CASE STUDY

Leading UK Telco Selects A10 Networks for TSA Compliance and DDoS Protection

Industry | Telecom

UK telcos need to quickly detect and respond to security breaches and vulnerabilities, rapidly recover from security incidents, and maintain visibility and control over potentially compromised systems.

A leading telecommunications provider, who needed to take a proactive approach towards network security to address TSA compliance, chose A10 Networks' high performance, end-to-end A10 Defend™ DDoS solution – delivering scalable, precise, and automated defence against increasingly sophisticated and frequent DDoS attacks.

> *Before choosing A10 Networks, we spoke to several mobile and telecom integrators for recommendations, who put A10 and its DDoS protection solution forward. This is where A10's credentials and experience of working with 90% of the global mobile network operators, made it a credible, competitive, and compelling proposition."*
>
> **– Head of TSA Compliance at leading telecommunications provider**

NETWORK SOLUTION

A10 Defend

CRITICAL ISSUES

- Addressing TSA compliance by enhancing threat detection and response capabilities
- Increasing network uptime
- Delivery of a superior customer experience for millions of mobile users

RESULTS

- Proactively addressed TSA compliance requirements
- Substantial increase in overall network protection and incident response capabilities
- Significant reduction in downtime and increased operational continuity

Proactive TSA Compliance as a Force Multiplier in Telecommunications

With the UK telecommunications market serving approximately 69 million residents and thousands of businesses, the Telecommunications Security Act (TSA) was introduced to strengthen the security and resilience of public telecom networks across the UK. This has never been more important; cyber threats and risks are growing in scale and sophistication, with infrastructure now needing to be not only robust, but agile enough to withstand and recover from attacks.

The enforcement of the TSA has required telecom providers to fundamentally rethink how they increase network resilience and operate in an increasingly volatile digital landscape.

As a result, the TSA Code of Practice (CoP) Requirement 1.11 mandates that telcos must adopt an "assumed breach" or "assumed compromise" mindset. To address this requirement, providers are looking for solutions that will help them:

- Minimise the blast radius of a cyber attack
- Detect and respond quickly to hostile intrusions
- Segment networks to contain threats and assaults that have arisen
- Develop mechanisms to help recover quickly from security incidents
- Maintain visibility and control over potentially compromised network systems

Putting Customer Experiences First

Driven by the risks of regulatory penalties, brand damage, and customer loss, the internal compliance team at a leading UK telecommunications provider needed to prioritise a proactive approach towards TSA compliance, believing that compliance would serve as a competitive advantage in the market.

As the provider deems that value for money, network reliability, connection speed, and improved service quality are key customer retention and loyalty drivers, it needed a scalable solution that could safeguard its multi-billion-pound investment in its advanced, hyper-fast 5G networks and overall infrastructure.

A Government-savvy Partner Rethinking Resilience and Network Protection for TSA Compliance

The provider needed a strong solution that could provide robust DDoS defence and mitigation. This would offer proactive and comprehensive protection for the underlaying infrastructure of its mobile network – something it was missing with its previous provider.

> *"Before choosing A10 Networks, we spoke to several mobile and telecom integrators for recommendations, who put A10 and its DDoS protection solution forward. This is where A10's credentials and experience of working with 90% of the global mobile network operators, made it a credible, competitive, and compelling proposition."*

Enhancing Proactive Threat Detection and Mitigation

The provider selected the A10 Defend high-performance DDoS detection and mitigation solution, helping it to achieve proactive TSA compliance. For a similar level of investment as the provider's previous vendor, A10 could provide scalable, precise, and automated DDoS defence. This enabled the provider to efficiently and proactively identify, mitigate, and prevent DDoS attacks before they impact critical systems or disrupt service availability.

The provider also deployed the management and analytics platform within A10 Control, increasing network intelligence to help mitigate the possibility and impact of future attacks.

Achieving TSA Compliance with Intelligent, Automated DDoS Protection

Proactive Cyber Threat Management

A10 Defend has played a critical role in enabling the provider to adopt a proactive approach to cyber threat management, facilitating compliance with TSA Security Directives Sections 105A and 105B. These require telcos to implement access controls, monitoring, and security measures to protect critical infrastructure, providing resilience, and safeguard sensitive data.

A10 Defend has significantly enhanced the provider's ability to detect and respond to emerging cyber threats in real time. It allowed the provider to analyse network traffic, patterns, and behaviours in granular detail, whilst real-time alerts quickly notify response teams at the first signs of an attack. This supported the provider's efforts to meet the TSA's requirement for real-time anomaly detection and alerting.

