FUJITSU

2024 Defence Industry Report

Uncover the trends and technologies shaping the future of defence

cisco Partner

Contents

The outlook for the UK defence and national security sector

Enabling an information advantage while reinforcing the fundamentals

In the face of global and digital disruption, defence and national security organisations are re-evaluating their strategic objectives.

Gaining and maintaining an information advantage still matters as part of a wider roadmap. However, the current situation in Ukraine and the Middle East has placed a renewed focus on the fundamental requirements of defence – delivering urgent, quick, short-term wins with cost-effective technologies, many of which have been adopted from solutions previously used for commercial activities or leisure.

On a basic level this means replacing old stock, ensuring sufficient weaponry, and funding additional troops (or resources). It also includes the need to identify and implement new technologies, such as commercially available drones, which are accurate, cost-effective and capable of streaming live video.

Organisations must fulfil these renewed objectives while tending to their requirements for best-in-class information assurance or when mapping high-security environments. They require the security of sovereign environments with the flexibility of a commercial-off-the-shelf (COTS) approach for next-generation networks. However, very few options exist to fulfil these requirements.

Defence spending in the UK

Despite being the sixth-largest global economy, the UK has the third-largest defence budget in the world.[1]

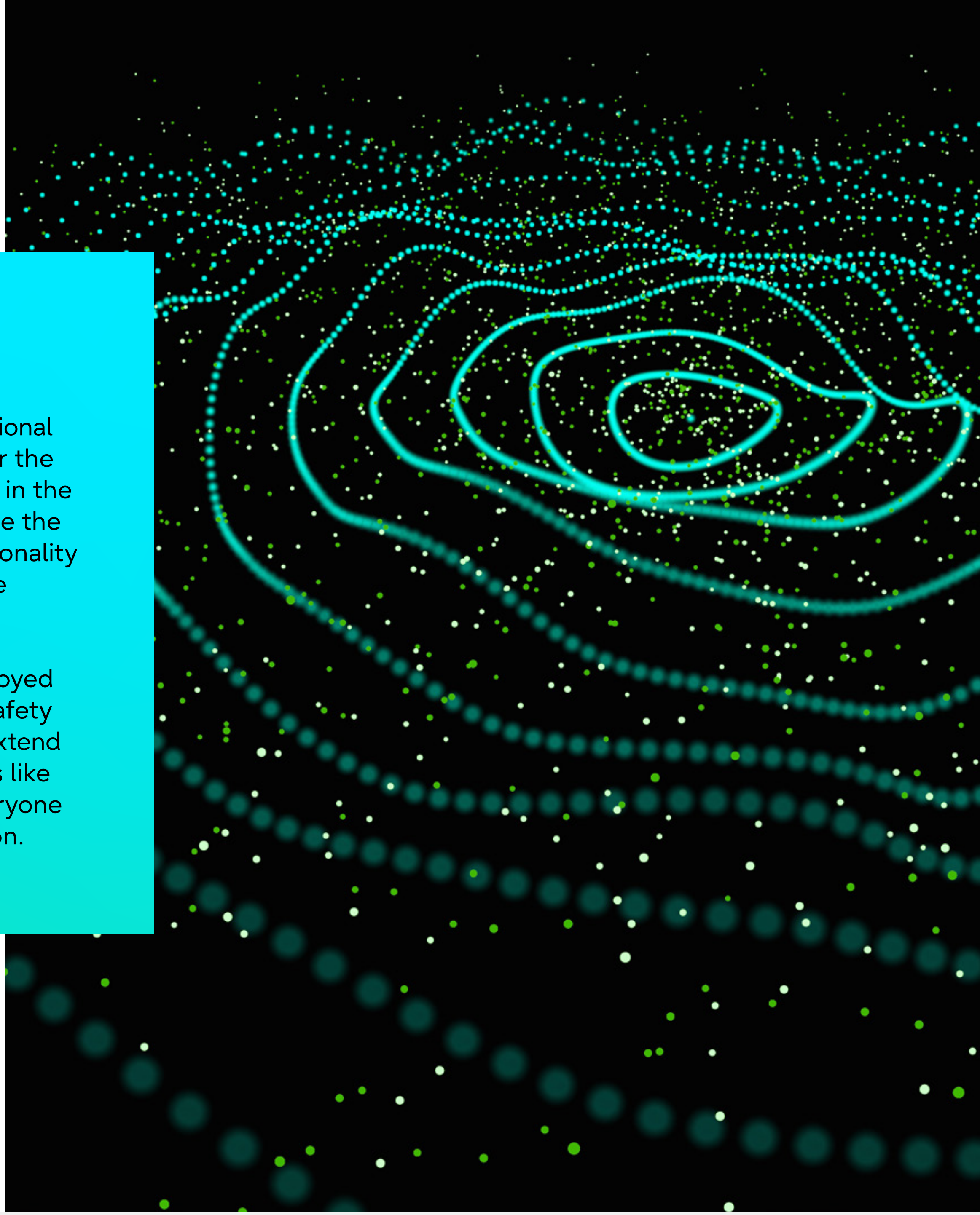
Defence spending is continuing to increase to meet the NATO 2% GDP target. In 2022, the UK was one of only nine NATO member countries to achieve the target.[2]

