XTS IRIS
Cross Domain Portfolio

Providing National Security and Defence organisations with the next generation of Cross Domain hardware enforced capability

Digital Intelligence

BAE SYSTEMS

Enabling secure information exchange between network domains of different classification or trust

Cross Domain Solutions

Supporting intelligence and defence missions with the enterprise-grade security relied on by governments to protect and connect their organisations.

For many years, BAE Systems has been providing Cross Domain Solutions (CDS) to Goverment organisations. These CDS provide content and network threat defence between networks of different security classifications or trust levels. This enables our clients in Intelligence Agenies, Law Enforcement, Military and Critical National Infrastructure (CNI) to move information between security domains without compromising the Confidentiality, Integrity or Availability of the information and networks concerned.

We do this at a global scale.

BAE Systems Global CDS Teams

When dealing with Government organisations which process information of the highest sensitivity, concern for security standards must cover not only the products and solutions produced by a vendor, but also the whole security ecosystem of that vendor. **This includes the security and accreditation of the vendor's offices, of its supply chain and partners, its staff and recruitment, amongst others.**

BAE Systems has been a partner of Governments, Defence and National Security Organisations for many decades. During this time, our working practices and environments have become an extension of many of our customers, ensuring that security principles are embedded in everything we do, how we operate, and how we function. We work closely with our customers to build, deploy and maintain solutions that help them achieve in their various missions.

Our customers are predominantly in the Government and CNI areas described above, and our Cross Domain Solutions are not sold to commercial organisations where the usage and handling of our solutions could cause concern.

To support our customers, BAE Systems has a global team delivering operational capability on a daily basis. We have **security-cleared 5-Eyes teams** based in the UK, Australia and US, each with deep expertise in hardware, firmware and software development, as well as in-country manufacturing capabilities.

In addition, these teams have **years of experience working in the most sensitive Government domains:** we are much more than hardware or software providers - we have a deep understanding of our customers and directly support them in every aspect of their missions.

For customers, our teams provide:

- **Technical Services and Consultancy** to support customers with specialist skills, information, research activities and advice across all areas of Cross Domain.
- **Systems Integration programmes** to design, deliver and hand over new operational capabilities.
- **Products built using BAE Systems specialist hardware and proprietary software** to solve the hardest problems.
- **Support and Managed Services** to ensure the deployed systems remain secure, operational and fit for purpose.

01

Security Target

Every CDS we design starts life with a Security Target. This defines the perceived threats the CDS is likely to meet, what security controls the CDS will implement and the residual risks.

02

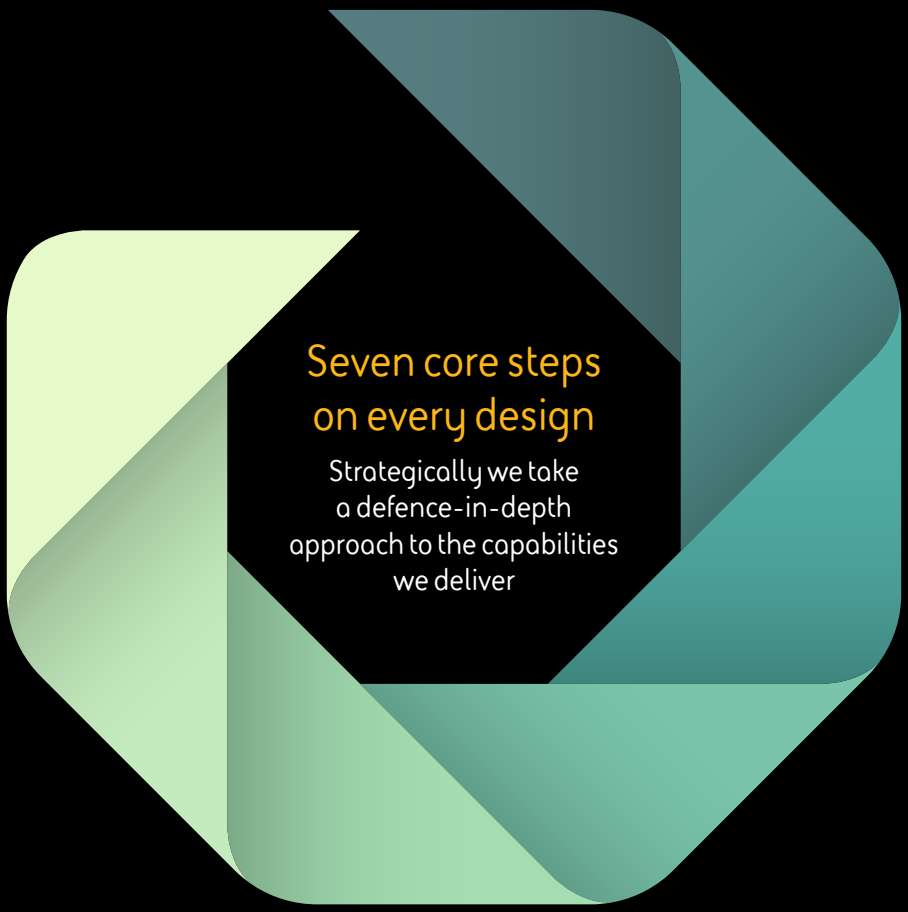
Security classification

Agreeing the classification of the design and implementation artefacts upfront with a National Technical Authority (NTA) is crucial. All our work is UK SECRET.

03

Manufacturing Security Plan

Defining and agreeing a robust MSP upfront with an NTA mitigates against supply chain vulnerabilities.



04

Application specific filters

An Access CDS will have a very different set of filter requirements to a Transfer CDS, while Transfer Streaming CDS will be different again.

05

Platform specific filters

A common extensible platform that can run many applications. Examples of these filters are system updates, log validation and system integrity.

06

Hardware/ software split

Define and agree the right balance of functions to be implemented in software and hardware. For us we assume that both high and low software is compromised.

07

Key Management

Our capability has numerous key material, some are specific to us, some are specific to an NTA and some are specific to system administrators. There might also be some application specific keys. This is all documented to ensure robust handling of key material.

We started our journey in hardware CDS in 2008, we were the first company to design and deliver hardware CDS into operational deployments.

We have always worked in partnership with NCSC, ACSC and the NCDSMO. Our existing portfolio of 5 hardware Gateways are in active service protecting up to TS networks.

in association with National Cyber Security Centre

ACSC Australian Cyber Security Centre

Secure Development:

Fully Cleared (SC & DV) product teams (Developers, Testers, Architects, Managers) working on Accredited SECRET development networks, following Secure Coding Guidance.

Securely Manufactured in the 5Eyes:

Built by BAE Systems utilising a Secure Supply Chain (NCSC Approved) using 5Eyes Security Cleared personnel.

Who can benefit from a Cross Domain Solution?

The need for more agile, efficient and collaborative ways of working is common across multiple organisations who can all benefit from their deployment. These include:

National Security and Law Enforcement

When every second counts, agencies must get sensitive data to those who need it, quickly, efficiently and securely. CDS support National Security and Law Enforcement Agencies by allowing users to securely bring information from other sources, partners, and remote networks into a centralised location to build a unified intelligence picture, and then collaborate and share intelligence insights rapidly with those who need them. CDS also enable users to browse down securely from networks of high trust to those of lower trust, from their own desktops, without adding significant additional network infrastructure.

