elastic | The Search Analytics Company

Elastic Observability in action in public sector

How organizations are using Elastic to drive operational resilience in government, education and healthcare.

Using the power of Elastic for operational resilience

The Elasticsearch platform has been a trusted tool for developers for over a decade, serving an essential role in the tech stacks of many public sector organizations. In addition to searching, analyzing, and visualizing data, customers are leveraging Elastic's two out-of-the box solutions – Elastic Security and Elastic Observability – that are built on the foundation of our search analytics platform. In this ebook, we'll share 10 examples of how public sector customers are using Elastic Observability to strengthen their organizations' operational resilience, modernize their IT, and monitor their apps and infrastructure.

The Elastic Public Sector Team

Check out more success stories from public sector:

Elasticsearch: elastic.co/public-sector/elastic-in-action
Elastic Security: elastic.co/pdf/ebook-elastic-security-in-action-in-public-sector.pdf

Table of contents

Modernizing IT for a better job-matching experience: **Swedish public employment service**

About Arbetsförmedlingen:

Arbetsförmedlingen, the Swedish Public Employment Service, provides information, analysis, and employment forecasts to create the best conditions for a well-functioning labor market in Sweden. Tasked with matching job seekers with employers, the organization must adapt to annual changes to government guidelines.

The challenge:

Arbetsförmedlingen had accumulated years of technical debt through multiple solutions from multiple vendors. “Our observability solution had long response times and was out of date. The APM [app performance monitoring] platform was expensive and complicated, and we wanted to consolidate several search tools into one solution,” said Tobias Ström, Product Owner, Operation Center.

The solution:

Arbetsförmedlingen decided to use Elastic Observability for logging and APM, hosted on ECE (Elastic Cloud Enterprise), to replace its legacy search and logging tools. A small team within the organization had been successfully using the free version of Elastic for logging, so they decided to upgrade and expand its use, while also relying on the technical expertise of the Elastic Professional Services team.

The outcomes:

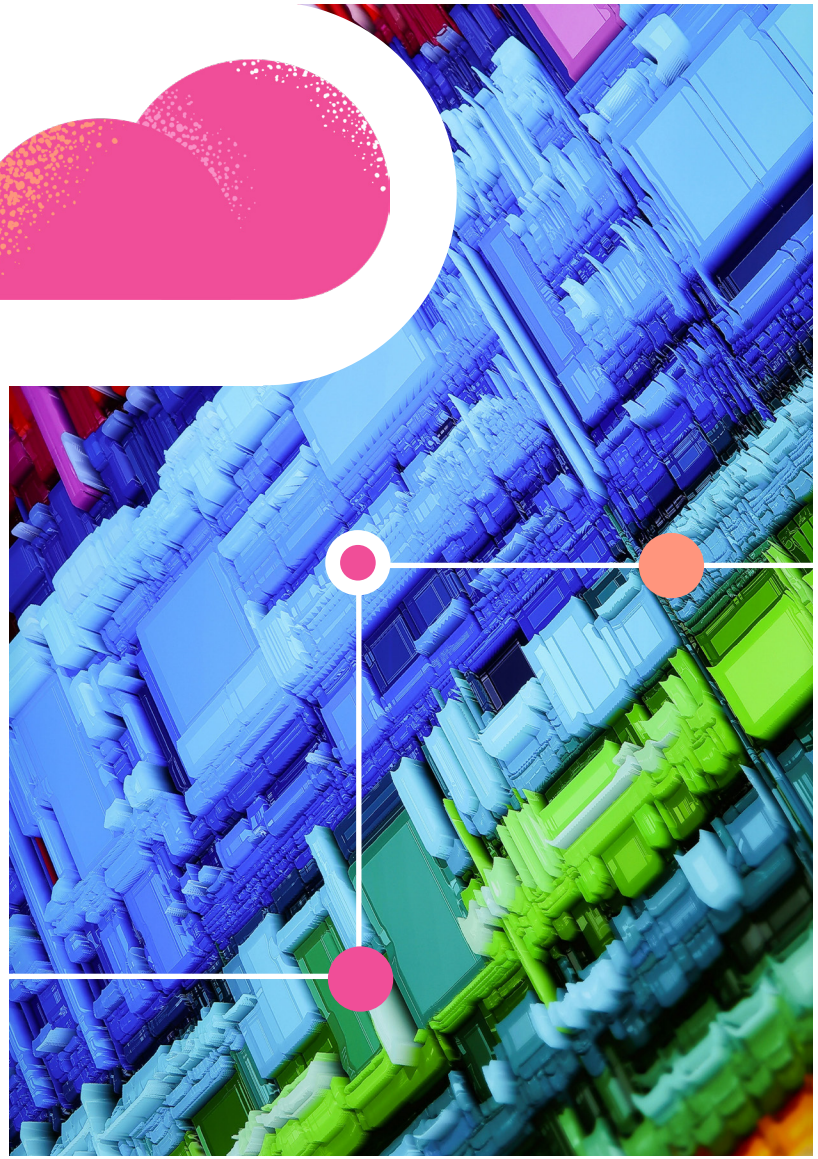
With Elastic Observability in place for logging and APM, Arbetsförmedlingen:

- Has reduced application performance monitoring (APM) license and storage costs by 75%
- Is accelerating its transition to a modern DevOps culture, by fixing errors earlier in the software development process and improving product quality
- Is now ahead of the IT benchmark for Sweden's public sector and is paving the way for other organizations that want to boost the performance of their observability, search and APM platforms

Read the full story

> Swedish and EU regulations mean that regulated or sensitive data cannot leave our internal network. With ECE [Elastic Cloud Enterprise], we get the power and scalability we need while complying with these requirements.

Stefan Jonsson
Product Owner, Arbetsförmedlingen



Reducing outages for a U.S. city government: **Mentat**

About Mentat:
Mentat is a cloud-agnostic consultancy that helps organizations simplify, automate, and orchestrate their cloud computing architecture. This includes managed migrations and deployments of web-scale architecture in private and public cloud settings. Over the years, Mentat has settled on a core set of automation and development tools for most of its engagements. Elastic Observability is a main component, as well as Elasticsearch as a storage and search engine, Kibana for analyzing and visualizing data, and Logstash for parsing logs. “Elastic is at the heart of our architecture, acting as a holding zone for data that we need to interface or transmit between different automation systems. It’s the glue that holds all of them together,” says Jonathan Doughty, founder and CEO at Mentat.

The challenge:

Mentat recently put its network and automation telemetry solutions to good use for a major U.S. city government's IT organization. Its infrastructure includes multiple data centers, tens of thousands of endpoints, and millions of users. Before the engagement with Mentat, the organization suffered data center outages about four times a day, and there was no one with the time or expertise to uncover the underlying problem.

The solution:

The U.S. city government turned to Mentat to identify the source of the problem and deploy a long-term fix to reduce outages. Elastic Observability was at the heart of this solution, which also included Kafka to act as a buffer and Ansible as the data collector and data manipulator.

The outcomes:

After implementing the solution, a network scan revealed that hundreds of devices were generating errors. "Once the client worked through all their physical devices and replaced or updated their cabling, they went from four outages per day to one outage per quarter," says Doughty. The error detection system was so successful for this client that Mentat has since deployed it extensively across its wider client organizations.