In February 2022, the government committed $257.2 billion (£202.9 billion) for military equipment and services from 2021 to 2031, focusing on digital, cyber, air, land and sea capabilities.[3]

2023's Spring Budget allocated a total of $13.9 billion to increase defence spending over five years. This includes $6.3 billion to 2023/24 and 2024/25 and a further $2.5 billion per year in subsequent years up to 2027/28.[2]

1 IISS Military Balance 2022
2 researchbriefings.files.parliament.uk/documents/CBP-8175/CBP-8175.pdf
3 mordorintelligence.com/industry-reports/united-kingdom-defense-market

Challenges impacting the defence sector



Strategic investments

Wars of the future are expected to be hyper-tactical and attrition-focused, with infrastructure being targeted before military targets. We're witnessing this in Ukraine, where Russia's evolving technological and strategic capabilities have highlighted gaps in the defence of Western nations. The UK is currently channelling just 1% of GDP for defence, less than the NATO commitment of 2%. Conversely, Russia has transformed its economy into a war machine, funnelling 18% of its GDP into weapons manufacturing.

Connecting the deployed space

Organisations in defence and the UK's Critical National Infrastructure (CNI) must level the playing field for the deployed space. This means ensuring personnel in the field, as well as home and embassy workers, have the same information advantage and network functionality as those operating in corporate networks or large campus environments.

However, connectivity is notoriously poor in deployed locations, which impacts the effectiveness and safety of operators and personnel. Organisations must extend network capabilities through secure frameworks like Software-Defined Perimeter (SDP) to ensure everyone has safe access to accurate, real-time information.

Challenges impacting the defence sector

Operational Technology (OT) and Internet of Things (IoT)

The number of devices being used to monitor things like performance, shipments, air conditioning, and power is skyrocketing. In the military, OT is being increasingly adopted to track a wide range of activities, such as security cameras and fence alarm systems.

However, these sensors and monitoring devices are increasing the threat surface, causing significant concern for defence organisations, especially the UK and US militaries. Organisations in the military sphere must carefully consider the connectivity and functionality of OT and IoT to ensure the most secure, future-proof deployment possible.

Digital transformation[4]

Advanced technologies like cloud, big data, Artificial Intelligence (AI) and Machine Learning (ML), digital twins, and IoT will help address operational challenges. It's expected that defence organisations will boost their agile production capabilities to counter future disruptions. UK organisations are starting to invest in digital capabilities, but only 32% of budgets are currently allocated to digitisation.[5]

The drive to achieve shorter lead times and cycle times while increasing factory efficiency may lead many defence companies to adopt "smart factory" initiatives. It's likely that the digital thread that connects engineering, supply chain, manufacturing, and aftermarket, will play a pivotal role in the future.

Supply chain resilience[4]

The UK's limited domestic production capability for complex weapons and a shrinking platform fleet has resulted in a dependency on the US for rapid resupply and logistics during a conflict. This dependency is shared by many other European NATO members and was highlighted by 2023's accelerated shift from global to regional sourcing. It led many organisations to enhance visibility into their supply chains for improved control, coordination and third-party risk management.

However, defence organisations are facing external threats to supply chains too. On average, they are impacted by three significant risk events per year, including cyberattacks, with 20% being affected by more than five.[6] As a result, we're seeing a stronger focus on risk mitigation through robust cybersecurity, cloud privacy and resilient systems and automation.