Defence Organisations

Defence organisations operate across many networks: they need to collaborate with other nations across sensitive networks, but control what is shared; they need to communicate quickly, often over disadvantaged links, with communication security being paramount; they need to run training exercises involving sensitive data and capability between different networks; they need to bring data together for monitoring (e.g. in a Security Operations Centre), or for Information Advantage in Joint Operations.

Secure Government Departments

Many aspects of governing a nation require utmost confidentiality. From government classified documents, defence plans, foreign policy documents, all the way down to lists of employees, governments often find themselves needing to share information across security domains.

Critical National Infrastructure

Industry is competitive and cost-driven. To become more efficient, drive down costs and improve competitiveness, CNI organisations need new ways to enable secure information exchanges to communicate with and control their industrial systems from their business IT networks – seamlessly and with minimal latency.

Transfer CDS:

Sensitive information needs to be shared between users or machines across network boundaries, often where the networks are of different security classifications. This class of CDS supports:

- Machine-to-machine data transfers.
- Secure mobile working and mobile device management.
- Secure email between domains.
- User and ad-hoc Import and Export of data between domains.
- Secure collaboration: organisations need to be able to hold secure voice and video calls both within their organisation and with partner agencies, efficiently, and with minimal latency

Access CDS:

Users on sensitive networks need to be able to access the internet or view information on networks of a lower trust class ('secure browse down').

"When every second counts, agencies must get sensitive data to those who need it, quickly, efficiently and securely."

BAE Systems XTS IRIS

Common hardware platform covers a wide range of mission needs

Transfer | Access

Certified for uni-directional and bi-directional Access and Transfer CDS requirements between networks, domains, and electronic assets.
Purpose built hardware by BAE Systems ensures supply chain integrity and highest level of risk mitigation a CDS can offer.

At the heart of the hardware is BAE Systems proprietary Transform, Verify and Reconstruct Engine (TVRE).
The TVRE is a hybrid capability implemented in hardware and software. This is unique, striking the right balance between systems integration and complexity vs hardware enforced security.

Available in a range of form factors covering:

Large Scale Enterprise, Small Scale Enterprise and Tactical (Roadmap)

BAE Systems XTS IRIS Portfolio Overview

Transform

The control mechanism to reduce the risk of a successful network-based attack

As data arrives into the TVRE for transmission through the CDS, the data is transformed from its original format into an 'easily verifiable format', which enables it to be handled by the Verification engine within the TVRE. The core functions of the Transform component are:

- **Simple transfer protocol with a protocol break:** A protocol break terminates the network connection, and the application protocol. The data payload is then passed via a simplified protocol to the verification component. This makes a protocol based attack against the destination system much more difficult.
- **Unidirectional flow control:** This ensures that data only flows one way through the channel. Flow control does not stop a vulnerability being exploited within the destination system, but it can make it difficult for an attacker to perform command and control, export data, or simply learn more from the sensitive services or data being protected.
- **Transform complex data types:** For complex file formats, building a robust Verification engine is not feasible. The Transform component therefore transforms complex data structures into simple ones that a robust verification engine can verify and thus reduces the risk of a malicious attack succeeding. The transformation process can neuter malicious content and remove unwanted content.

Verify

The control mechanism to ensure the data passed by the transformation engine is syntactically and semantically as expected. It is the component that ensures the validity of content before it reaches the system that will interpret it.

Once the data has been transformed into an easily verifiable format it is passed to the verification component for processing. Note the BAE Systems Verify component also enforces the protocol break and unidirectional flow control and is always implemented in FPGAs. The core functions of the Verify component are:

- **Syntactic verification:** Ensures the structure and syntax of the data object are correct (e.g. that the content is valid XML or JSON which conforms to a specified schema).
- **Semantic verification:** Ensures that the meaning of the data is valid in the context of the operation or business process being performed.

Reconstruct

The control mechanism to rebuild the verified content into its original (or different) format so that it matches the format expected by the destination system

Once the data has been verified it is passed to the reconstruction component for processing.

The core function of the Reconstruct component is:

- **Reconstruct data into format required by destination system:** The data being transmitted is rebuilt and reconstructed into the correct format and protocol required by the destination system. In some architectures and use cases where data is transmitted between two CDS, each on the boundary of different networks, data may at this stage be encapsulated within a proprietary protocol and encrypted for transmission across a WAN.

"Building on over fifteen years of high speed Cross Domain information exchange capabilities for the most secure and mission-critical organisations on earth and space."

BAE Systems XTS IRIS Portfolio Overview

The BAE Systems XTS IRIS platform is a new Cross Domain Solution (CDS) with ultra-high bandwidth, offering extreme scalability, ultimate flexibility and impressive modularity. Building on over fifteen years of high speed Cross Domain information exchange capabilities for the most secure and mission-critical organisations on earth, this CDS enables secure collaboration and data sharing between organisations and security domains to deliver game-changing performance at unrivalled scale.

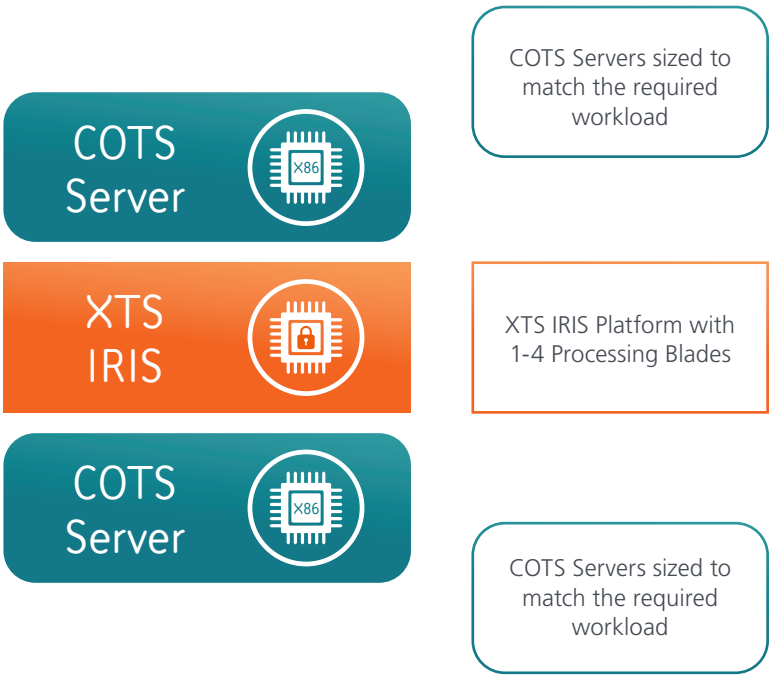
The capability is compliant with the UK NCSC, Australian ACSC and the US NCDSMO Cross Domain Architectural Patterns and specification for the full lifecycle of the capability.

UK CAPS Approved. Being evaluated against the US Raising The Bar (RTB) 4.1 specification.