Read the full story

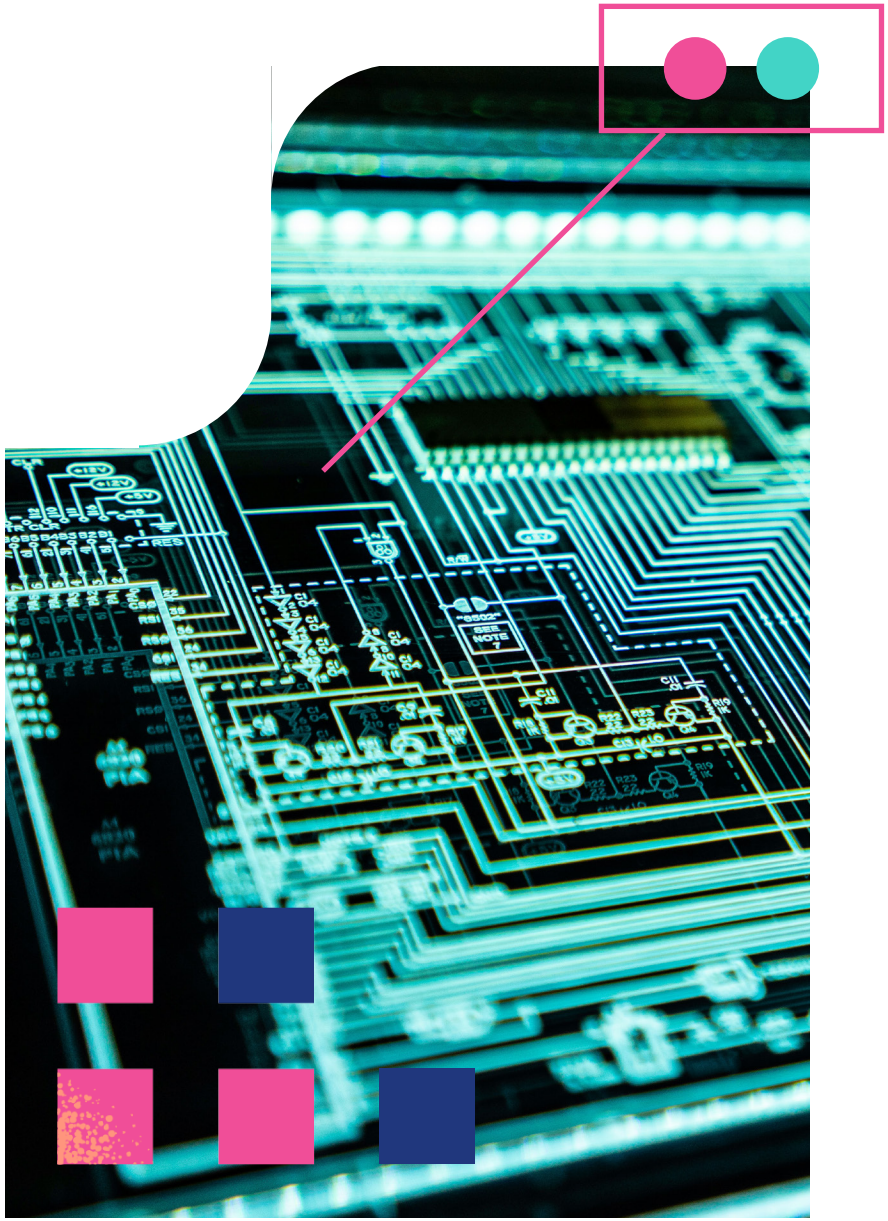
I like everything about Elastic. Its engineers are easy to work with and there's always great support. The tool itself fits our vision exactly. It is easy, simple, secure, and it scales. It is also future proof thanks to frequent new releases and enhancements that we can apply to existing Elastic deployments.

Jonathan Doughty
Founder and CEO, Mentat

Optimizing supercomputer performance: **Lawrence Livermore National Laboratory**

About Lawrence Livermore National Laboratory (LLNL):

Founded by the University of California, Berkeley in 1952, Lawrence Livermore National Laboratory, a part of the U.S. Department of Energy and the National Nuclear Security Administration, applies science and technology to ensure the safety, security, and reliability of the U.S. nuclear deterrent. These activities are supported by a high-performance computing (HPC) environment, including a new greater-than-two-exaflop supercomputer.



The challenge:

- Increase HPC availability for scientific research and automate tasks to free up security resources
- Maximize performance of supercomputer projected to be world's fastest
- Migrate from Splunk to Elastic to improve performance

- Comply with U.S. federal government regulations (such as M-21-31) that impact logging, scanning, and remediation timelines.

The solution:

LLNL decided to use Elastic Security for its SIEM, including centralized logging for cyber analytics across the HPC environment. Elastic Observability will be used for data aggregation, analysis, and evaluation of logs, metrics, and event data. The team is configuring dashboards that warn engineers of system vulnerabilities and errors.

The outcomes:

With Elastic, LLNL:

- Has simplified data ingestion with a single, unified method for adding logs, metrics, and other types of data
- Successfully migrated its logging infrastructure from Splunk to Elastic
- Spends less time manually upgrading infrastructure, and more time working on compliance, threat hunting, and other tasks that deliver clear benefits to the organization

Read the full story

We believed that Elastic was well-suited for our needs, especially when it came to feeding data into a centralized repository and then visualizing the information. Elastic's performance, responsiveness, and user interface, as well as its ability to handle large volumes of data were critical to our decision, given recent executive orders that require us to search back through up to two years' worth of data.

Ian Lee
Security Operations Team Lead, Lawrence Livermore National Laboratory

Monitoring advanced weather equipment: **The Met Office**

About The Met Office:

The UK's Met Office uses more than 10 million weather observations and an advanced atmospheric model to create 3,000 tailored forecasts and briefings every day. To make its forecasts, the Met Office uses some of the most advanced technology on the planet, including one of the world's most powerful supercomputers. It also runs a mix of on-premise, cloud, and software-as-a-service platforms.