[4] deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-eri-2023-outlook-aerospace-and-defense.pdf
[5] Digital Value and The Industry Context
[6] interos.ai/wp-content/uploads/2022/05/Resilience-2022_Interos_Annual-Global-Supply-Chain-Report_5_11_2022.pdf

Challenges impacting the defence sector

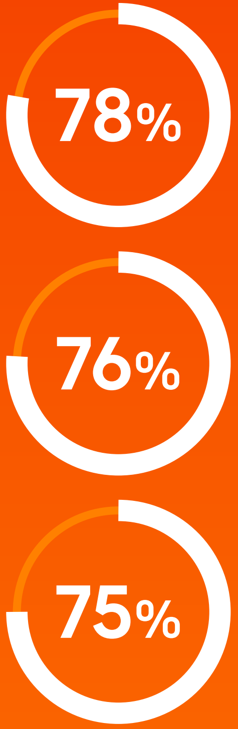
Talent retention[4]

There's an industry-wide challenge for attracting, retaining and developing top talent. These issues are being exacerbated by automation and advanced digital technologies that are reshaping the industry's workforce. All of which require new skills in aerospace engineering, mathematics, data science and digital technologies.

3,999,964 is the global cybersecurity workforce gap, with **73,439** in the UK, up +29.3%[7]

Defence organisations must foster an innovative culture and enhance digital skills to prepare a future-ready workforce. In addition, deep engagement with communities and schools through partnerships, internships, co-investments and sustained collaboration is required to shape better industry perceptions and establish talent pipelines.

Which defence organisations are facing cybersecurity skills shortages?



78% Government (non-military)[7]

76% Military/military contractor[7]

75% Aerospace[7]

[4] deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-eri-2023-outlook-aerospace-and-defense.pdf
[7] ISC2 Cybersecurity Workforce Study 2023

The evolving threat landscape

Today's threat landscape is multifaceted, which poses significant challenges for defence and national security organisations that require information assurance or those that map to high-security environments. These challenges are being magnified by the adoption of technologies that depend on connected networks and systems. In turn, this is increasing the threat surface with information networks, weapon systems and platforms all at risk.

Hostile states such as Russia, Iran and North Korea continue to pose significant risks to the global security environment. If successful, their cyberattacks have the potential to endanger lives, disrupt democracy and result in costly damage. National infrastructure and public sector organisations are responding by increasing investments in proactive mitigation measures to combat threats and ransomware tactics.[8]

In addition, phishing, credential theft, social engineering attacks and known vulnerability exploits are being used as a vector to launch cyberattacks on the UK's CNI. The UK Parliament's Science and Technology Committee has launched an inquiry into the cyber resilience of the nation's CNI. The committee is due to assess the progress towards achieving UK CNI resilience targets by 2025.[9]

$4.45 million
is the average cost for a successful attack globally, a 15% increase since 2020.[10]

34%
of organisations across the UK's CNI anticipate a rise in cybercrime as a direct result of the current economic situation.[11]

30%
of the detected Russian state and Russian-state-sponsored network intrusions were directed against governments.[12]

This evolving, unpredictable threat landscape is driving growth within the UK's cybersecurity software and IT services market, which experienced a 19.2% rise to $3.3 billion in 2023. However, not all cybersecurity professionals agree that the threat landscape is going to get worse:

79%
of cybersecurity professionals **working in military** settings think the threat landscape has reached its peak.[7]

78%
of cybersecurity professionals **working in government** think the threat landscape has reached its peak.[7]

[7] ISC2 Cybersecurity Workforce Study 2023
[8] TechMarketView Market Trends & Forecasts 2023
[9] csoonline.com/article/657273/mps-to-examine-cyber-resilience-of-uks-critical-national-infrastructure.html
[10] IBM, 2023, Cost of a Data Breach Report
[11] Cyber Security in Critical National Infrastructure Organisations: 2023 Report
[12] statista.com/statistics/1427805/russian-state-cyber-threat-most-targeted-sectors

The technologies shaping the future of the industry

Network as a Service (NaaS)

The need for secure, high-speed network connectivity has become a critical requirement for the defence industry. Thanks to its flexible, powerful, secure and cost-efficient architecture, NaaS looks to be a promising solution for network management, we can soon expect NaaS to address IoT requirements for the individual, reducing connectivity hardware to be built within the application itself or added to the communication device deployed.

