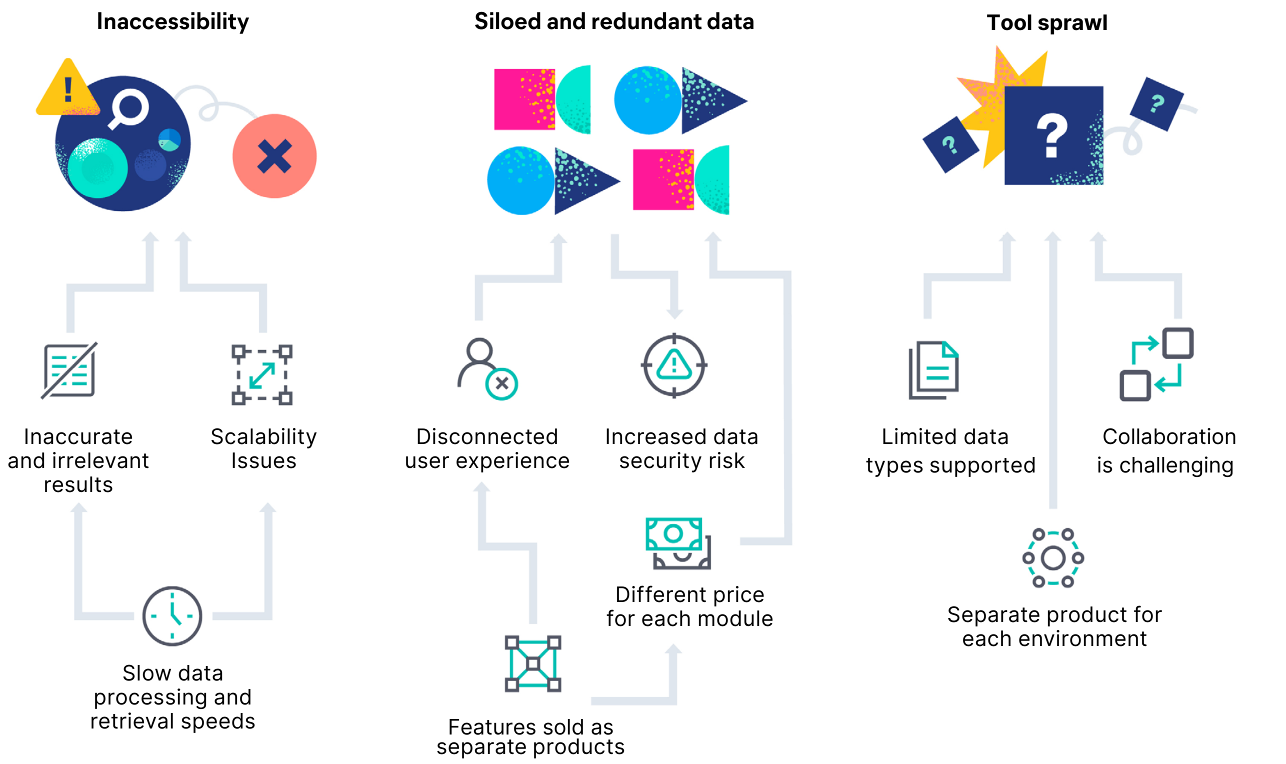
Siloed and redundant data

- Features sold as separate products
- Disconnected user experience
- Different price for each module
- Increased data security risk
- Difficulty sharing data

These challenges are further exacerbated by:

1. **Slow data processing and retrieval speeds.** These slow speeds can lead to inaccurate and irrelevant results and scalability issues. This impacts the ability to iterate through your data. And when you can't iterate, your data is useless.
2. **Product silos that lead to data silos.** When you have all of these different products that each perform a few tasks, you're getting fractured user experiences for your data teams, increased costs with different pricing for each module, and ultimately, siloed and redundant data and increased security risk. You then have a sizeable data tech stack that doesn't allow for your data to be used across multiple environments.