As part of its modular flexibility, the XTS IRIS platform is available in the following form-factors to suit a wide variety of deployment scenarios:

XTS IRIS Large Scale Enterprise

A modular architecture using a blend of BAE Systems proprietary hardware and Dell COTS servers to deliver enterprise scale and flexibility. Available in 1, 2, 3 and 4 blade configurations delivering between 10 to 40Gbps of network connectivity and between 40 to 160Gbps of raw data throughput.



Key Specifications

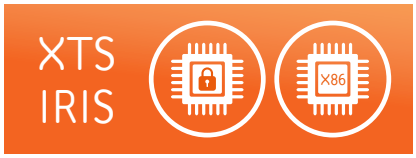
- Blade and Chassis System allowing up to 4 Processing Blades per Chassis
- 10Gbps to 40Gbps per Processing Blade, and up to 160Gbps of raw Application power per chassis
- Ability to mix and match Applications on one Chassis (e.g. Video, Browse and Transfer)
- Further scalable via Load Balancers

COTS Servers

- Supplied by BAE Systems or Customer
- Fixed part numbers to guarantee compatability & support

XTS IRIS Small Scale Enterprise

A single 1U 19" rack mountable appliance using a blend of BAE Systems proprietary hardware and COTS Single Board Computers (SBC) to deliver small scale enterprise capability. Available in a single blade configuration delivering 10Gbps of network connectivity and 30Gbps of raw data throughput.



XTS IRIS Platform with
1 Processing Blade and
2 SBCs

Key Specifications

- Compact 1U CDS for smaller requirements
- 1 Processing Blade
- 1 or 2 SBC Blades for pre/post data processing
- Up to 30Gbps of Application power
- 10Gbps network connectivity
- Further scalable with Load Balancers

Both form factors can run any of our Cross Domain applications and the Large Scale Enterprise can run multiple different applications simultaneously.
This enables organisations to run the first ever hybrid cross domain capability.

XTS IRIS Tactical (In development)

A variety of tactical form factors are being developed, these will share common components and security features as the data centre form factors. These are expected to include:

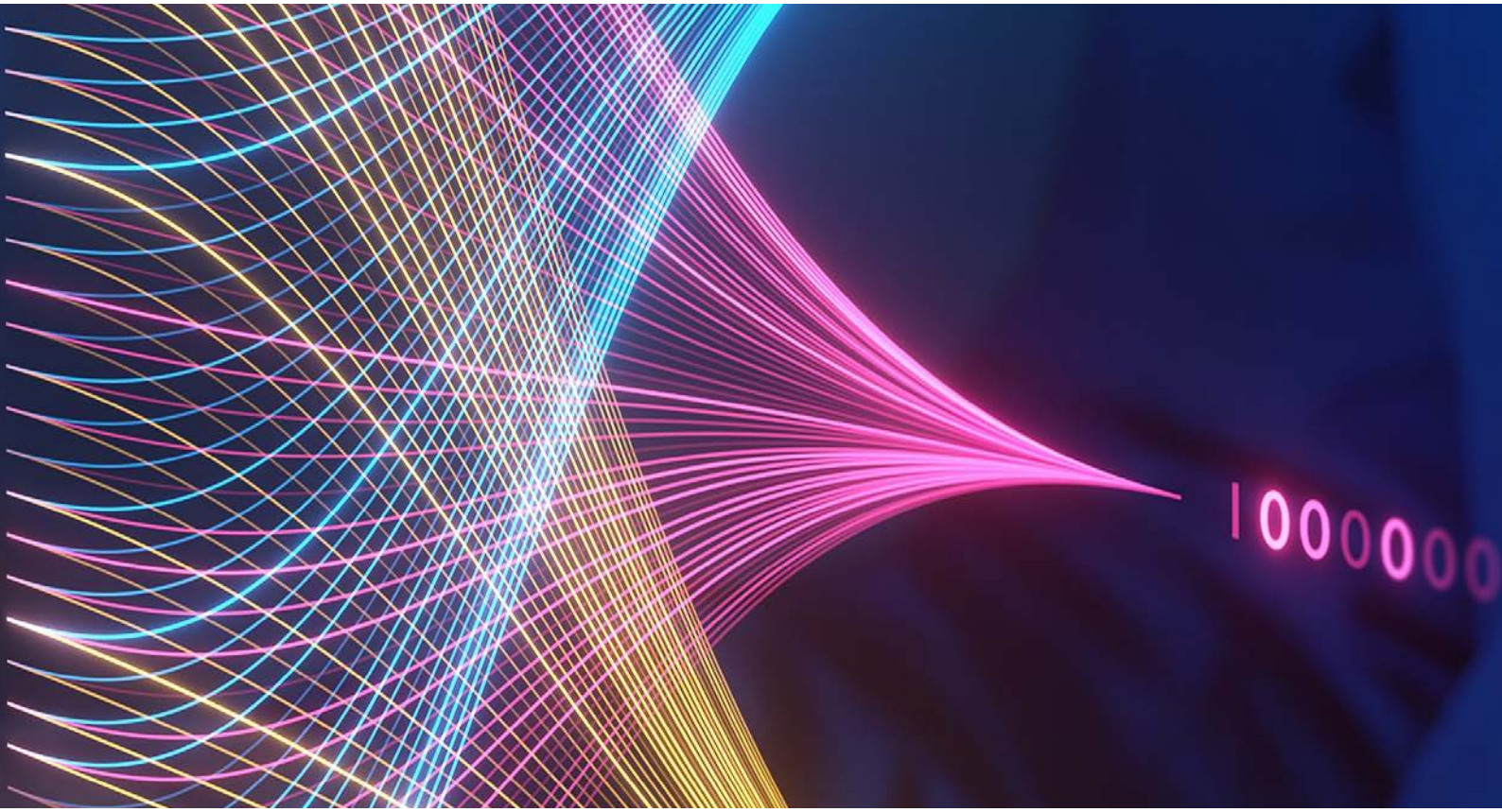
01 **Forward deployed enterprise –** the power of a enterprise CDS with features allowing it to be forward deployed.

02 **Forward deployed –** reduced capacity man packable CDS for rapid deployment scenarios.

03 **Platform mounted –** suitable for use on Land, Sea and Air platforms, including Uncrewed Systems (UxS).

04 **Wearable –** extremely low Size, Weight and Power (SWaP) device providing CDS at the edge.

05 **Space –** hardened and designed for the extreme environment of space.



We work collaboratively across the globe to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments.

Access CDS

Secure Access Gateway

The Secure Access Gateway (SAG) allows an organisation to take the next step in collaboration, enabling their workforce to achieve higher productivity by unlocking traditionally siloed networks and systems. The SAG allows users to securely connect to networks of different trust levels either inside or outside an organisation, while ensuring this does not introduce unacceptable risk into the organisation through a blend of hardware based security controls and human-factor features to assist users.

Alongside the benefit of enabling wider collaboration and increasing user productivity, by deploying the SAG, organisations can rationalise their communications estate by reducing the number of devices on a user's desk, reducing operational costs year after year.

