

# BAE Systems DataRetain™

Compliance for the Digital Era

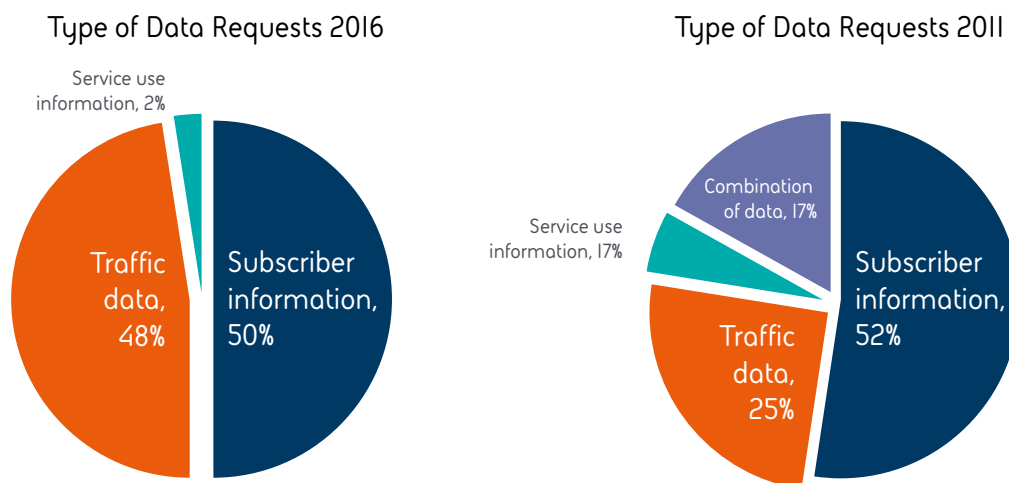
Serving your business risk and compliance requirements while your technology drives towards virtualisation and cloud

# The Business Challenge

Communication Service Providers (CSPs) continually walk a fine line between their obligation to maintain customers' privacy and their obligation to government regulations as a key intelligence asset for law enforcement to combat serious crime. It is an ongoing responsibility as they drive to build efficiencies and be agile in the face of changing customer demands. On top of this Law Enforcement Agencies (LEAs) are eager for quicker and easier access to information whilst still in a controlled and regulated manner.

The CSPs have to find the right balance of technology, people and processes to enable both - strong control of the personal data and being a good responsible company in the light of the government and regulatory body. Many have turned to producing transparency reports that show what obligations they have and how they respond to these queries. This on the surface seems simple yet for large and small CSPs alike the effort to support this can be burdensome.

Data gathered using publicly available sources shows that LEA demands for support from CSPs, ASPs and other content providers has been on rise<sup>1</sup>. Tier 1 CSPs like Verizon and AT&T receive more than 250,000 such requests every year<sup>2</sup>. In addition, LEAs are beginning to request new types of information including IP, Wifi and OTT services. These requests have more than doubled over the last few years:



Data Source: Interception of Communications Commissioner (IOCCO), UK<sup>3</sup>

These new types of information sources are not easily retained, searched or intercepted. Some cases have even led to wrongful arrests, for example, The Interception of Communications Commissioner (IOCCO) has expressed concern around errors especially in tracing IP addresses<sup>4</sup>.

<sup>1</sup> Data collected from IOCCO in the UK and individual CSPs in the US

<sup>2</sup> AT&T 2019 Transparency Report

<sup>3</sup> Data for more recent years is not available

<sup>4</sup> Interception of Communications Commissioner's (IOCCO) letter 2017

# The Opportunity

Historically, data requested by LEAs has been generated as part of normal business processes for CSPs, but increasingly, it's not as straightforward as the CSPs architecture moves towards virtualisation and LEAs need responses to more complex questions. Network Functions Virtualisation (NFV) and Software-Defined Network (SDN) are the underpinning foundational technology pieces for 5G. And the implication of it is that CSPs' approach of building their own data storage and data analytics would no longer be enough.