The provider can now triage and respond to potential security incidents in under 60 seconds. This rapid response capability means that any detected threats are swiftly contained, minimising the risk of network downtime or data compromise and facilitating compliance with the TSA's mandates on advanced and adaptive threat detection.

Fast and Effective Incident Response

A10's solutions have enabled the provider to generate clear, actionable insights for both rapid response and thorough post-incident analysis, enabling it to align with CoP (Section 5) and Regulation 6 requirements under the TSA.

A10 has also given the provider's security operations center (SOC) visibility into all security incidents. This enables the provider to create and maintain detailed audit trails, demonstrate enhanced situational awareness, and enables documentation required to demonstrate TSA compliance. Together, these capabilities allow the provider to detect threats faster, respond more effectively, and conduct thorough post-incident reviews.

Resilience and Continuity

A10's solutions have reinforced the provider's network security and ability to deliver uninterrupted service in line with CoP Sections 2 and 8. These sections focus on the provision of robust network and system security through controlled segregation, redundancy, and resilience measures to maintain continuous, reliable operations.

A10's automated failover capabilities allow providers to seamlessly redirect traffic should a network failure occur, maintaining service continuity and minimising downtime. It also creates clear separation between operational zones and other network areas. This approach is aimed at the prevention of lateral threat movement and protection of critical systems. Together, these measures enable a secure, resilient, and compliant network environment, enhancing TSA compliance.

Maintaining Operational Security

Under TSA, CoP Sections 11 and 13 mandate that telco providers maintain software integrity, secure updates, and have effective vulnerability management to protect network systems from compromise and maintain operational security.

A10 has assisted the provider in addressing TSA compliance considerations by sharing its engineering, testing, and security practices. This support gives the provider confidence that A10 solutions align with TSA expectations for software integrity, secure updates, and vulnerability management.

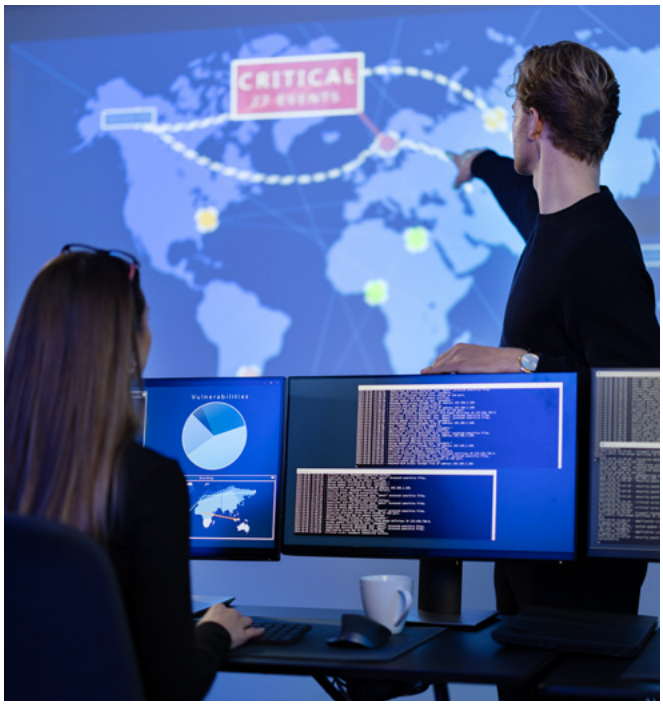
> *"A10's DDoS solution has successfully detected sophisticated low-and-slow attacks targeting our environment – which the previous solution had overlooked entirely. The comprehensive logging offered by A10's solution has simplified our compliance audits, with its pre-production environment allowing us to test optimisations entirely risk-free."*

Streamlining Processes and a Better Way of Working

Previously, the provider managed compliance in silos, with mobile, core, security, and infrastructure teams working independently and having minimal interaction with the TSA compliance team. This fragmented approach led to oversight gaps and inefficiencies.

A10 Networks helped streamline project management and foster collaboration across these groups, breaking down silos and uniting technical and compliance teams under a single, coordinated approach to facilite TSA compliance.

> *"A10's behavioural recognition solution has drastically reduced false positives – and alert fatigue for our SOC team – ultimately resulting in fewer disruptions to legitimate network users. Attacks identified as routine are now fully automated, freeing up our analysts for increasingly strategic tasks."*



The 2025 Global DDoS Weapons Report

DDoS Attacks - Evolving Game of Threat Actors

Read Report

Request a live demo and experience the

A10 Networks Difference

Schedule a Demo

About A10 Networks

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must ensure business-critical applications and networks are secure, available, and efficient. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10Networks.com and follow us @A10Networks.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-CS-80256-EN-01 December 2025