Key Security Features

- Hardware filtering of screen, interactions (keyboard/mouse), audio and session data
- Full protocol break (Protocol Filtering Diode (PFD))
- Full logging and audit capabilities

Example Use Cases

- Web Browsing from secure systems
- Remote fleet management (CLI/GUI)
- Cross-network browsing
- Desktop rationalisation
- Remotely managing Operational Technology (OT) equipment

Features

- Dedicated Resource Mode: Dedicated resources reserved for each session
- Shared Resource Mode: All resources are shared with all sessions
- Low latency near real time experience for users
- Dual Monitor support
- Supports full-screen Video and Voice
- Support for 4k, Ultrawide and FHD (and below) screen resolutions
- Further scalable via Load Balancers

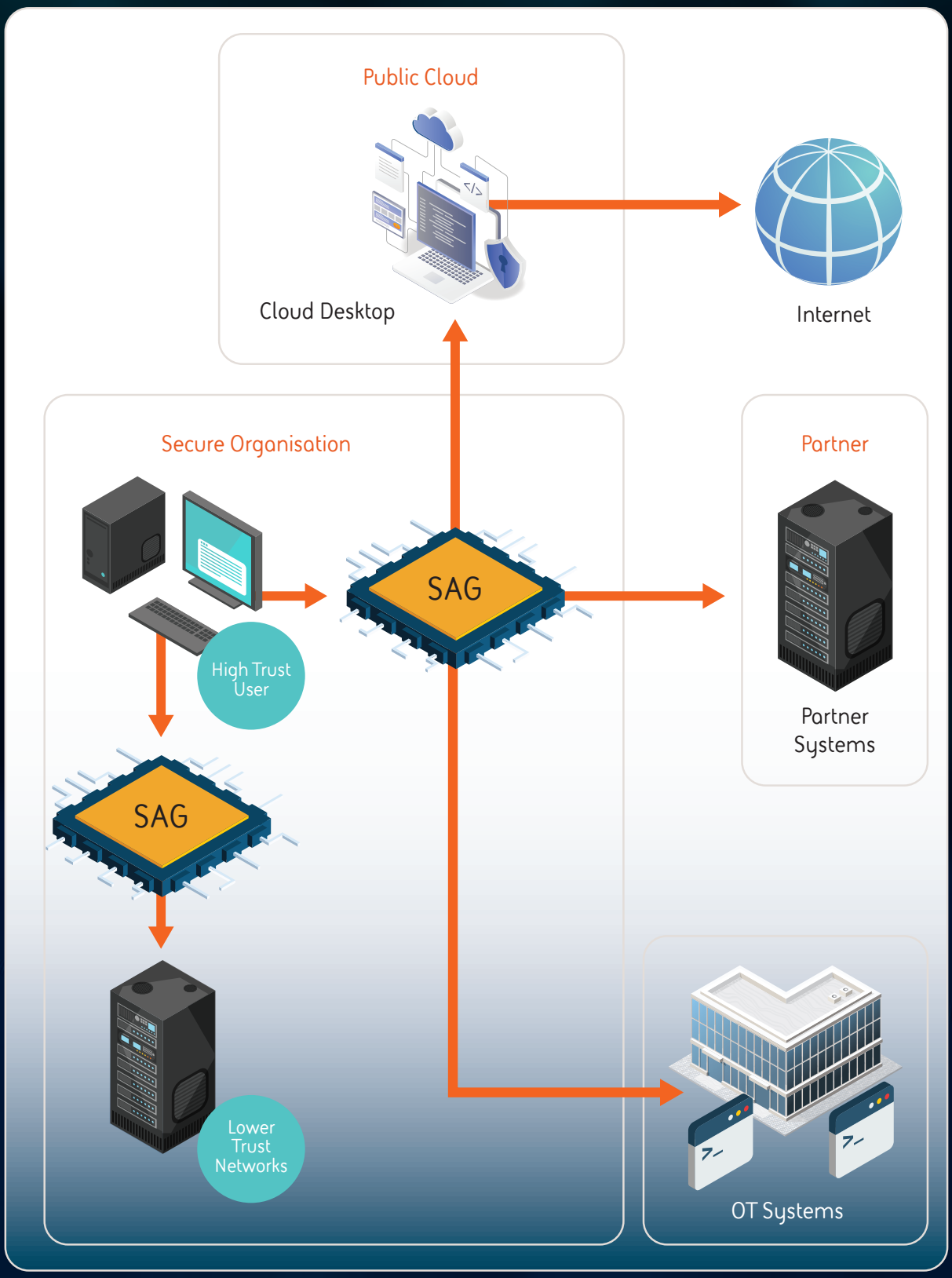
Supported Destination Systems

- MS Remote Desktop Services
- MS Azure Virtual Desktop
- VNC
- Citrix
- VMWare Horizon
- AWS Workspaces
- SSH-based CLI

Resolution

- Up to 150 sessions per Blade, or 600 per Chassis
- 1080p at 30fps

Allowing users to securely connect to networks of different trust levels without introducing unacceptable risk


Public Cloud
Cloud Desktop
Internet
Secure Organisation
Partner
SAG
High Trust User
Partner Systems
SAG
Lower Trust Networks
OT Systems

Transfer CDS

Secure Voice & Video Gateway

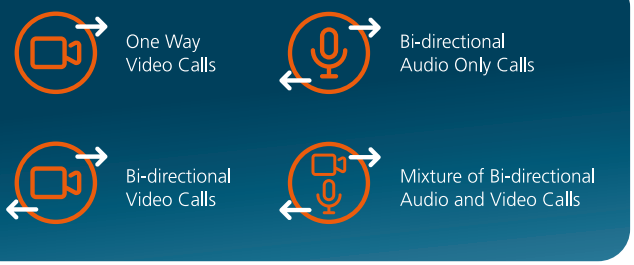
The Secure Voice and Video Gateway (SVG) allows an organisation to take the next step in collaboration, enabling their workforce to achieve higher productivity by unlocking traditionally siloed communication systems. The SVG Application can securely connect communication systems of different trust levels either inside or outside an organisation, whilst ensuring this collaboration does not introduce unacceptable risk into the organisation through a blend of hardware based security controls and human-factor features to assist users.