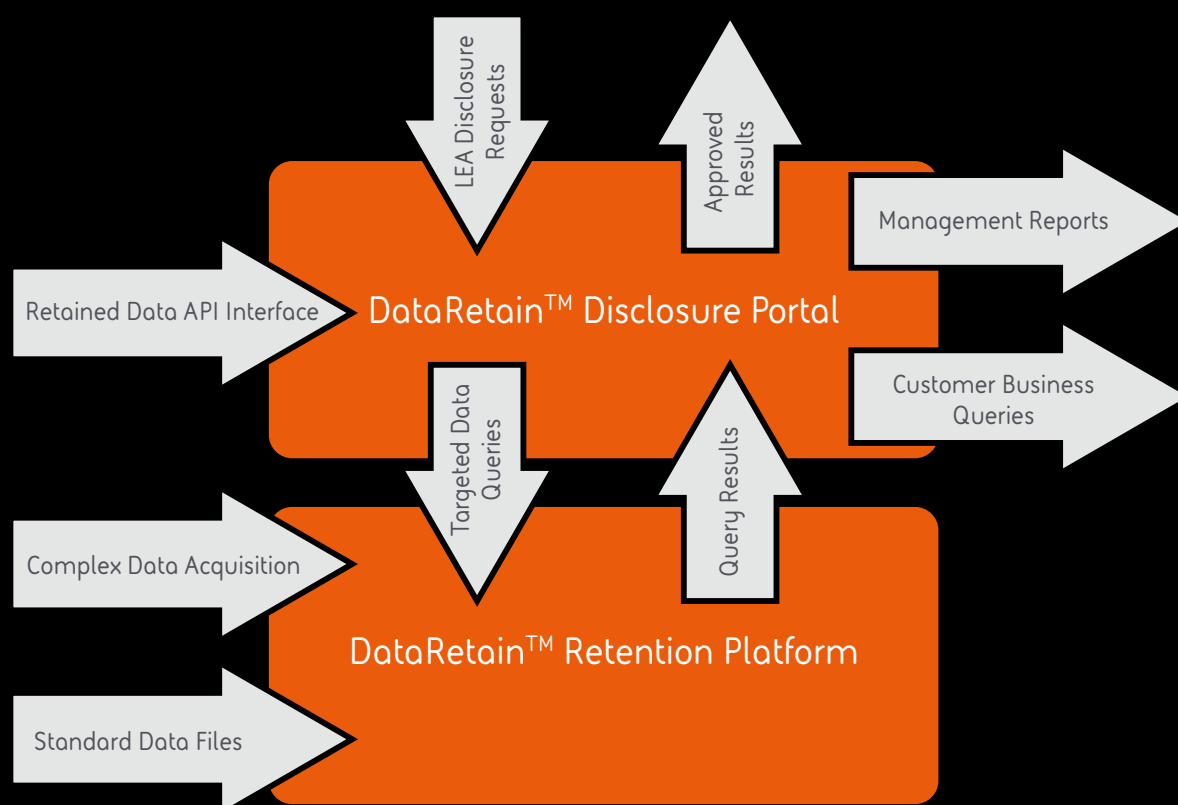
Furthermore, as new data retention regulations come in to place that ask CSPs to provide fine grained access to specific events linked to individual customers and to store data for longer periods of time, CSPs are finding that their existing in-house solutions cannot scale to the sheer volumes of data they must now store or the growing number of requests they receive from LEAs. In addition, as communications data volumes explode, many CSPs are struggling to achieve this without dedicating resources specifically for this purpose.

CSPs are realising that the only way to successfully manage their obligations with existing and future data retention legislation, is by implementing a dedicated data retention solution.

# DataRetain™ – Compliant by Design

BAE Systems NG-DataRetain™ is virtualised and cloud-ready. It is purpose built to support CSPs' data retention and disclosure requirements and is incredibly adaptable to fit with most CSPs internal business systems and workflows.

The solution provides a seamless interface between LEAs and CSP police liaison units. It provides authorised CSP users with the full breath of functionality required to run a trusted, secure, data disclosure service for compliance with LEA requests. It features a quick and simple user interface whose workflow management features can be easily configured to adapt to your current business processes and query types. This allows a CSP compliance team to provide top quality, highly-automated responses to LEA data requests with minimal disruption to business operations. In particular, the automation of common, repetitive tasks in the disclosure process allows a higher volume of requests to be processed by a lower number of staff.