As a cloud model, NaaS will allow defence organisations to operate the network without owning, building, or maintaining their infrastructure. It replaces hardware-centric VPNs, load balancers, firewall appliances, and MPLS connections, providing seamless demand-based scalability, faster services deployment and zero hardware costs.

34% of organisations' IT teams see NaaS' ability to enhance network agility as its greatest benefit.[13]

35% of organisations recognise NaaS as being crucial for deploying new technologies, such as s Wi-Fi 6, software-defined WAN (SD-WAN), secure access service edge (SASE), 5G and AI.[13]

NaaS will simplify network complexity to an on-demand level. It enables the use of both cloud and private infrastructure, converting the last mile into high-performing connectivity while securing connectivity across the entire infrastructure. In addition, NaaS will reduce the number of staff required to maintain a network, remove dependency on network providers' core network (backhaul) and reduce the level of training and skills required for greater cost efficiency.

NaaS adoption is expected to grow at a compound annual growth rate of 40.7% from 2021 through 2027.[14]

Currently, NaaS is a conceptual solution in the public sector, but it's already resonating with the Chief Technical Officer (CTO) community. Its ease of deployment and management will underpin successful bring-back-in-house network management strategies. It's expected to become a significant capability and alternative service offering over the next two years.[15]

[13] Cisco, 2022 Global Networking Trends Report
[14] cisco.com/c/dam/en/us/solutions/enterprise-networks/nb-06-2022-networking-report-cte.pdf
[15] Strategy Paper Introduction to Fujitsu's Network as a Service Offering

The technologies shaping the future of the industry

Secure Access Service Edge (SASE), Open-RAN 5G, and edge computing

Defence organisations often operate in challenging environments that have little or no infrastructure in place, but their networking requirements remain complex at the edge.

Even with these challenges, the number of smart devices is increasing – placing further pressure on networks to perform efficiently and securely. SASE is seen as a solution to address these challenges by providing secure and fast network connectivity, regardless of the user's location or the type of device they're using.

79.4 zettabytes* of data will be generated by IoT connections in 2024.[16]

13.6 zettabytes in 2019 – a rising trend that will be felt in the defence sector too.[16]

Investments in edge computing and IoT are set to increase, driving new possibilities with real-time decision-making, seamless data exchange and on-demand communication and collaboration. SASE's integrated networking and security services can support these investments by ensuring secure and reliable connectivity between IoT devices and edge computing resources.

80% of enterprises will have adopted a strategy to unify web, cloud services and private application access using a SASE or Secure Service Edge (SSE) architecture by 2025... Adoption was at **20%** in 2021.[17]

Edge computing improves security and resilience by incorporating security features into frontline devices in tandem with established security standards. This is crucial in the defence industry, where information assurance and intelligence-led decision-making determine operational success.

***Zettabyte** *noun*
A unit of information equal to one sextillion bytes.

[16] statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size
[17] 2022 Strategic Roadmap for SASE Convergence

The technologies shaping the future of the industry

75% of all enterprise-generated data will be created and processed outside a traditional centralised data centre or cloud by 2025.[18]

Open-RAN 5G is expected to drive previously impossible levels of connectivity to campus areas that are hard to reach with traditional infrastructure. The technology has the performance needed to support many more OT and IoT devices while creating a secure network environment. When paired with edge computing, Open-RAN 5G enables OT and IoT to operate more efficiently and with less human intervention.

SASE can support this by providing secure, reliable network connections that can handle the high data volumes generated by these technologies. It's a significant step forward that will enable defence organisations to reach new levels of agility, flexibility, security and innovation from wherever they operate in the world.

[18] What Edge Computing Means For Infrastructure And Operations Leaders

Artificial intelligence and machine learning

For IT operations (AIOps)

Today's IT landscape is increasingly diverse, dynamic and difficult to monitor. Defence organisation networks are under constant threat from malicious traffic such as ransomware, inside threats and lateral movements.

It can be extremely challenging to detect threats without impacting performance or security when operating within an encrypted network. These challenges are not helped by expectations that application performance and availability receive no interruptions.

The adoption of AIOps is rising globally and in the defence sector, with the market estimated to triple in size.

$11.7 billion in 2023 to **$32.4 billion** by 2030.[19]

By pairing AI and ML with a secure software-defined networking (SDN) toolset, AIOps can rapidly identify, address and resolve slow-downs and outages in comparison to manually sifting through alerts from multiple IT operations tools. **The US Air Force has used AI-driven analysis to achieve a 40% reduction in unscheduled maintenance across its monitored systems.**[20]

What's possible with AI and ML?