Key Security Features

- Hardware filtering of Video
- Hardware filtering of Audio
- Hardware filtering of Session Data
- "Human Factor" controls
- Full protocol break (Protocol Filtering Diode (PFD))
- Full logging and audit capabilities

Features

- 500 concurrent VoIP streams across network boundaries per Blade (2000 per IRIS Chassis)
- 25 concurrent VTC streams up to a resolution of 1080p at 30fps per Blade (100 per IRIS Chassis)



Supported Protocols and Codecs

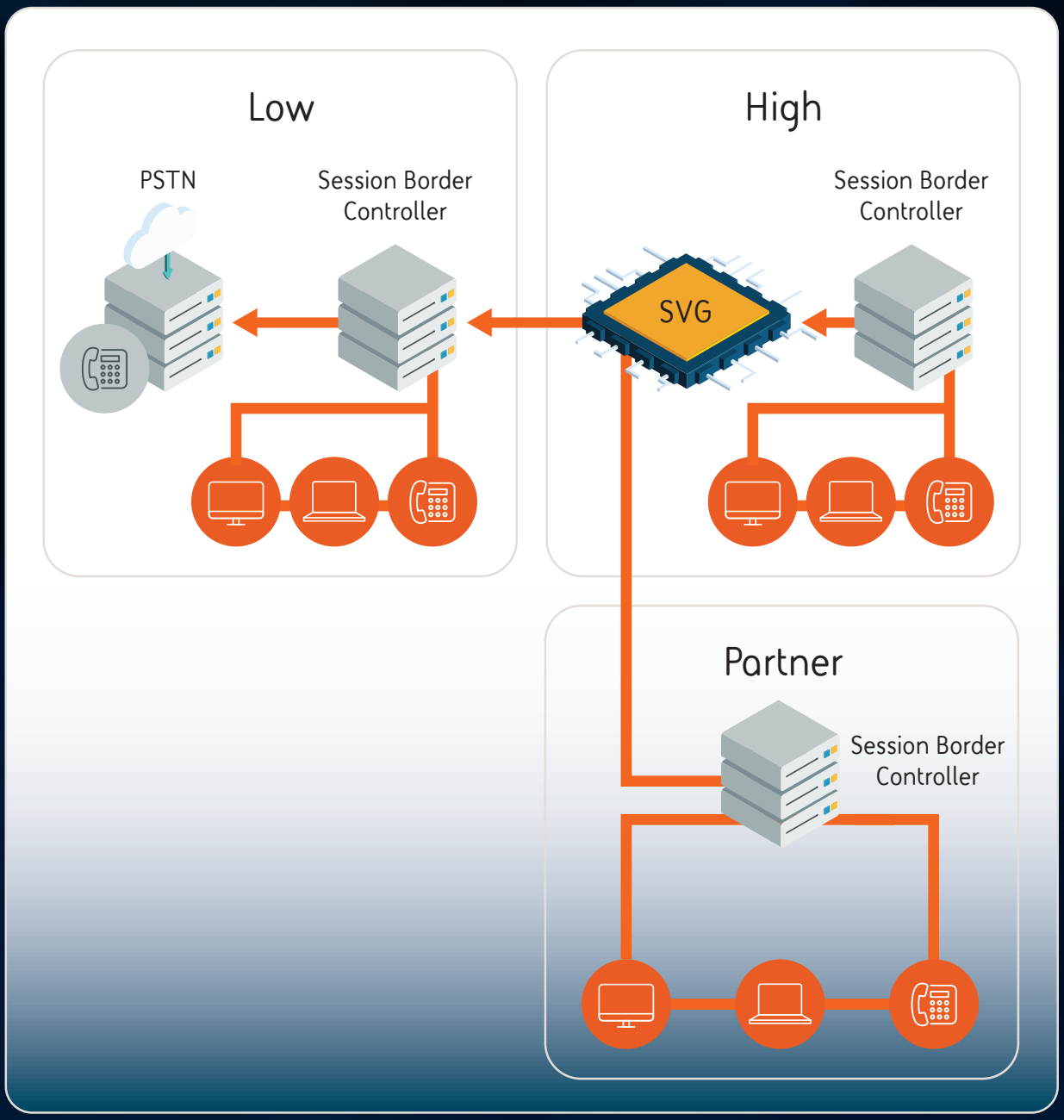
- SIP, SIP/S
- RTP, SRTP
- H.264
- G.722

Standards Compliance

- RFC5359, RFC3261, RFC3264, RFC4961

Alongside the benefit of enabling wider collaboration, by deploying the SVG, organisations can rationalise their communications estate by reducing the number of different devices on a user's desk, reducing operational costs year after year.

The SVG has been designed to easily integrate into an organisation's communications systems by utilising Commerical Off The Shelf (COTS) Session Border Controllers (SBC) (e.g. Cisco CUBE). This enables the Gateway to support a wide number of end-points allowing the existing infrastructure to operate without costly replacement programmes.



Transfer CDS

Secure Transfer Gateway

The Secure Transfer Gateway (STG) allows an organisation to take control of their data by allowing the controlled secure transfer of data between security domains – at scale. By replacing inefficient air-gaped processes and simplistic Software & Diode-based systems with the hardware-based STG an organisation can support the data needs of their users and the business this provides the confidence and ability to exploit modern technologies such as Cloud and Big Data, all without compromising the security of protected networks.

Key Security Features

- Encapsulation of non-verifiable payloads for safe delivery to destination (not constrained by file size)
- Hardware Syntactic Validation of structured data (up to 2GB)
- Hardware based Digital signature verification and label checking to ensure reliability
- Full protocol break (Protocol Filtering Diode (PFD))
- Full logging and audit capabilities
- Roadmap – Hardware Semantic Validation

The STG can be configured to enforce a variety of scenarios

Low to High (Import) Only

Bidirectional (2x Independent pipelines)