Demands escalated by ongoing data challenges


Inaccessibility
Siloed and redundant data
Tool sprawl
?
?
?
Inaccurate and irrelevant results
Scalability Issues
Slow data processing and retrieval speeds
Disconnected user experience
Increased data security risk
Different price for each module
Features sold as separate products
Limited data types supported
Collaboration is challenging
Separate product for each environment

Section 3:

Why it’s necessary to combat these challenges

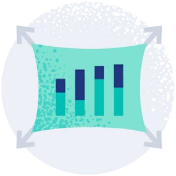
We already addressed how data volume will continue to exponentially increase. And with that increase in data, we’ll see an increase in the complexity of security threats, requiring more monitoring. As the use of SaaS solutions increases, so will the number of cloud providers you use, and so will the number of partners using those solutions and providers. With the increased economic uncertainty, public sector organizations will find it more important than ever to have a tech stack that consolidates solutions and saves money.

Organizations that use real-time data for the right purpose[6] are:

8x
more likely to grow revenue by 20% or more

1.4x
more likely to uncover new revenue streams

1.6x
more likely to create data-driven experiences



1.8x
more likely to commercialize their data

[6] The state of the insights-driven business, 2022. Forrester. https://www.forrester.com/

Section 4:

How search-powered solutions help you get ahead of your data and make use of it in real time

You probably know where we're going with this... the way for you to make use of all this data is through search-powered solutions delivered on a single platform with a flexible architecture.

When it comes to your data, search-powered solutions help you:

1. **Capture all of your data**
   The first step in making use of all this data is bringing it all together. From the cloud to on-prem and machine-generated data to consumer-generated data, all of your data needs to be brought together — very quickly and at scale — into a system where you can derive value from it.

   Every error message, security event, text log line, and time stamp needs to be captured from all of your data sources. Terabytes of this type of data are being created every day. Sure, one single log could mean nothing, but it could be the indicator of the latest ransomware attack or an indicator that your system is about to reach max capacity.

   > **Before any mission critical event happened in the past, there were data points that signaled there would be a crash or a security breach.**

   You need a line of sight into everything happening in your infrastructure.

2. **Make your data searchable and analyzable**
   Once you've captured all of that data, you now need to make it searchable and analyzable in real time with machine learning. Don't be content with just storing your data. You need to put it to work for you. **Make your data help with the rent**.

   Think about your unstructured data, like a log file. You're not sure which elements of that log file will be of value to you. By asking freeform questions through search and iterating your search terms, you can quickly get the actual information you're looking for.

   Humans aren't the only ones that can make use of your searchable and analyzable data. Machines can as well. When you have a million log lines to go through, you need machine learning running analysis across the data to find the insights you want.

3. **Make your data explorable**
   Make your data visual, explorable, and easy to interpret with curated workflows to help you make sense of your data and take action. You may currently have disconnected workflows and solutions that are drawing from over 400 data sources[7] and using over 300 applications[8] to manage it all. This impacts the time it takes to gain insights from all that data and ultimately, the time it takes to act on it.

   Imagine one of your security analysts has siloed data sources that are only accessible through different tools. They would have to go through each tool and tie the context together manually. That wastes their time and yours — leaving you vulnerable to security risks.

[7] Matillion and IDG survey: Data growth is real, and 3 other key findings, 2022. Matillion. https://www.matillion.com/
[8] Less than half of company SAAS applications are regularly used by employees, 2021. Business Wire. https://www.businesswire.com/

By exploring the data seamlessly within one unified platform, you can iteratively refine the information and apply relevance to the data insights in real time. This enables you to derive value from all of your data continuously in real time to address broader challenges, opportunities, and priorities, like improving customer experience, increasing resiliency, and reducing security risks.

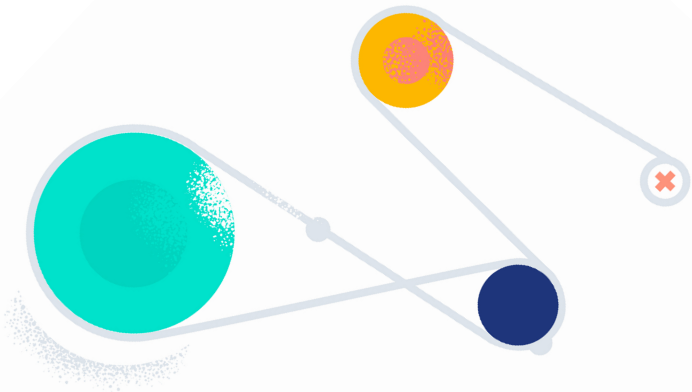
Excitingly, public sector organizations are already deploying search-powered solutions that help them capture all of their data, search and analyze it, and visualize it and are finding success.

Oak Ridge National Laboratory uses search-powered solutions to reduce the costs of their security tool, reduce search time from minutes to seconds, and aggregate and centralize its logs.

CISA uses search-powered solutions to drive its CDM dashboard, which US federal civilian agencies use to detect and respond to cyber threats.

The State of Arizona Enterprise Security team uses search-powered solutions to increase the automation and reporting capabilities of its risk assessment and threat intelligence.

The UK Driver & Vehicle Licensing Agency uses search-powered solutions to manage large volumes of Kubernetes data, reduce time spent on infrastructure management, and provide more time to develop new apps.



Search-powered solutions give your organization:

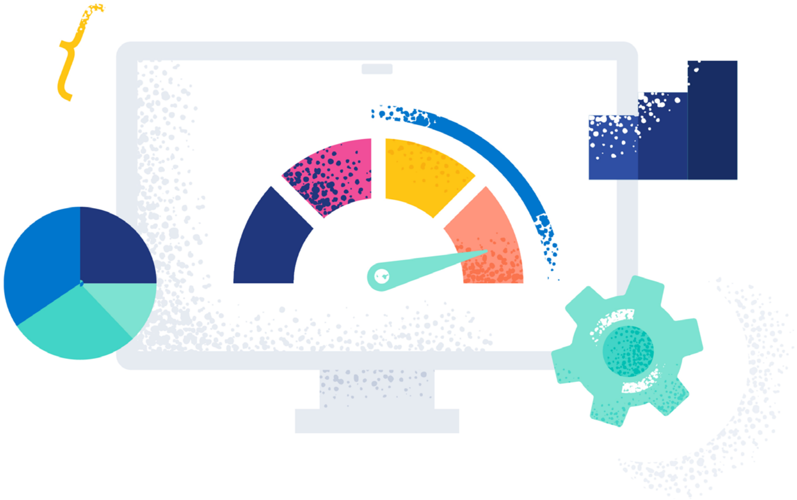
Speed: Just like Google, type your search term and press enter to get fast results across all of your data sources. Not seeing what you're looking for? Just try another search and get those results just as fast.

Scalability: As your data grows (and it will grow!), search-powered solutions allow you to seamlessly meet your needs at any scale, with no hardware-driven limitations.

Relevance: The context of a search will be different between a security analyst conducting a search versus a developer, or a student browsing a course catalog at a university. Context matters. Search-powered solutions provide relevant, in-context results.

Iterative exploration: All of these aspects combined gives you the opportunity to iteratively explore and analyze all of your data. You are able to slice and dice in different ways by searching different terms.

How your solution goes about putting your data to work in real time matters. Also, how that solution is delivered matters. Your search-powered solution needs to be simple, flexible, and work across all of your environments without you needing to move your data from where it is.



Section 5:

What to look for in a search-powered solution

Not all search-powered solutions are built the same way. When comparing solutions, we've compiled the many features you should consider.