- Faster mean time to resolution (MTTR).
- Lower operational costs through automatic issue identification and liberated employee time.
- Improved visibility, transparency and collaboration for faster, more accurate decision-making and response times.
- Predictive management and analytics to identify and address issues before they cause more serious problems.

[19] marketsandmarkets.com/Market-Reports/aiops-platform-market-251128836.html
[20] On the warpath: AI's role in the defence industry – BBC News

Artificial intelligence and machine learning

For big data and analytics

Data is a mission-critical strategic asset, providing decision-makers with real-time operational intelligence that can save lives. However, defence organisations are facing ever-increasing volumes of data that are impossible to analyse using manual processes.

64.2 zettabytes of data were created, captured, copied and consumed in 2020 globally, but this is expected to rise to...

180 zettabytes in 2025.[21]

The number of sensors for telemetry is also rising considerably and increasing to already huge volumes of data. For example, drones and other surveillance and reconnaissance technologies generate huge amounts of data, such as videos, text files and satellite imagery. The issue is exacerbated when dealing with heavily structured datasets, as non-conforming unstructured data can be omitted, which dilutes the value of the intelligence.

In addition, traditional pattern matching and probabilistic approaches are prone to generating false correlations and hallucinations.

The global military and defence sensor market size is projected to reach $14.4 billion by 2031, up from $8.3 billion in 2021.[22]

Unstructured data represents between 80 and 90% of all new enterprise data, and it's growing three times faster than structured data.[23] **Machine learning can analyse both structured and unstructured data, producing connected, comprehensible and accurate relationships between the two.**

The benefits are enhanced with natural language and structured searches, allowing analysts to explore insights and build an evidential chain faster. Outputs in natural language text aid in report production, allowing defence and intelligence analysts to spend more time on investigation rather than data entry.

[21] Data growth worldwide 2010–2025 | Statista
[22] Military and Defense Sensor Market Size, Share, Trend, Analysis
[23] gartner.com/en/documents/4006789

Moving forward with Fujitsu and Cisco

At Fujitsu, we focus on bringing the best complementary technologies together and enhancing them with our innovations. We achieve it with our innovative COTS approach, ensuring organisations that require high information assurance get the flexible, tailored approach needed for their unique networking environments.

Secure software-defined network (SDN)

The defence industry is facing an ever-increasing pool of data, incoming threats and global disruption. Overcoming these challenges requires the effective integration of new technologies with existing systems and information.

SDN provides the foundation for the mission-critical technologies of today while acting as a reliable, future-ready platform for tomorrow. It enables the industry to meet the demands of the digital age, ensuring secure, high-speed connectivity and the effective integration of new technologies while remaining cost-efficient. That's why the shift to SDN for defence and national security organisations is more than just a trend, it's now a necessity.

With SDN, the defence industry can benefit from an integrated, resilient, and secure network that extends end-to-end across the organisation. This not only enhances the industry's ability to handle large volumes of data but also improves the overall efficiency and security of its operations.

Cisco-based SD-WAN

Fujitsu's Software-Defined Networking (SDN) platform pairs a best-in-class, customised version of Cisco's (Viptela) SD-WAN software with central orchestration and management tools hosted in Fujitsu's industry-leading sovereign environments in UK List-X data centres.

This is complemented by Fujitsu's wider SDN Portfolio of hosted services, SaaS, or cloud services, supporting network infrastructure and associated services. As an assured Next Generation Network (NGN) service, Fujitsu's SDN will optimise existing network capacity, enabling application-based routing and securing data flows across any available untrusted bearer.