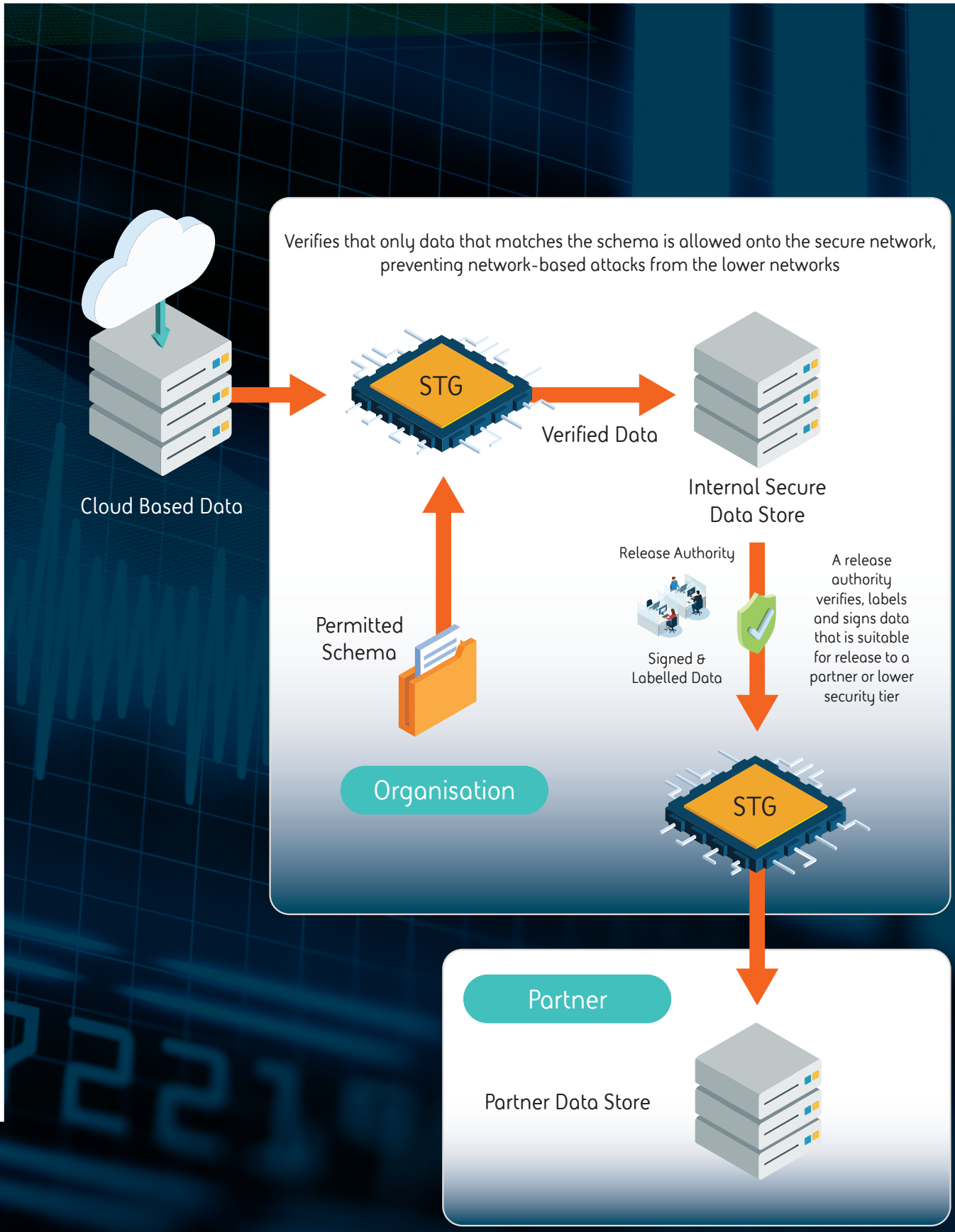
High to Low (Export) Only

Features

- Low latency
- High throughput, up to 25Gbps per Processing Blade or 100Gbps per IRIS Chassis
- Integrates with BAE Systems and third-party software tools (such as Datagate Orchestrator and Glasswall)
- Multiple segregated virtual flows on a single Processing Blade

Supported Native Interfaces:

- AMQP(S)
- TCP
- JSON
- XML


Verifies that only data that matches the schema is allowed onto the secure network, preventing network-based attacks from the lower networks
Cloud Based Data
STG
Verified Data
Internal Secure Data Store
Release Authority
Signed & Labelled Data
A release authority verifies, labels and signs data that is suitable for release to a partner or lower security tier
Permitted Schema
Organisation
STG
Partner
Partner Data Store

Transfer CDS

Secure Full Motion Video (FMV) Gateway

The Secure FMV Gateway (SFG) has been developed to allow organisations to fully exploit and share valuable FMV data internally and with partners, without compromising Operational Security or the integrity of the systems being connected together. The SFG allows an organisation to carefully control the metadata being released with video feeds in order for it to reach a wider audience, or to allow untrusted but useful feeds to be consumed by high classification systems without compromising them.

Key Security Features

- Hardware-based Metadata inspection, modification and redaction
- Hardware filtering of Video and Audio
- Full protocol break (Protocol Filtering Diode (PFD))
- Full logging and audit capabilities