The challenge:

The Met Office was gathering logs from multiple systems in many locations. This was a fragmented process with different teams managing their own logging systems and storing data in multiple formats.

The solution:

The Met Office created a unified platform using Elastic Observability and Elastic Security that enabled different teams to access the data that they needed from a single pane of glass. Elastic Cloud (running on AWS and Azure) is an essential part of this platform, allowing the Met Office to scale to over 2 billion data logs each day.

The outcomes:

With Elastic powering their platform, The Met Office can:

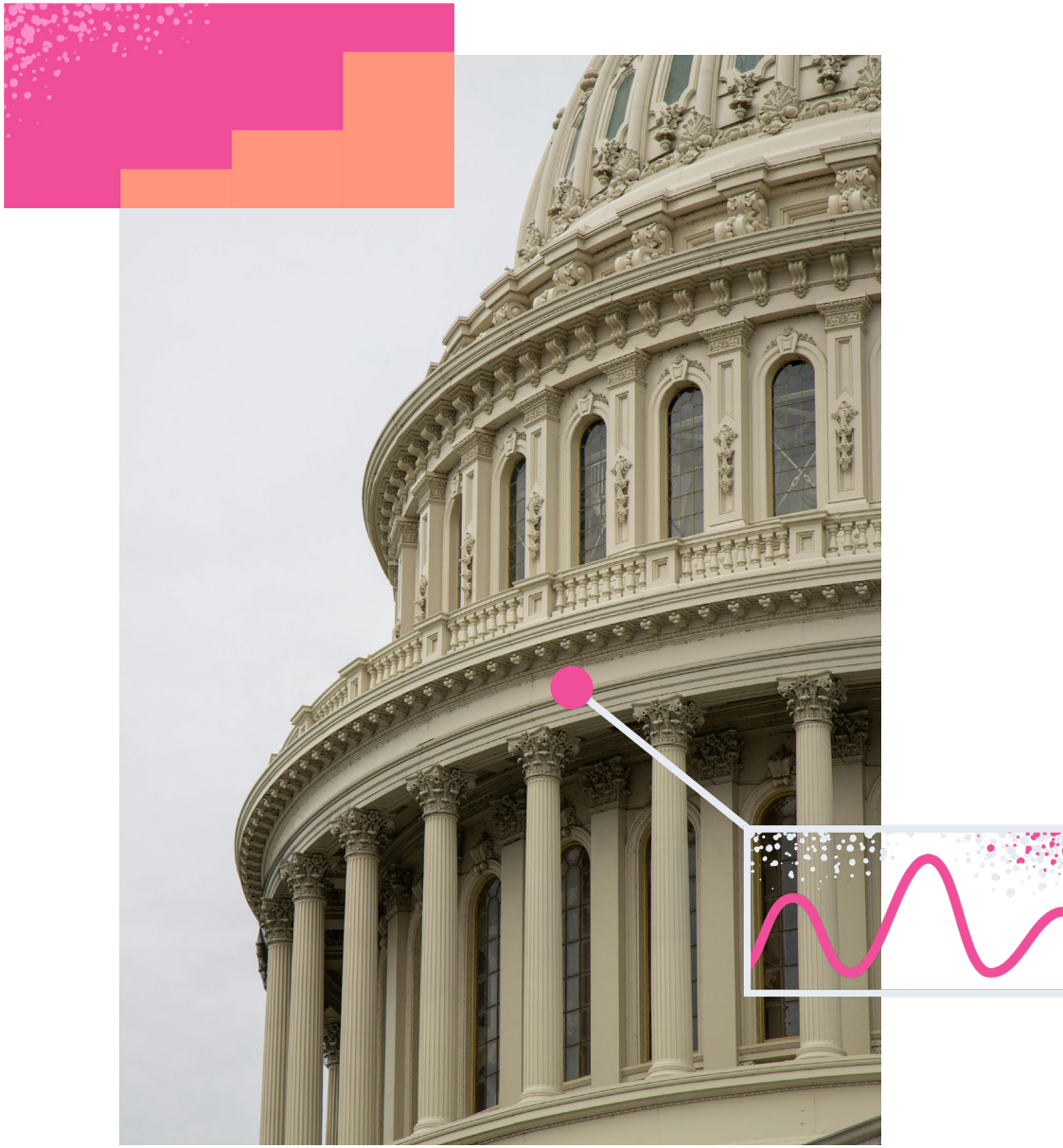
- Run searches and correlate insights that speed up the resolution of network issues
- Get a clearer view of its systems, including its National Severe Weather Warning System, which issues alerts to regions affected by extreme conditions
- Build simple search queries to find impactful events on multiple systems
- Boost system security by providing a complete view of system activity and suspicious behavior

Read the full story

> Moving to Elastic Cloud means we no longer have to worry about scaling up capacity or maintaining our observability environment. We can concentrate resources on getting the greatest possible value from information contained in our logs.