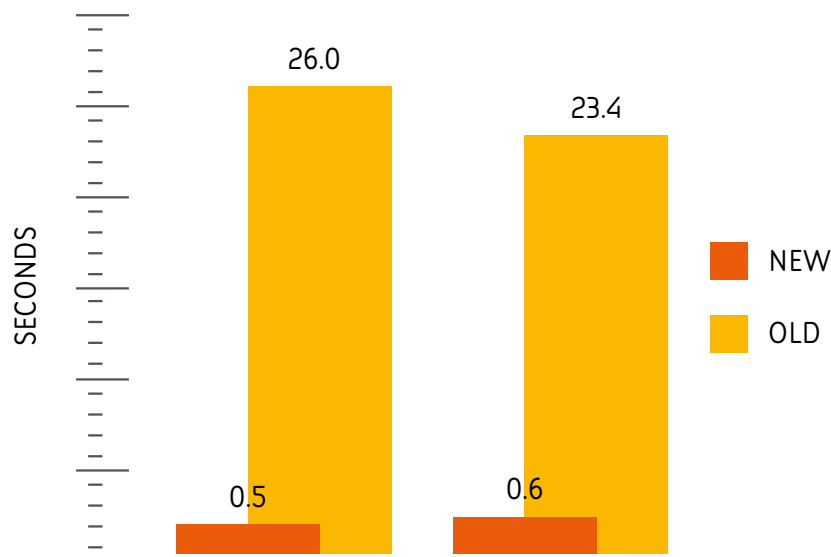
# DataRetain™ Features

BAE Systems DataRetain™ is a cost-effective data retention compliance solution which:

- Provides a comprehensive workflow and request management web portal with support for single sign on
- provides a self-service data retrieval portal and retained data API for law enforcement agencies
- provides a comprehensive audit trail of user transactions, helping assure that retained data is of evidential quality
- provides a REST based API for connectivity to existing business systems for standard data requests
- provides fast, compact and scalable encrypted data storage and retrieval for more complex data types, capable of storing billions of data records securely
- increases automation so records are available for retrieval within seconds of being stored and can be retrieved within milliseconds
- enables data records and results to be set for automatic deletion at the end of mandated data retention periods
- can be implemented as a highly available solution with full back-up and disaster recovery achieved by replicating all data to a secondary system
- can be configured in multiple languages

## Key advantages

Significant reduction in data disclosure request processing time – customers using BAE Systems data retention solution can enjoy reduction of over 95% in the time taken to view requests, resulting in faster processing of overall disclosure requests.



- **Complete deployment flexibility** - in your own cloud or subscribe to the BAE Systems Cloud Data Retention service. It runs in any cloud or physical environment using the latest container based architecture
- **Minimal implementation time** - as a subscription service can be setup and configured in the space of 6 weeks
- **Trusted by customers** - more than 90% of our customers are using solutions for over a decade, with prompt upgrades to newer versions
- **Extensive product development** - 25+ years of credibility in the lawful interception and data retention space, from both CSPs and national security sides

BAE Systems processes over **60%**  
of the UK Lawful Communications  
Data Disclosure Requests