Models of Operation

Import of FMV data

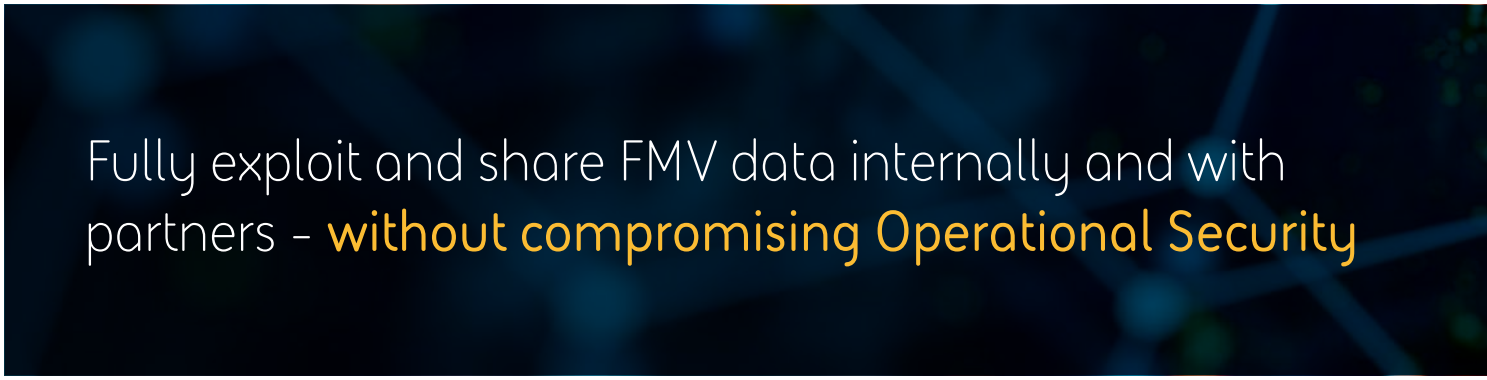
Export of FMV data

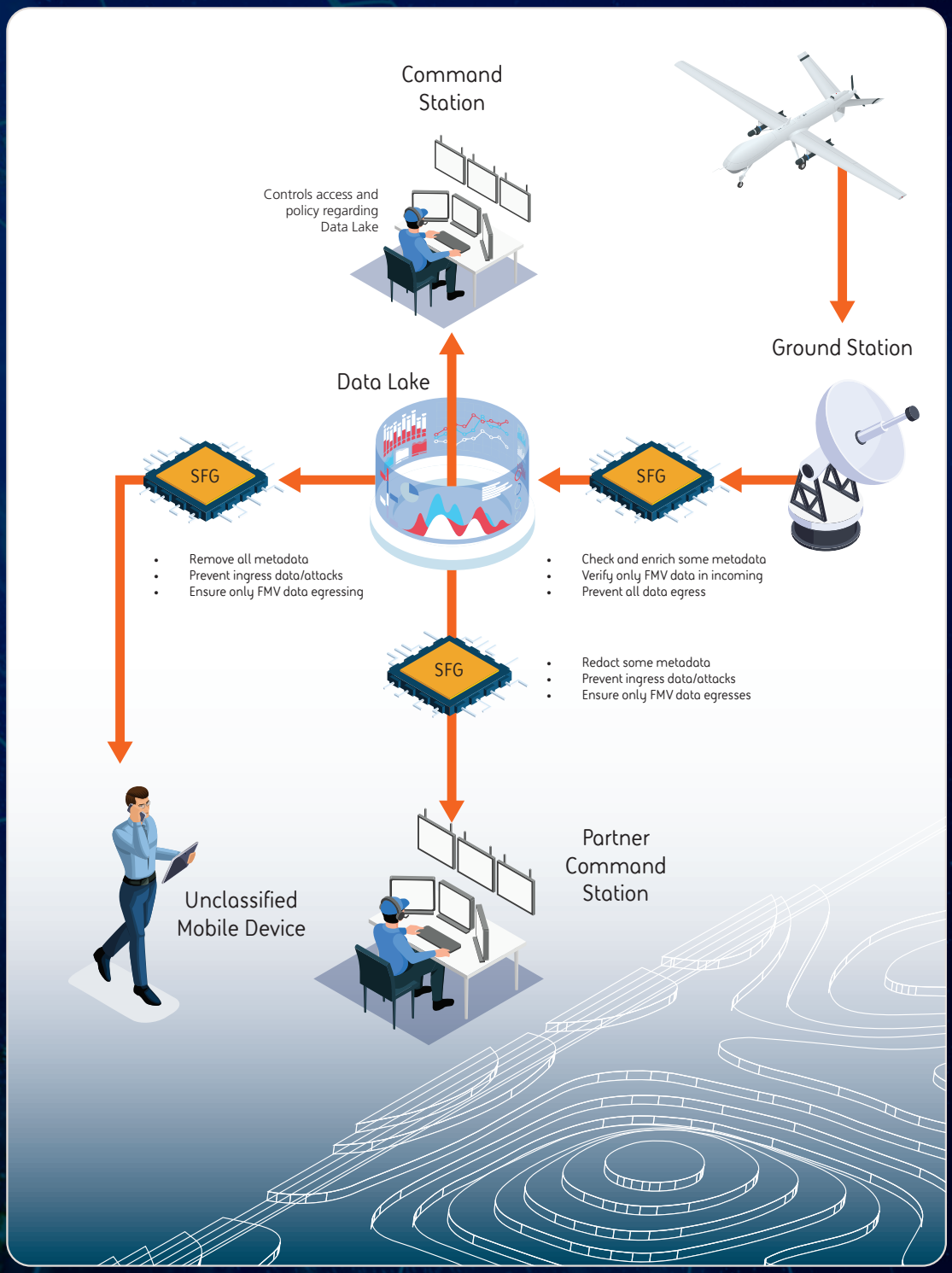
Features

- Low latency near-real time
- Can be configured to support the Import or Export of FMV data
- Integrates with BAE Systems and third-party software tools (such as SOCET GXP)
- Up to 4k (60fps) per FMV stream
- Up to 100 concurrent Full High Definition (FDH) (1080p30) streams per Chassis

Supported Protocols, Codecs and Formats

- STANAG 4609 (MPEG2 with KLV metadata)
- Metadata conforming to MISB ST 0601.15 (Uncrewed Air System)
- H.264, H.265 (roadmap)
- MPEG-2 Audio, MPEG-2 Video



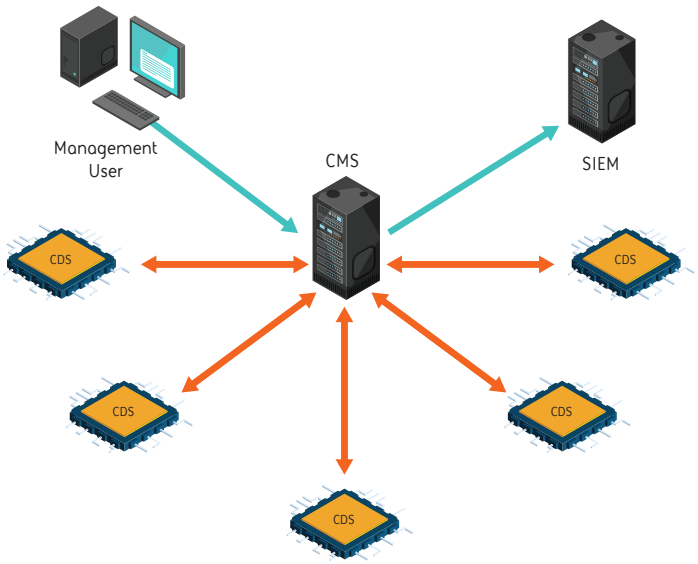

Command Station
Controls access and policy regarding Data Lake
Ground Station
Data Lake
SFG
SFG
SFG
Remove all metadata
Prevent ingress data/attacks
Ensure only FMV data egressing
Check and enrich some metadata
Verify only FMV data in incoming
Prevent all data egress
Redact some metadata
Prevent ingress data/attacks
Ensure only FMV data egresses
Unclassified Mobile Device
Partner Command Station

Central Management

All the BAE Systems CDS capability can be managed from a single fleet management tool, the CDS Management System (CMS). This unified tool can manage up to 100 CDS instances, which includes all aspects of the system, including the Hardware Gateway, the Application & COTS elements – simplifying the management overhead of CDS throughout your organisation.

Key features:

- Granular Role-Based Access Control (RBAC) and User Management integrated with organisational directory and identity systems
- Fleet management of up to 100 complete CDS systems
- Simple and intuitive Dashboard UIs
- Management of the whole CDS (Hardware, Application and COTS servers) in one place (high and low sides)
- Signed configurations and system updates
- Centralised auditing and logging capability with interfaces to customer Security Information and Event Management (SIEM) systems

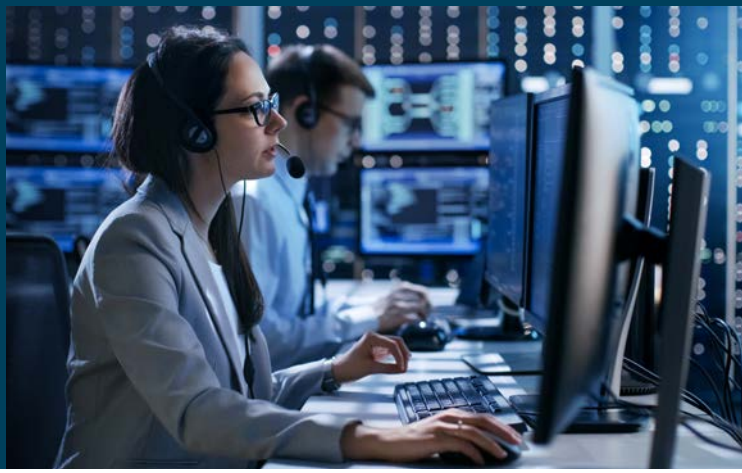


Support & Maintenance

The BAE Systems Cross Domain Support Service provides Service Desk and 3rd & 4th line hardware & software support to our Customers. The support process is an integral part of the whole lifecycle management approach undertaken by BAE Systems where we utilise the Information Technology Infrastructure Library (ITIL) v4 framework for the management of incidents, timely restoration of service and escalation.