John MacGrillen
Solutions Architect, Core Services, The Met Office

Meeting constituents' digital expectations: **U.S. State Agency**



About the U.S. State Agency:

This agency – anonymous at their request – is part of a state government in the United States.

The challenge:

As its workforce suddenly needed to work remotely during the Covid-19 pandemic, the agency urgently needed to strengthen IT infrastructure resilience and increase visibility into that infrastructure. It also needed the ability to meet the new expectations of its constituents, who required services delivered to them digitally. "As the agency became more complex through technology expansion, additional legislative demand, and increased attention on cybersecurity, we needed a consolidated view of operations," noted a Consultant & Technical Lead at the agency.

The solution:

The state agency modernized its technology systems with app migration to the cloud and increased visibility with Elastic Observability. The agency created an extensive infrastructure on AWS with Elastic providing a single pane of glass to view it.

The outcomes:

With Elastic Observability, the state agency:

- Can monitor all IT processes and apps end-to-end, allowing the agency to be more proactive
- Has improved efficiency by 80% through automating processes
- Has created multiple dashboards to visualize, automate, and analyze the data gathered by Elastic
- Can monitor live support interactions and performance patterns to improve the constituent experience

Read the full story

We are transforming the way we do business internally and how we serve constituents through our technology. A key part of that success is having clear observability into our systems.

CIO
State Agency

Building safe learning environments online: **Network for Learning**

About Network for Learning:

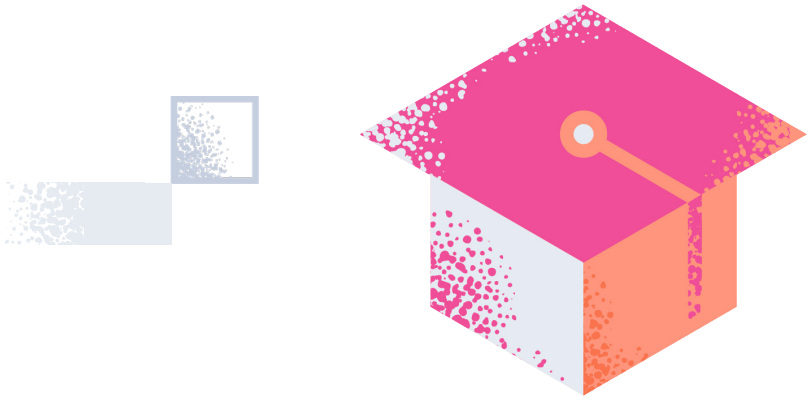
Network for Learning (N4L) is a government-affiliated organization in New Zealand that focuses on providing secure digital learning. Through its Managed Network internet services – including advanced firewall services, managed Wi-Fi, and email security – N4L helps protect approximately 900,000 users across more than 2,450 New Zealand schools.

The challenge:

N4L's log-gathering process was largely manual and time-consuming, involving simple data integration, tooling, and scripts. Another challenge was lack of visibility into the code powering their applications. "In the past, if there was an error, the DevOps team had to run lengthy investigations, from opening code repositories to debugging logs and testing a solution," said Clayton Hubbard, Head of Architecture at N4L.

The solution:

N4L had already been using the free and open version of Elasticsearch and saw the opportunity to extend Elastic across all its data platforms. This led to the deployment of Elastic Observability and Elastic Security on Elastic Cloud Enterprise. N4L uses Elastic Observability to optimize application performance in containerized environments.



The outcomes:

With Elastic, N4L:

- Pulls in multiple terabytes of data every day and handles more than 300,000 events per second
- Has a simpler way to visualize observability data in dashboards, making it easier to communicate with schools and internal customers
- Shields students from 13 million security threats each month
- Has achieved a 91% customer satisfaction rating
- Has reduced security response times from days to hours

Read the full story

> Elastic Observability puts the information at our fingertips. With APM [application performance monitoring], we can identify the line of code almost immediately and make the necessary modification on the spot.