**30 Years**

Heritage in providing law  
enforcement compliance  
solutions to CSPs



**20%**

Increase in  
portal speed in  
latest release V8

**15** Solutions worldwide  
spanning **4 continents**



**10,000**

Queries processed  
every day **24\*7\*365**



**100 Trillion**

Records retained over  
rolling 2 years and  
searched in sub-seconds

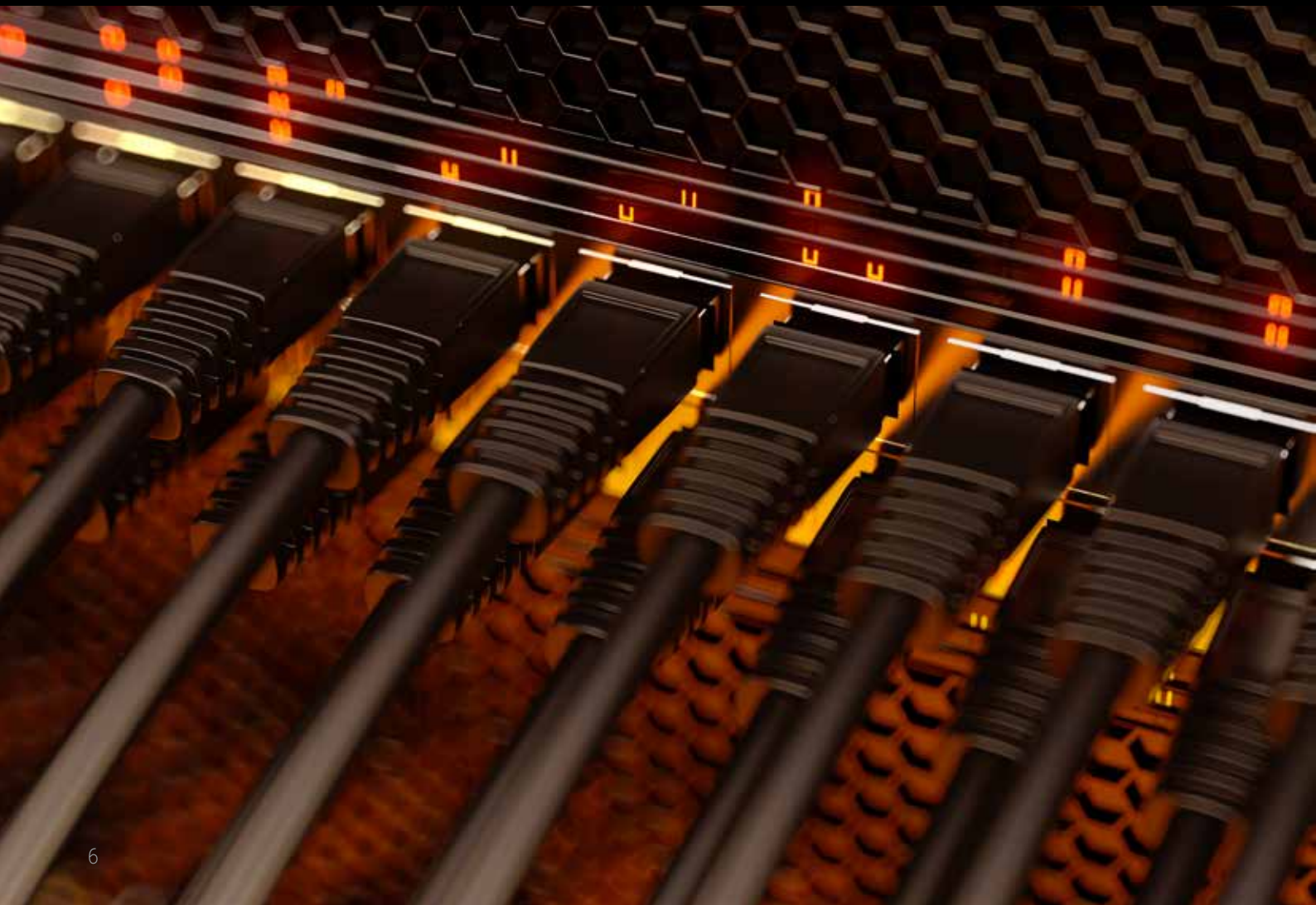
# BAE Systems Portfolio

## Lawful interception

BAE Systems' Lawful Interception (LI) product – DataBridge™ is cloud-native and 5G ready. It is built with the virtualisation principles in mind that will enable CSPs to remain compliant with their LI obligations whilst still being agile and driving efficiency in the network. Without scaling down any of the functionality of hardware-based solution, DataBridge (vLI) now enables CSPs to automatically orchestrate and provision the required LI capability at the same time as the CSP services in the cloud. This provides significant flexibility to the CSPs and allows them to focus on virtualising, safe in the knowledge that the required lawful interception service can easily be added to ensure any new capacity or service remains compliant with the local Lawful Interception regulations.

## Secure and enhance the connected world

BAE Systems helps our clients thrive in the connected world, across all three primary digital transformation domains – business, customer engagement and operations.





## cyber\_reveal

A comprehensive suite of technology and services that bring clarity to your cyber security.



## National threat defence

We make the tools and provide the skills that help nations form intelligence to protect their citizens from harm, and help secure their networks and organisations from the most advanced, hostile threat actors and cyber attacks.



## Digital and Data Services

We provide comprehensive digital, data and cyber security services to government and commercial customers.

## We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters  
BAE Systems  
Surrey Research Park  
Guildford  
Surrey GU2 7RQ  
United Kingdom  
T: +44 (0) 1483 816000

BAE Systems  
265 Franklin Street  
Boston  
MA 02110  
USA  
T: +1 (617) 737 4170

BAE Systems  
Level 12  
20 Bridge Street  
Sydney NSW 2000  
Australia  
T: +612 9240 4600

BAE Systems  
Arjaan Office Tower  
Suite 905  
PO Box 500523  
Dubai, U.A.E  
T: +971 (0) 4 556 4700

BAE Systems  
1 Raffles Place #23-03, Tower 1  
Singapore 048616  
Singapore  
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford  
Surrey, GU2 7RQ, UK

E: [learn@baesystems.com](mailto:learn@baesystems.com) | W: [baesystems.com/businessdefence](http://baesystems.com/businessdefence)

 [linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)

 [twitter.com/baesystems\\_ai](https://twitter.com/baesystems_ai)

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155  
UK: 0808 168 6647  
Australia: 1800 825 411  
International: +44 1483 817491  
E: [cyberresponse@baesystems.com](mailto:cyberresponse@baesystems.com)



Certified Service

CPNI  
Centre for the Protection  
of National Infrastructure

Cyber Incident Response



Copyright © BAE Systems plc 2019. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.