Moving forward with Fujitsu and Cisco

Sovereign security

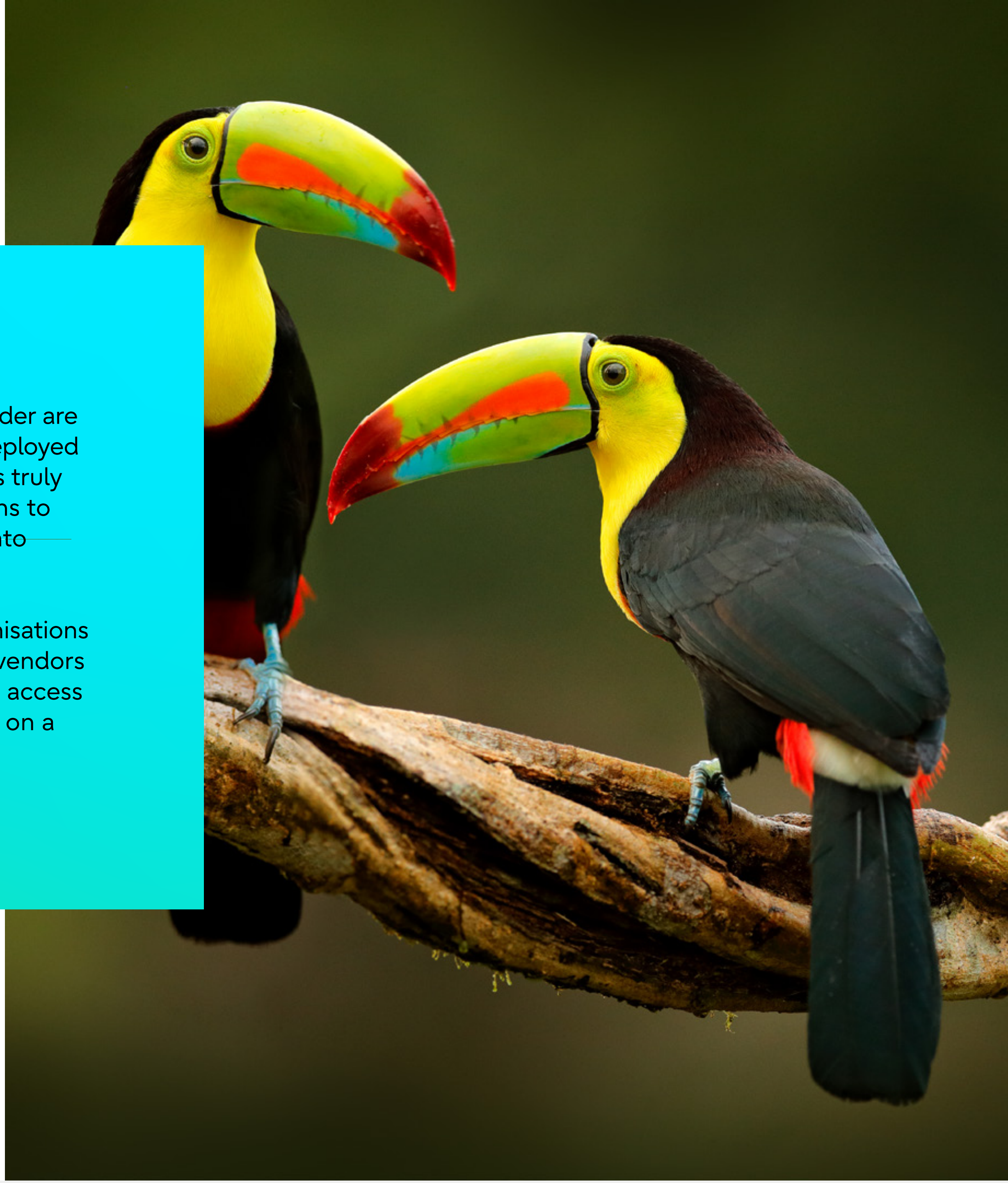
Fujitsu's SDN platform is secure by design, operating inside an air-gapped, UK-based sovereign environment, with protective monitoring aligned to Mitre Attack and MEF SDN standards. The platform offers a fast, secure and affordable route to networking with defence-grade agility and seamless scalability – spinning up connectivity in minutes, not weeks or months.

It's been developed with the sovereign organisation in mind while also offering the flexibility to operate within a cloud environment. This kind of UK-based sovereign capability is uncommon and remains crucial for organisations with complex information assurance requirements for sensitive data.

Advanced SASE

Fujitsu's technical capabilities as a SASE provider are highly advanced, ensuring that equipment deployed on-site can activate any existing licences. It's truly flexible, with Fujitsu supporting organisations to import existing Cisco licensing or export onto another cloud service provider if preferred.

Fujitsu's multi-vendor approach allows organisations to activate and deactivate services or swap vendors whenever required, offering straightforward access to best-of-breed services and technologies on a catalogue basis.



To learn more about Fujitsu's Cisco-powered SDN solution, explore our guide or contact a member of our team.

Access guide on our website

Partner