Clayton Hubbard
Head of Architecture, N4L

Centralizing logging in a complex environment: **Driver and Vehicle Licensing Agency (DVLA)**

About DVLA:

The Driver and Vehicle Licensing Agency (DVLA) sits at the forefront of public digital services in the UK. The agency maintains more than 48 million driver records, 40 million vehicle records, and collects approximately £6 billion ($7.75 billion USD) a year in vehicle excise duty.

The challenge:

DVLA's IT department had been undergoing change for a decade, including moving to the cloud. However, they also faced technical debt, data silos, and system interoperability that slowed their pace and threatened their cybersecurity posture. The team wanted to increase cloud adoption so that they could centralize everything in one place.

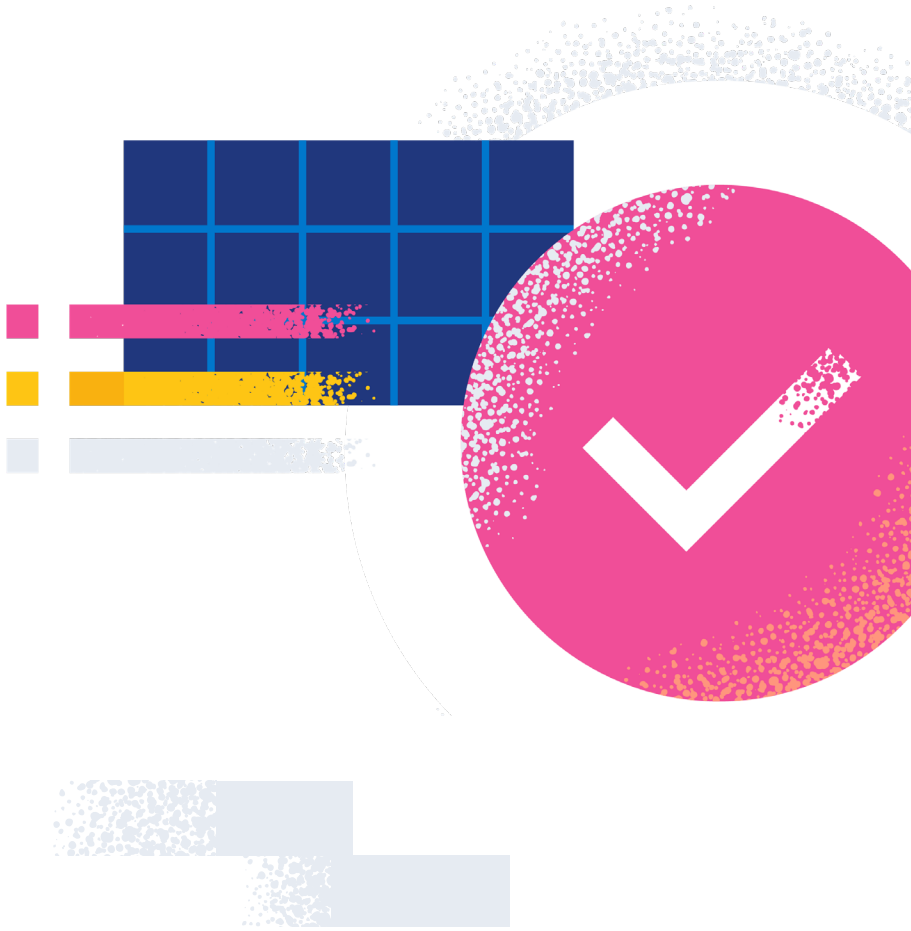
The solution:

As it moved toward its goal of delivering a cloud-first strategy, DVLA's cloud engineering team started using Elastic Observability in the cloud to centralize logs so that its employees could measure and monitor their entire ecosystem and analyze and quantify the usage of their apps.

The outcomes:

With Elastic Observability, DVLA has been able to:

- Deliver a better user experience for internal users and UK motorists in general
- Manage large quantities of data
- Create a centralized cloud platform to deliver valuable apps to UK citizens
- Leverage automation to save its engineers time
- Reduce time managing infrastructure by deploying with Elastic Cloud
- Create a center of excellence for cloud, where they share learnings with other government agencies



Hear the full story

Analyzing and monitoring infrastructure metrics: **Will County Sheriff's Office**

About Will County Sheriff's Office:

Will County has the second largest sheriff's department in the state of Illinois in the United States. Its IT department was responsible for maintaining hundreds of desktops, laptops, in-car camera systems, as well as laptops in squad cars that were disconnected to the department's network. The department had 52 servers and worked in a 24/7 environment.