Unified platform

A search-powered data solution that is delivered on one platform provides simplicity through an end-to-end experience with your data lifecycle. From ingest to insights, you're using one data store that uses lifecycle management, search capabilities, access rights, and provides machine learning. And all of this needs to encompass data from the back end to the front end of your systems. With a single, unified platform, you get:

- ☑ **A unified user experience** across all of your solutions and data stores. With one, single-user experience, IT teams don't need to relearn a new tool each time a new solution is deployed.
- ☑ **Uniform resource-based pricing** means you only pay for the resources you consume, independent of your use case. This is essential as you scale and add more users (and, of course, more data), knowing you're only paying for the additional resources you consume.
- ☑ **A single data store** reduces data redundancy by storing all of your data across different solutions. Since observability data can be identical to security data, there's no need to store that twice and waste resources. With a single data store, you decrease licensing and storage, hardware, and infrastructure costs.
- ☑ **Data correlation** allows you to bring data together that may not reside in the same place, doubling the value of your data. For example, when it comes to infrastructure monitoring, you're monitoring your systems to understand uptime and slowdowns. But this data is also useful when it comes to cybersecurity. You can monitor the same data to look for anomalies and patterns. Are these humans interacting with your application? Or bots? Bringing together all these solutions and all of your data allows you to unlock these insights that you may have missed if they weren't correlated.

Flexible architecture

A flexible architecture provides extensibility, allowing you to scale and grow seamlessly and rapidly. You can ingest everything and bring it all together, which means all of your data, images, documents, logs, metrics, geo locations, IP addresses, and everything in between is in one place. With a flexible architecture, you get:

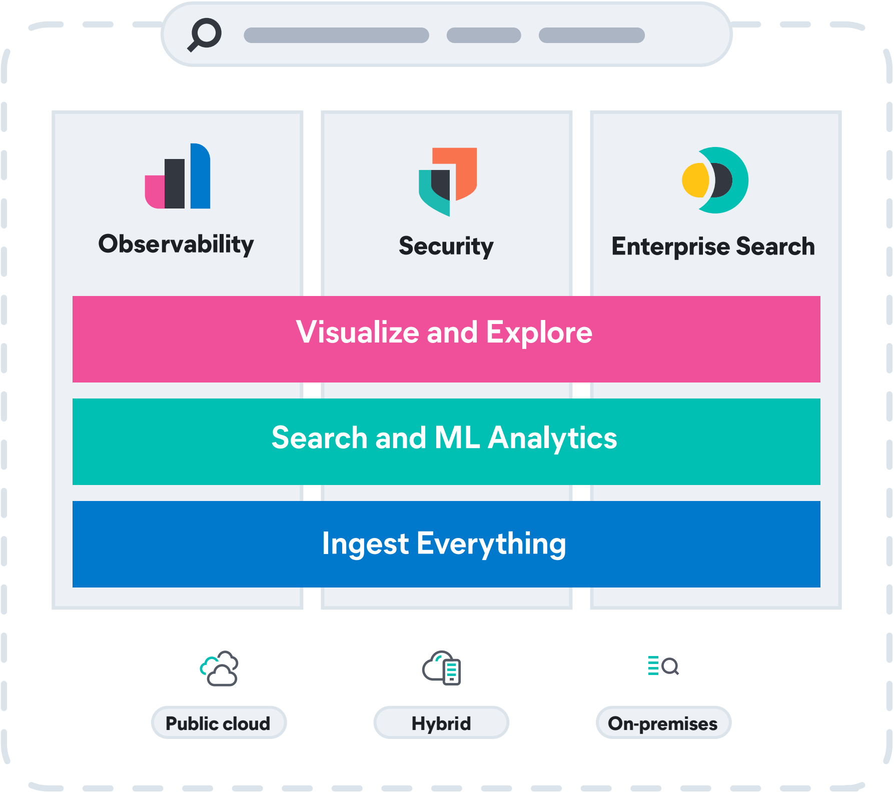
- ☑ **A multi-purpose data store.** No matter if it's your security team storing security events or your dev team storing application traces and profiling data or your business team storing product information, a flexible architecture enables you to store it all.
- ☑ **The ability to deploy anywhere.** From cloud, on-prem, hybrid, and Kubernetes, you need a solution that follows your lead, whether that's in the cloud or on the ground.
- ☑ **Integration with existing tools** so you don't have to overhaul your legacy systems (you've spent money and time on those and you shouldn't need to rip it all out to replace it). A flexible architecture will allow you to run side by side with what you already have and upgrade those legacy systems when it works best for you.
- ☑ **The ability to fill feature gaps** to fit the solution to your exact needs and extend freely with an open code base. If you do see feature gaps, and you have the resources, make sure the solution you chose allows you to take the code and customize it how you see fit. You shouldn't need to rely on the roadmap of the solution vendor.

Section 6:

Elastic to the rescue

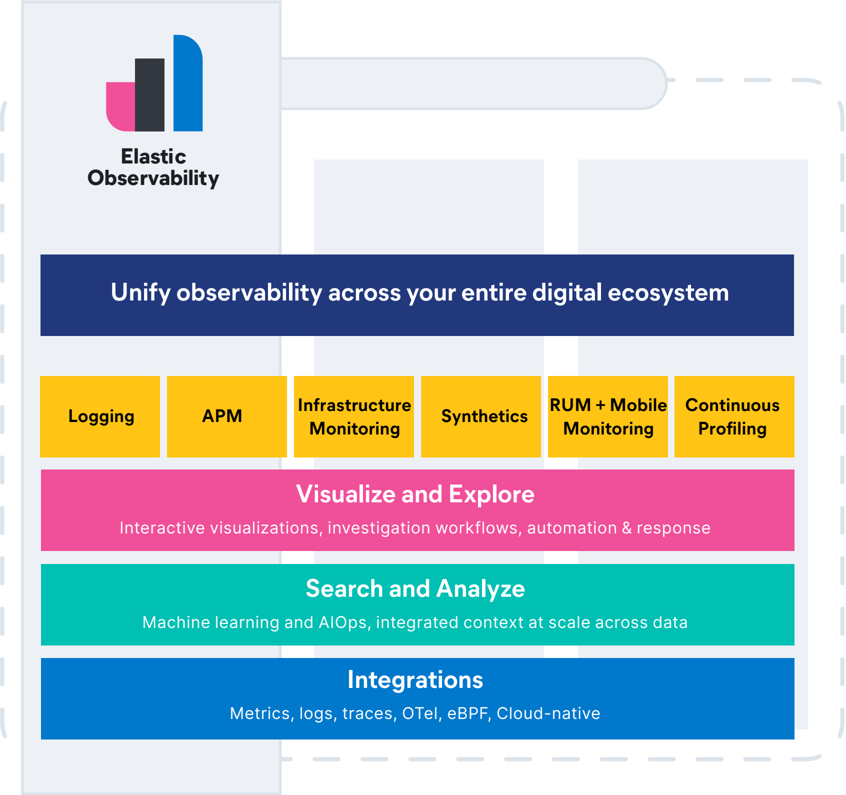
You can probably see where this is going… What solution do we recommend to meet all of your search-powered data platform needs?

Meet the Elastic Platform. It's a unified data analytics platform that solves all of these data problems and more. It includes all of the must-have features you need to unlock your company's secret sauce: data.



Elastic has three built-in search-powered solutions: **Elastic Observability**, **Elastic Security**, and **Elastic Enterprise Search**, all on our single, unified platform. You will have access to all of these solutions as an Elastic customer.

With **Elastic Observability**, quickly get to the root cause of why your systems aren't working as expected by surfacing the indicators that really matter. Rapidly figure out why your application might not be performing as well as you expect it to or why some transactions may not be completing how they're supposed to. To do that, Elastic helps you bring in all of your application infrastructure logs and then correlate them with application traces, metrics, and open telemetry information to then apply machine learning (aka AIOps).

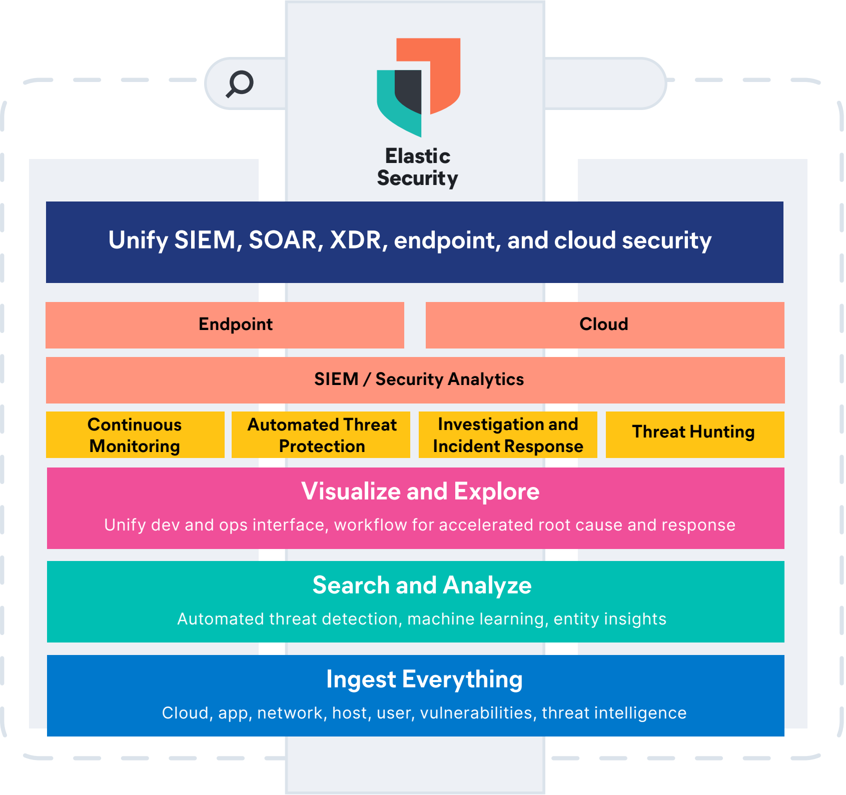

Elastic Observability
Unify observability across your entire digital ecosystem
Logging
APM
Infrastructure Monitoring
Synthetics
RUM + Mobile Monitoring
Continuous Profiling
Visualize and Explore
Interactive visualizations, investigation workflows, automation & response
Search and Analyze
Machine learning and AIOps, integrated context at scale across data
Integrations
Metrics, logs, traces, OTel, eBPF, Cloud-native

With Elastic Observability, you'll be able to:

- Custom-build workflows for site reliability engineers for accelerated root cause and response (included in our unified platform)
- Scale and efficiency to keep systems running as you grow
- Have visibility into the most complex hybrid and multi-cloud environments
- Ingest telemetry data with high cardinality and dimensionality, metrics, logs, and traces quickly and easily from applications and infrastructure hosted in a data center or on cloud providers
- Access actionable insights into your serverless, microservices and cloud-native environments to optimize use experiences

Learn more about Elastic Observability ⟶

With **Elastic Security** you can detect an indicator of compromise by pulling in that unstructured data, including network logs, application logs, and identity and access management (IAM) logs from across your organization to search and correlate it all to see if there are any patterns. You can do that quickly and apply machine learning algorithms and behavioral analyses through workflows that are suited for the SOC/ security analyst.



Elastic Security

Unify SIEM, SOAR, XDR, endpoint, and cloud security

Endpoint

Cloud

SIEM / Security Analytics

Continuous Monitoring

Automated Threat Protection

Investigation and Incident Response

Threat Hunting

Visualize and Explore

Unify dev and ops interface, workflow for accelerated root cause and response

Search and Analyze

Automated threat detection, machine learning, entity insights

Ingest Everything

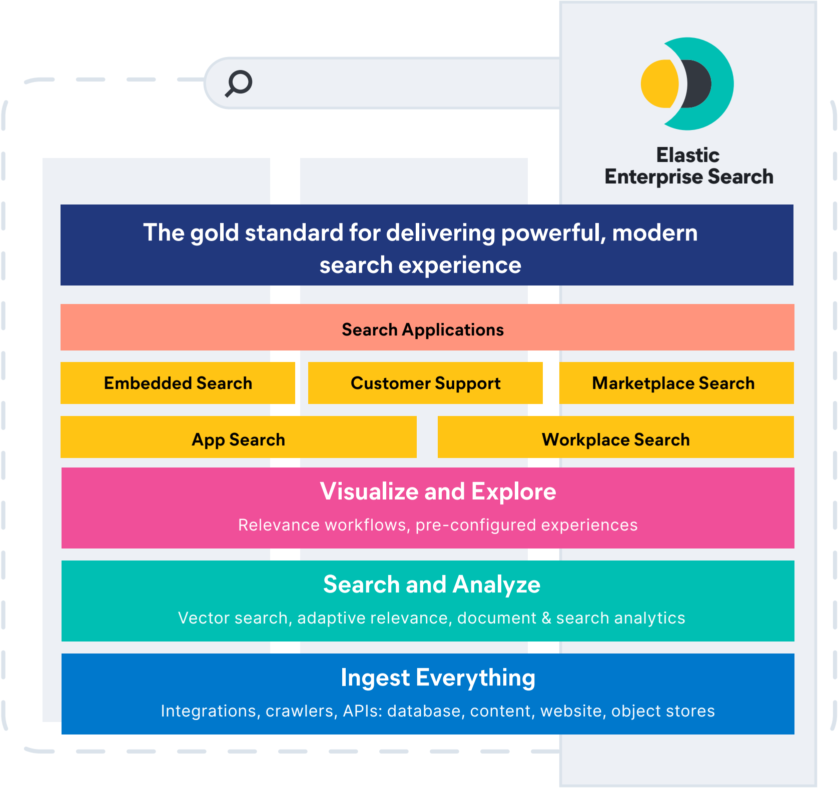
Cloud, app, network, host, user, vulnerabilities, threat intelligence

With Elastic Security, you'll be able to:

- Detect and respond to threats at speed and scale with SIEM
- Streamline SOC workflows with orchestration and automation with SOAR
- Make threat intelligence actionable with automated threat detection, machine learning, and interactive visualizations with Threat Intelligence
- Prevent, collect, detect, and respond — all with one agent with Endpoint Security
- Power SecOps across your hosts, cloud, network, and beyond with XDR
- Assess your cloud posture and protect cloud workloads with Cloud Security

Learn more about Elastic Security ⟶

With **Elastic Enterprise Search**, you can quickly deliver results that matter to you, your employees, and your mission. As one of the most sophisticated open search platforms available, you can power critical user experiences. Search provides visibility and real-time reporting for analysis across massive datasets whether your team relies on geo data, operational intelligence, or complex queries and rankings for mission-critical operations.


Elastic
Enterprise Search
The gold standard for delivering powerful, modern search experience
Search Applications
Embedded Search
Customer Support
Marketplace Search
App Search
Workplace Search
Visualize and Explore
Relevance workflows, pre-configured experiences
Search and Analyze
Vector search, adaptive relevance, document & search analytics
Ingest Everything
Integrations, crawlers, APIs: database, content, website, object stores

With Elastic Enterprise Search, you'll be able to:

- Help your employees quickly find what they need to do their jobs
- Assist students and citizens in quickly finding the services and information they need and come back again knowing their digital experience is seamless and meets their expectations
- Use machine learning to determine what search results are most relevant
- Create relevant workflows and pre-configured experiences to make the roll-out of Elastic Enterprise Search simple

Learn more about Elastic Enterprise Search ⟶

Unlock your data beneath the surface

Search-powered solutions can transform your big data problems into mission results by helping you continuously derive value from petabytes of data — in real time. And you don't have to break the (IT) bank because you only need one, flexible data analytics platform for search-powered solutions to do it: Elastic Platform. Easily deploy in your favorite public cloud, or in multiple clouds, and extend the value of Elastic with cloud-native features.

See how it works

Start a free trial

elastic

Now go off and harness the power of your data!