SOLUTION BRIEF

TSA Compliance and Network Resilience for UK Telcos

Rethinking Network Infrastructure in the Face of New Compliance Demands

Overview

In the current hyperconnected landscape, the UK's telecommunications sector faces a pivotal shift driven by the Telecommunications Security Act (TSA), enforced in October 2022. With millions relying on uninterrupted connectivity, TSA is more than regulation, it's a strategic response to rising cyber threats, geopolitical instability, and digital complexity.

Traditional security models are no longer sufficient and the TSA's "assume breach" mandate demands resilience at the core of telecom operations. Providers must adopt integrated, agile security strategies that encompass network architecture, supply chain integrity, and real-time threat mitigation, making technologies like those from A10 Networks essential for compliance, infrastructure protection, and public trust.

Challenge – Meeting Strict Regulatory Requirements

UK telecom providers face mounting pressure to comply with the Telecommunications Security Act (TSA), enforced beginning October 1, 2022. The regulation introduced:

- New security mandates and oversight powers for Ofcom
- A requirement to 'assume breach' and act as if systems are compromised
- The need to remove high-risk vendor equipment, including legacy infrastructure (e.g., Huawei), causing operational complexity and cost escalation

Challenge

UK telecom providers must urgently comply with the TSA, requiring removal of high-risk vendor equipment and adoption of holistic, breach-assumed security strategies across legacy infrastructure.

Solution

A10 Networks provides TSA-aligned security solutions that enhance visibility and threat response, and support resilient, compliant network architecture for national telecom providers.

Benefits

- Real-time DDoS, encrypted traffic, API and web application protection
- Centralised control across hybrid environments
- Compliance-ready with certified security standards
- Future-proofed infrastructure with IPv6 and zero-trust support

Service providers struggle with:

- Fragmented security tools and siloed infrastructure
- Limited visibility across hybrid environments
- Inadequate threat detection and response capabilities
- Compliance burdens tied to the TSA Code of Practice (CoP)

Enabling Compliant, Resilient, and Future-ready Networks

A10 Networks enables UK service providers to meet the stringent requirements of the UK TSA and the Telecoms Security Code of Practice (CoP) through advanced, automated, and secure networking solutions. Its carrier-grade security solution delivers high-performance DDoS protection, encrypted traffic inspection, and intelligent traffic management. These are core components required under the TSA to safeguard national infrastructure.

With A10's deep visibility, analytics, logging, and policy enforcement, providers can detect and mitigate threats in real time, ensure resilience, and maintain compliance with minimal operational overhead.

A10's solutions also support secure software supply chains and offer zero-trust architecture principles, helping providers align with the code's guidance on vendor risk and network segmentation. Trusted globally, A10 helps UK operators not only stay compliant but build more secure, future-ready networks.

Security Compliance Support

A10's solutions such as converged firewalls, DDoS protection, and traffic management help providers secure their networks by:

- Detecting threats via analytics and intrusion detection
- Mitigating risks with filtering, load balancing, and threat protection
- Enhancing incident response through logging and SIEM integration
- Providing API and web application protection via ThreatX by A10 Networks

This proactive cyber threat management ensures compliance with TSA Sections 105A and 105B.

Responding to Security Compromise

A10's solutions help providers comply with TSA (Sections 2, 105C–105D) by mitigating threats such as DDoS and zero-day exploits through rate-limiting, geo-blocking, and session termination. ThreatX adds advanced protection for APIs and web applications, using behavioural analytics and adaptive profiling to detect and neutralise sophisticated attacks targeting digital interfaces.

In line with the CoP (Section 5) and Regulation 6, A10 enables deep traffic visibility via SSL inspection, anomaly detection, and real-time alerting. Integrated with SIEM and SOAR platforms, these solutions generate actionable insights for rapid response and post-incident analysis.

Network Oversight and Architecture

A10 helps providers meet CoP Sections 2 and 8 by securing network architecture and ensuring service continuity. Solutions enable zone segregation to limit incident impact, enforce strong management plane controls with MFA and encryption, and protect oversight functions like load balancing and traffic steering.

To maintain availability, A10 solutions provide automated failover, redundancy, and smart load distribution, ensuring resilience even during disruptions.

> “*The TSA is a turning point for UK telecom providers. By meeting regulations, they can build secure and trusted networks. We offer the tools and expertise to help providers make compliance a competitive advantage.*”
>
> **— Sean Pike, CISO, A10 Networks**

Supply Chain and Third-party Control

A10 adheres to best practices in software integrity, secure updates, and vulnerability management. For providers needing to comply with CoP Sections 11 and 13, A10 provides signed firmware, regular patches, hardening guides, and a UK TSA Compliance Analysis document. Its security advisories and testing protocols help operators meet Regulations 7 to 9, ensuring equipment integrity, resilience, and operational readiness.

Protection of Data and Functions

A10's security capabilities help protect data and critical functions in networks by ensuring encrypted traffic inspection, secure communications, and robust access control. Capabilities also enable role-based access, secure administration, and user activity logging, while integrating with identity management and MFA systems as required by compliance standards.

By adopting A10's solutions, providers can:

- Comply with proactive security architecture
- Reduce operational risk and faster recovery from breaches
- Enhance visibility and real-time threat mitigation
- Future-proof infrastructure with support for IPv6
- Competitively differentiate through demonstrable resilience and trustworthiness

Summary

A10 Networks enables providers to meet TSA requirements by delivering robust, multi-layered security solutions that strengthen network resilience and operational integrity. Through high-performance DDoS protection, advanced traffic inspection, and scalable web and converged firewalls, A10 safeguards critical services from evolving threats. Its hardware-based defences ensure predictable performance and compliance with TSA's resilience standards, helping providers avoid service disruption, reputational damage, and financial loss.

Next Steps

To learn more, visit A10Networks.com/TSA or book a TSA briefing with a member of our specialist team.

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 provide business-critical applications and networks that 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-SB-19214-EN-01 October 2025