The challenge:

The IT team at Will County Sheriff's Office needed to ensure operational resilience across its complex, always-on IT environment, without overtaxing its small team.

The solution:

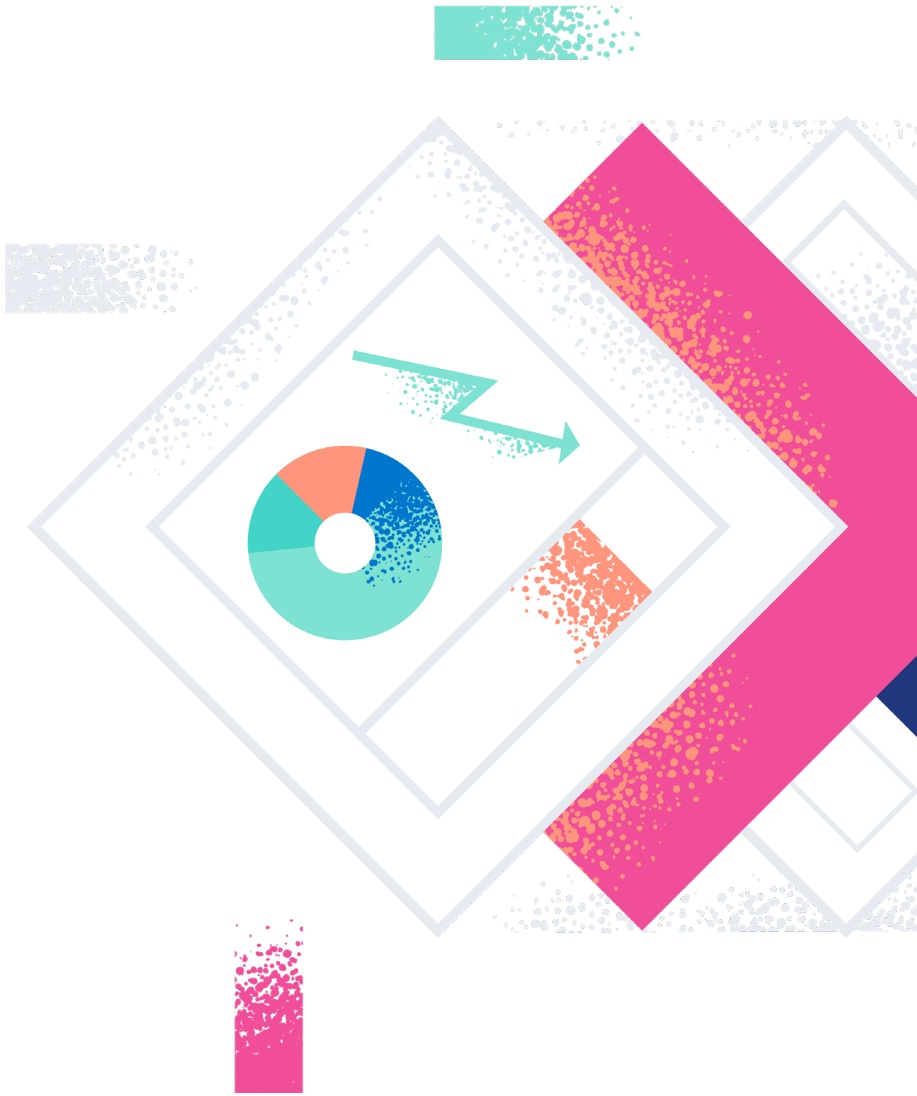
Will County Sheriff's Office turned to Elastic Observability for monitoring its network and hardware, including server metrics, network events, packet tracing, and Windows logs. The IT team also leveraged the analysis and visualization capabilities of Elastic to better understand their operations.

The outcomes:

With Elastic deployed in its IT environment, Will County Sheriff's Office can:

- Access a more in-depth picture of hardware performance and network events so that they can find issues and anomalies
- Better track employee time and attendance for more precise staffing and scheduling
- Use data to place deputies based on current and forecasted trends

Hear the full story



Unifying visibility at scale for better healthcare outcomes: **Lean Business Services**

About Lean Business Services:

Lean is a leading company that develops and empowers the health sector in Saudi Arabia, through numerous initiatives and digital products with the aim of improving healthcare and is part of the Healthcare Sector Transformation Program (HSTP) projects in Saudi Arabia. It relies on a complex IT architecture including Kubernetes and dozens of microservices that run software and applications in the cloud.

The challenge:

Lean lacked full visibility into the logs generated by its systems and relied on the efforts of Lean's engineers to identify an issue, determine the root cause, and implement a fix. "We wanted to be more proactive in our efforts to detect issues and ensure they were fixed before they impacted end users," says Haitham Alsulmy, IT Operations and Services Executive Director, Lean.

The solution:

The team shortlisted three observability platforms and ran proof of concepts to measure their compatibility with many virtual machines, Kubernetes clusters, and legacy applications. They ultimately opted for Elastic Observability for its ability to "give us full visibility into our complex cloud-native systems: to show us the full spectrum of the service and the full spectrum of the impact, so we can be proactive," said Alsulmy.

The outcomes:

With Elastic Observability, Lean:

- Has a single gateway for ingesting 1.2 terabytes of data each day
- Can significantly accelerate root cause detection and remediation anywhere in its IT environment
- Reduces the time its engineers spend reacting to incidents so they can focus on activities that support new healthcare applications and solutions
- Reduced costs of storage hardware with Elastic's ability to search and access frozen tiers, and reduce its reliance on costly warm storage

Read the full story

> By widening the Kibana dashboard availability and democratizing the benefits of data, Elastic Observability plays a key role in our efforts to bring better healthcare services and outcomes to the people of Saudi Arabia.

Haitham Alsulmy
IT Operations and Services Executive Director, Lean

Helping law enforcement accelerate criminal investigations: **Bluestone Analytics**

About Bluestone Analytics:

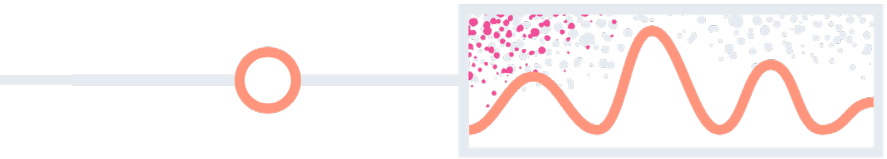
Bluestone Analytics, a CACI company, is an international leader in dark web analysis. Its technology suite, DarkBlue Intelligence, enables clients, including national security and intelligence teams, to search open-source intelligence (OSINT) and unveil the identities of criminals operating on the dark web.

The challenge:

Law enforcement organizations tasked with investigating activities such as drug trafficking and weapon sales need access to information that's only found on the quickly-evolving dark web. This data is difficult to access, and directly browsing the dark web exposes a user to risks such as malware, as well as to potentially disturbing content.

The solution:

With the DarkBlue Intelligence suite, powered by Elasticsearch and Elastic Observability, users can search information from the dark web in a safe, text-based environment without having to download an actual dark web browser. The Bluestone Analytics team leverages Elastic Observability for application performance monitoring (APM) and real user monitoring (RUM).



The outcomes:

With Elastic deployed in its IT environment, Will County Sheriff's Office can:

- Get detailed web application performance metrics and error tracking, as well as distributed tracing for all outgoing requests
- Archive data indefinitely and quickly access historical data for a complete view into investigations
- Quickly ingest and incorporate structured and unstructured data, ensuring long-term scalability and agility
- Provide potentially life-saving insights to the right people, regardless of how the dark web evolves

Read the full story

Our clients trust us, and we trust Elastic. It has always been the best search and observability technology to discover, pursue, and engage criminals who rely on the dark web to obscure their identities and conduct illicit activities.

Jason Nack
Head of Technology, Bluestone Analytics

Summing up

Elastic Observability leverages the power of Elastic's search analytics platform, delivering speed, scale, and relevance that public sector organizations need to ensure operational resiliency in their IT environments. A 2023 Forrester Economic Impact Study found that Elastic customers experienced the following benefits from Elastic Observability:

85%
less time identifying & resolving incidents by year 3

75%
reduction in application deployment time by year 3

+22K%
data analyst hours saved by year 3

3%
increase in customer retention rate by year 3

25%
reduction in customer support calls

+1.2M
savings from tool consolidation

elastic | The Search Analytics Company

To learn more about Elastic for public sector, visit our website: elastic.co/industries/public-sector, or contact us directly at elastic.co/contact/publicsector.

We'd love to hear your story.