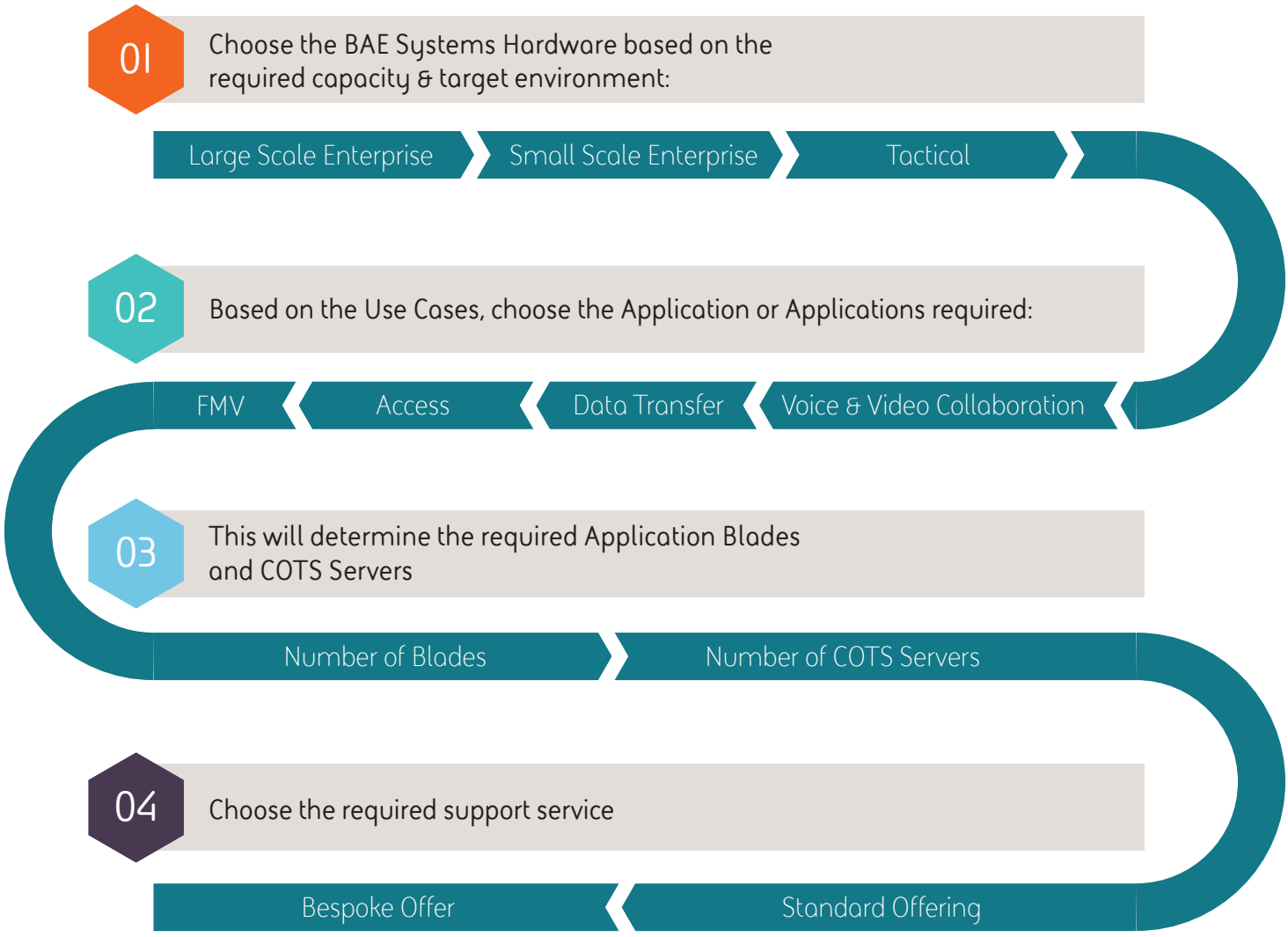
We have standard and bespoke service offering that include:

- Service Desk
- Incident & Problem Management
- On-site Support
- 24/7/365 Support
- 4th Line Product Support
- Regular Patching Cycles
- Hardware Warranty
- Service Delivery Managers



Building up a Cross Domain Solution

The BAE Systems IRIS Platform is a modular system that is flexibly built and configured to suit the Use Case(s). Use the process below to build up a CDS that is tailored to your needs:



Note: Step 3 is only applicable to "Large Scale Enterprise"

Form Factor Summary Table

	Large Scale Enterprise	Small Scale Enterprise	Tactical
Form Factor	1 Rack Unit	1 Rack Unit	Various
COTS Servers	Yes Depends on application and capacity	No Compute resources embedded on the platform	No Compute resources embedded on the platform
Physical Specification (excl. COTS Servers)	• QSFP+ modules (copper or fibre) • 4 x 10Gbps per Processing Blade • 4 Processing Blades per Chassis • 1U 19" rack-mount • 100-240V AC • < 350W • CE and FCC (part 15) compliant • 10-35 °C ambient	• 10Gbps SFP Ethernet (copper or fibre) • 1U 19" rack-mount • 100-240V AC • < 350W • CE and FCC (part 15) compliant • 10-35 °C ambient	TBC

"We have security-cleared 5-Eyes teams based in the UK, Australia and US, each with deep expertise in hardware, firmware and software development, as well as in-country manufacturing capabilities."

Application Summary Table

Please refer to the individual Application Pages for more detailed information

	Transfer			Access
	Secure Voice and Video Gateway	**Secure Transfer Gateway**	**Secure FMV Gateway**	**Secure Access Gateway**
Key Security Controls	• Hardware filtering of Video • Hardware filtering of Audio • Hardware filtering of Session Data • Full protocol break • "Human Factor" controls	• "Encapsulation" of non-verifiable payloads for safe delivery to destination • Hardware Syntactic Validation of structured data (up to 2GB) • Hardware based Digital Signature verification and label checking • Full protocol break	• Hardware-based Metadata inspection, modification and redaction • Hardware filtering of Video and Audio • Full protocol break	• Hardware filtering of Screen data • Hardware filtering of Audio data • Hardware filtering of Session data • Hardware filtering of User Inputs • Full protocol break • "Human Factor" controls
Main Supported Protocols & Standards	• SIP/SIP(S) • H.264 • G.722 • RTP/SRTP	• AMQP(S) • TCP • JSON • XML	• STANAG 4609 • MISB ST 0601.15 • H.264 • MPEG-2 Audio • MPEG-2 Video	• MS Remote Desktop Services • MS Azure Virtual Desktop • VNC • Citrix • VMWare Horizon • AWS Workspaces • SSH
Typical Capacity per Processing Blade	• Varies depending on resolution • 500+ VoIP Calls • 25 FHD Concurrent Sessions	• Varies depending on data type and security control • Up to 25 Gbps	• Varies depending on resolution & security policy • Up to 25 FHD Streams	• Varies depending on Resolution • Up to 150 sessions • 25 FHD Concurrent Sessions
Features	• Microsoft Teams • Cisco Jabber • Cisco CMS • Cisco WebEx • A wide range of hardware endpoints and Session Border Controllers	• One-way or bidirectional data flow • Integrates with BAE Systems and third-party software tools (such as Glasswall & Datagate Orchestrator) • Multiple segregated virtual flows on a single Blade • Choice of encapsulation or verification per virtual flow	• Low latency near-real time • Can be configured to support the Import or Export of FMV data • Integrates with BAE Systems and third-party software tools (such as SOCET GXP)	• Dedicared Resource Mode • Shared Resource Mode • Low latency near real time experience for users • Dual Monitor support • Supports full-screen Video and Voice • Support for 4k, Ultrawide and FHD (and below) screen resolutions

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Cybersecurity
11091 Sunset Hills Road
Reston, VA. 20190
USA
T: +1 877 277 22315

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS