eBook

Stronger Networks, Safer Services:

Building TSA-ready Telecom Infrastructure

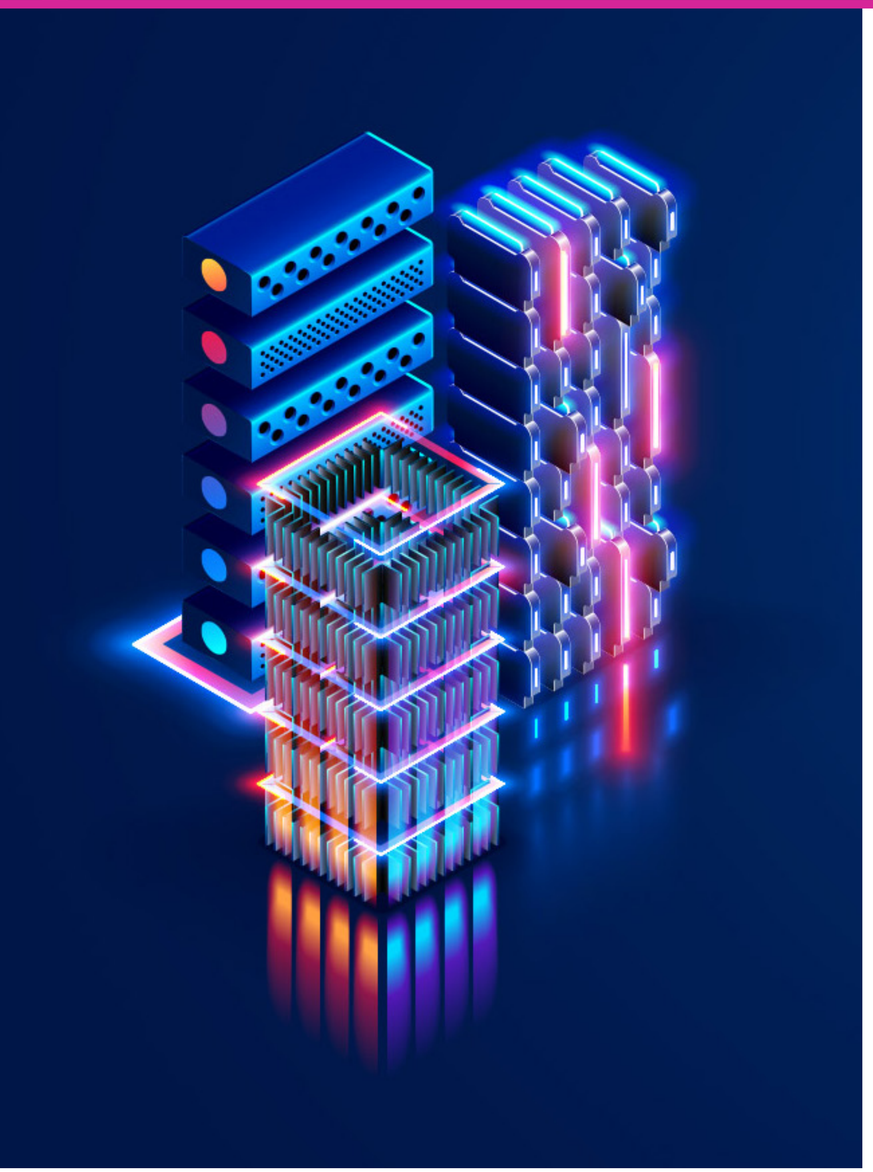


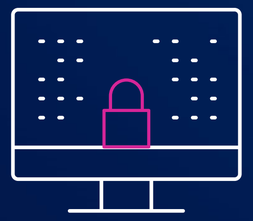
TABLE OF CONTENTS

Introduction

The Telecommunications Security Act (TSA), in force since October 2022, marks a turning point for UK telecom providers.

More than a compliance measure, it demands a strategic overhaul of network security, resilience, and operations. With Ofcom oversight and strict technical standards, providers must adopt zero-trust principles, remove high-risk vendor equipment, and modernise legacy infrastructure. With 69 million UK residents and thousands of businesses depending on secure networks, the stakes are high.

This eBook explores the TSA's requirements and operational impact. It outlines how providers can shift from reactive compliance to proactive resilience with the help of A10 Networks.



With 69 million UK residents and thousands of businesses depending on secure networks, the stakes are high.

Under Siege: How AI-driven Attacks are Reshaping Telecom Defences

For telecom providers, their networks are their business. Ensuring capacity, resilience, security, and public trust is essential.

Yet access is complex, spanning internal systems, websites, retail environments, and operational support networks. A **compromised DNS system**, due to overload or attack, may result in a slow or unreliable network for users or potentially cause website downtime. A case in point is the recent AWS outage which occurred as a result of a technical update error to the DynamoDB API, which unintentionally disrupted DNS configuration and led to service interruptions on platforms including Snapchat, Reddit, Venmo, Roblox, and several major airlines.

Subscribers judge networks by:

Reliability: Is the service consistently available, even under attack?

Speed: How quickly does the network respond?

Safety: Are users protected from redirection to malicious sites?

To meet expectations and drive growth, telecom providers increasingly use AI to automate processes and improve efficiency, often via APIs. But this also expands the attack surface. Cybercriminals now use AI to automate reconnaissance, steal credentials, and exploit API flaws. These attacks mimic legitimate behaviour, making them harder to detect.

AI has also supercharged **Distributed Denial of Service (DDoS) attacks**, which caused 53% more downtime in 2025 than previous years. As the most common form of cyberattack, frequently topping the Verizon Data Breach Report, DDoS attacks are increasingly becoming more complex and harder to detect.

Attackers now combine DDoS attacks with ransomware and other threat vectors, shifting between network and application layers to bypass defences. As a result, telecom providers must invest in robust, scalable infrastructure to stay resilient and secure networks against increasingly sophisticated, AI-driven threats.

A10 addresses telecom providers' challenges by creating solutions that boost resilience and support sustainable growth, while also aligning with TSA requirements.

Telecom providers must invest in robust, scalable infrastructure to stay resilient and secure against increasingly sophisticated, AI-driven threats.

TSA: Raising the Standard for Telecom Security and Resilience

The TSA is pivotal in reshaping the UK telecom industry's approach to network security and resilience. It's not just another compliance requirement; it signals a strategic transformation in how providers must defend their infrastructure against the evolving threats outlined above.

In a hyper-connected world, telecom networks are critical national infrastructure. They underpin everything from emergency services to financial transactions and public communications. The TSA recognises this and mandates that providers take proactive and robust measures to secure their networks against both current and emerging risks. This includes cyberattacks, supply chain vulnerabilities, and systemic failures.

For telecom providers, this means rethinking security from the ground up. The TSA requires them to assess and mitigate risks across their entire ecosystem: hardware, software, third-party suppliers, and operational processes. It enforces stricter controls on access management, data integrity, and incident response, compelling providers to build resilience into the very fabric of their networks.

The TSA mandates that providers take proactive and robust measures to secure their networks.

Providers must also adopt integrated, agile security strategies that encompass network architecture, supply chain integrity, and real-time threat mitigation. This makes solutions – such as those offered by A10 Networks – essential for compliance, infrastructure protection, and safeguarding public trust.

This is especially vital as threats grow more sophisticated. AI-driven cyberattacks, API exploitation, and hybrid DDoS campaigns are becoming more frequent and damaging. The TSA pushes providers to stay ahead of these risks by adopting modern security practices, investing in threat intelligence, and ensuring continuous monitoring and rapid response capabilities.

Ultimately, consumers expect networks to be fast, reliable, and secure. Any breach or disruption, whether due to poor DNS performance or a targeted attack, can erode confidence and cause widespread impact. By enforcing high security standards, compliance with the TSA helps ensure that telecom providers remain resilient, responsive, and trusted in an increasingly volatile digital landscape.

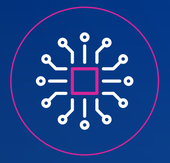
Providers may face fines of up to 10% of turnover, or £100,000 per day for continuing failure

TSA: Key Provisions and Why This is Important

The TSA introduced new security mandates and oversight powers for Ofcom which now has the authority to issue fines to telecom providers that fail to comply with the security duties outlined in the Act. This means that providers must demonstrate they have:

Secure and resilient networks

The ability to log and report



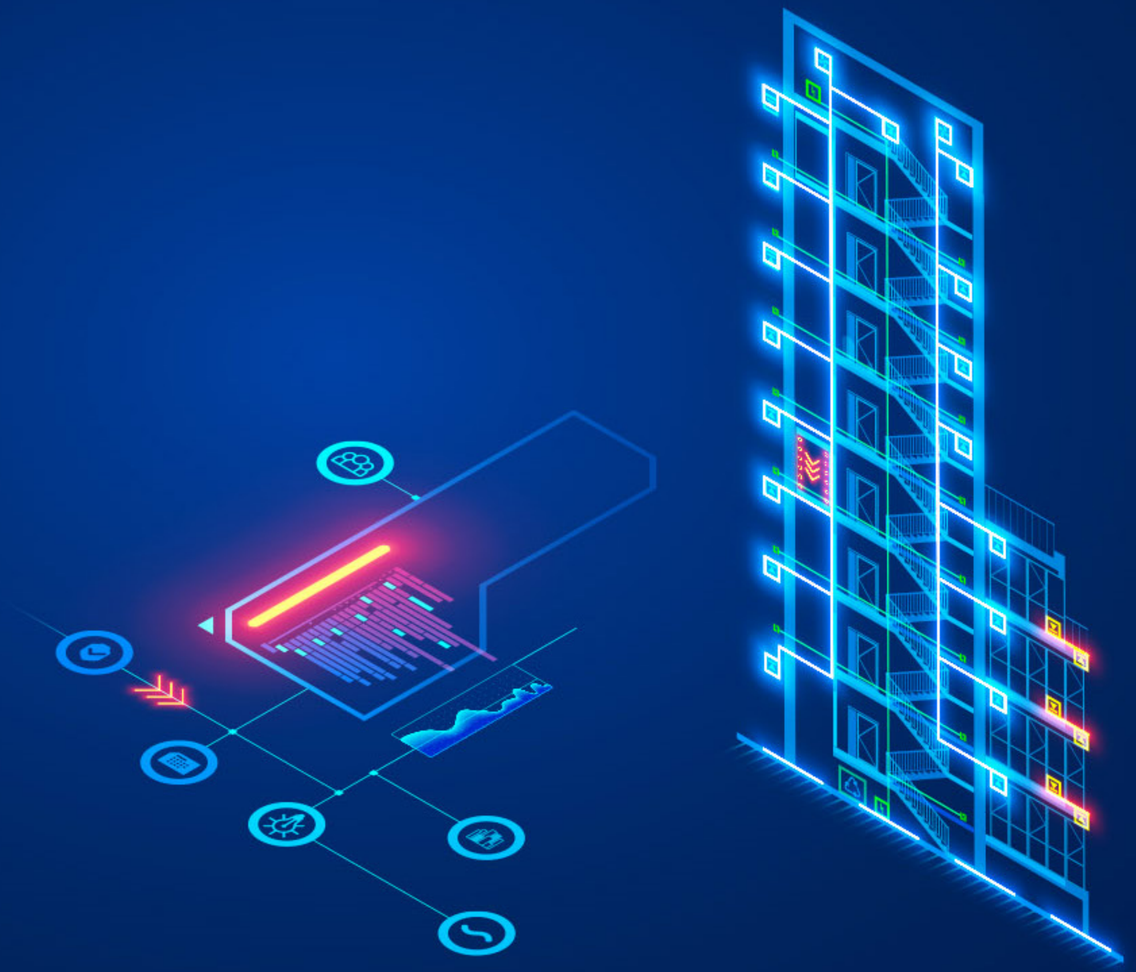
A requirement to ‘assume breach’ and act as if systems are compromised

Removed high-risk vendor equipment, including legacy infrastructure

Meet compliance requirements tied to the TSA Code of Practice (CoP)

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

How A10 Networks is helping Telcos meet TSA requirements



Outlined below are the CoP requirements and how A10 Networks can help telecom providers comply:

Duty to Undertake Stringent Security Measures

TSA Requirement	How Can A10 Networks Help?
Providers must undertake proactive cyber threat management to ensure compliance with TSA Sections 105A and 105B.	A10 solutions such as convergent firewalls, DDoS protection, and traffic management help providers secure their networks and: **Identify** risks of security compromise (e.g., intrusion detection, analytics). **Reduce** risks via inline traffic filtering, load balancing, and threat protection. **Prepare** for incidents with logging, event correlation, and integration with SIEMs.

Responding to Security Compromise

TSA Requirement	How Can A10 Networks Help?
Providers must mitigate threats such as DDoS and zero-day exploits to comply with TSA Sections 105C and 105D.	A10 solutions enable rate-limiting, geo-blocking, and session termination. 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. Additionally, A10's entity-based web app and API protection delivers real-time visibility and defence against evolving threats. This directly supports the TSA Code of Practice requirements for securing critical network interfaces and implementing "assumed compromise" principles across the expanding API attack surface.

Network Oversight and Architecture

TSA Requirement	How Can A10 Networks Help?
Providers must meet CoP Sections 2 and 8 by securing network architecture and ensuring service continuity.	A10 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 provides automated failover, redundancy, and smart load distribution, to help ensure resilience even during disruptions.

Supply Chain and Third-party Control

TSA Requirement	How Can A10 Networks Help?
Providers need to comply with CoP Sections 11 and 13 which demonstrate software integrity, secure updates and vulnerability management.	A10 solutions provide signed firmware, regular patches, hardening guides, and a UK TSA Compliance Analysis document. A10's security advisories and testing protocols help operators meet Regulations 7 to 9, ensuring equipment integrity, resilience, and operational readiness.

Protection of Data and Functions

TSA Requirement	How Can A10 Networks Help?
Providers must demonstrate that they are protecting data and critical functions in their network.	A10 solutions provide encrypted traffic inspection, secure communications, and robust access control. They also enable role-based access, secure administration, and user activity logging, while integrating with identity management and MFA systems as required by compliance standards.

Turning Compliance into Competitive Advantage for Telecom Providers

A10 Networks provides powerful, carrier-grade solutions that enable telecom providers to not only meet but exceed TSA requirements. By transforming compliance into a strategic force multiplier, A10 helps providers build resilient, secure, safe and future-ready networks.

Why Telecom Providers Choose A10

- Align with national infrastructure protection standards through proactive security architecture
- Minimise operational risk and accelerate breach recovery with intelligent threat detection and mitigation
- Gain enhanced visibility and real-time threat response across IT and production networks

By adopting A10 solutions, providers can:

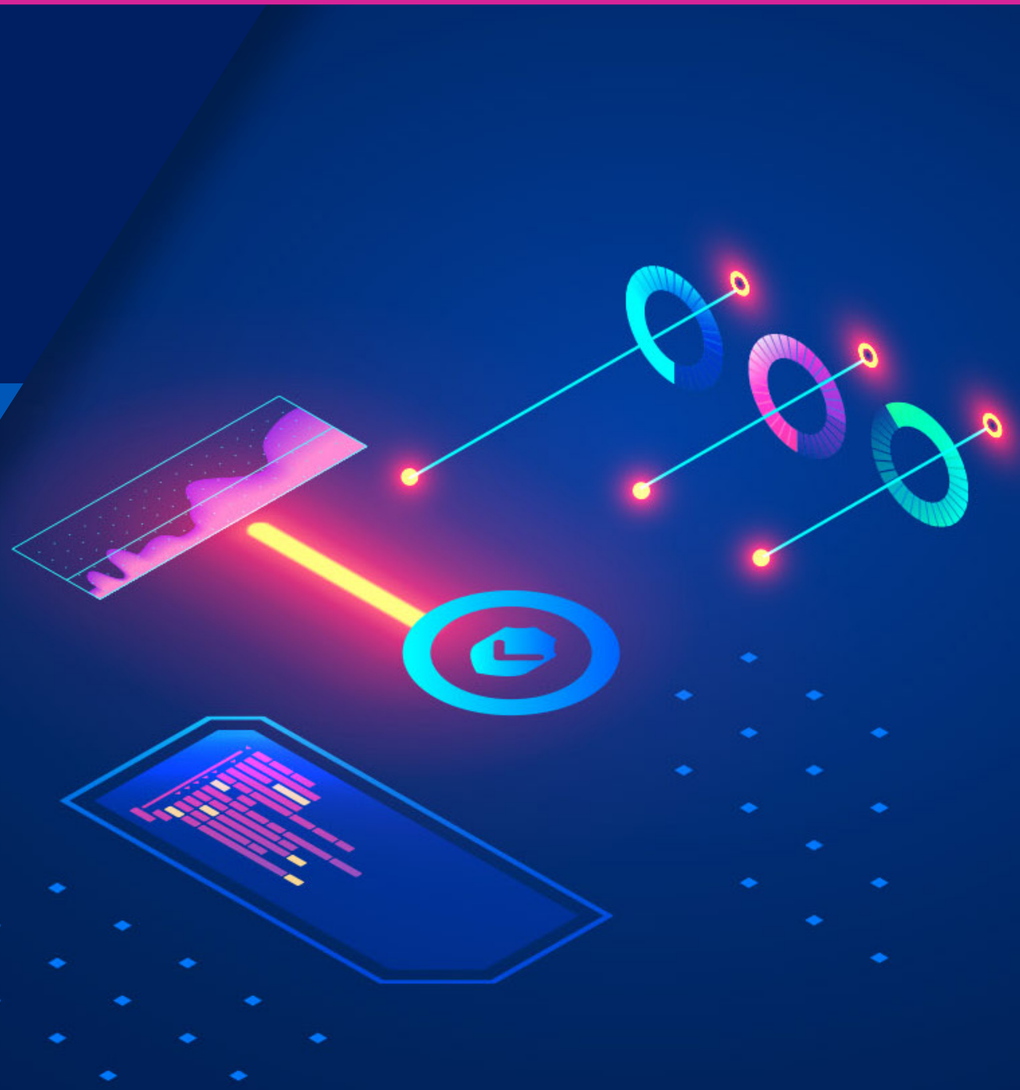
- Protect APIs and web applications using ThreatX, defending against advanced attack vectors targeting digital interfaces
- Future-proof infrastructure with seamless IPv6 support and hybrid cloud capabilities
- Differentiate competitively by demonstrating resilience, reliability, and trustworthiness to customers and regulators

Scalable Solutions for Every Provider

A10's carrier-grade solutions are built to support providers of all sizes, from regional broadband operators to Tier 1 mobile players. The same robust core technology powers every deployment, helping to ensure performance, security, and scalability across the board.

Comprehensive Protection Across the Stack

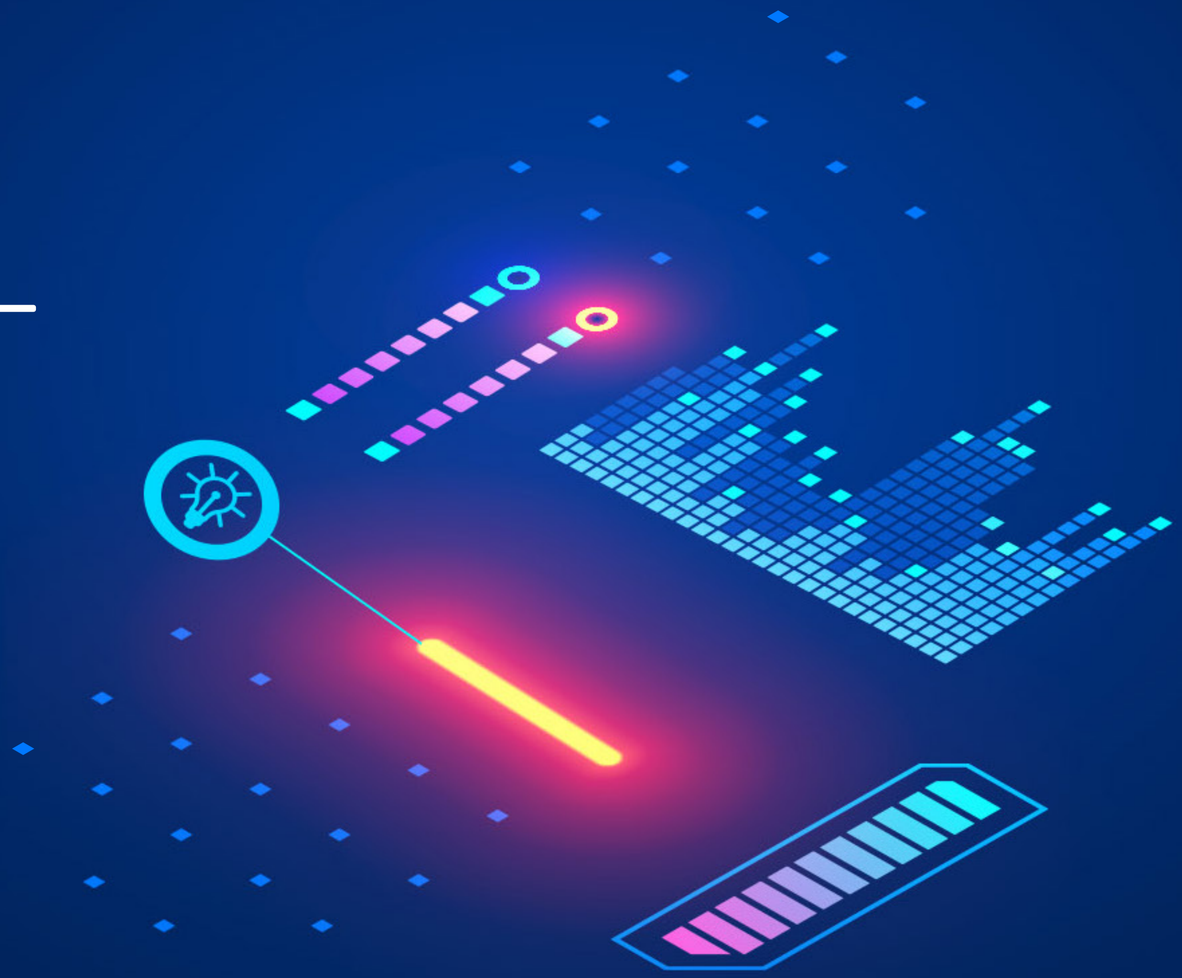
- **A10 Defend** provides end-to-end DDoS protection, covering detection, mitigation, intelligence, and centralised control for both IT and production environments.
- **A10 Thunder CGN** enables providers to stretch limited IPv4 address pools while transitioning smoothly to IPv6. With built-in DDoS protection and failover capabilities, it ensures uninterrupted service, even when networks are under pressure.
- **ThreatX by A10 Networks** secures APIs and web applications, helping to ensure digital operations are protected.



> Together, these solutions offer a unified defence strategy that meets TSA mandates while safeguarding mission-critical infrastructure.

More than Compliance – A Strategic Imperative

A10 Networks empowers telecom providers to go beyond regulatory checkboxes. It unlocks strategic, operational, and reputational advantages that position them for long-term success.



Strengthen National Infrastructure

- TSA compliance ensures telecom networks are resilient against cyber threats, supporting the continuity of critical services like energy, transport, and healthcare.
- It reinforces the role of telecom providers as guardians of national infrastructure, elevating their importance in public safety and economic stability.

Gain Competitive Advantage

- Providers that proactively meet TSA standards can differentiate themselves by showcasing robust security and reliability to customers, partners, and regulators.
- Compliance becomes a badge of trust, helping attract enterprise clients and government contracts that demand high security standards.

Improve Operational Resilience

- The TSA mandates a holistic approach to resilience, integrating business continuity, disaster recovery, supply chain security, and crisis management.
- This reduces downtime, improves incident response, and ensures providers can adapt quickly to disruptions, from cyberattacks to natural disasters.

Streamline Risk Management

- Providers must identify and protect their critical business services, shifting focus from isolated systems to end-to-end service delivery.
- This strategic clarity helps prioritise investments, optimise resources, and reduce exposure to systemic risks.

Strengthening Supply Chain Security

- TSA compliance extends to third-party vendors, encouraging providers to vet and secure their supply chains.
- This reduces vulnerabilities introduced by external partners and ensures consistent security across the ecosystem.

Enhance Regulatory Relationships

- The TSA mandates a holistic approach to resilience, integrating business continuity, disaster recovery, supply chain security, and crisis management.
- Demonstrating TSA compliance builds credibility with regulators like Ofcom, fostering smoother audits and fewer penalties.
- It also positions providers as proactive collaborators in shaping future telecom security standards.

Your Journey to Achieving TSA Compliance

In today's rapidly evolving digital landscape, TSA compliance isn't just about meeting stringent standards, it's about setting them. For organisations aiming to build secure, resilient networks, compliance can become a strategic advantage in the face of ever-growing cyber threats.

Start with the TSA Compliance Checklist

Ensure the vendors you're evaluating have the required critical capabilities to meet TSA requirements

Request Now

Explore the Latest TSA Solutions Brief

Ready to rethink your infrastructure strategy? Read our TSA Compliance and Network Resilience for UK Telcos brief to stay ahead of emerging compliance demands

Read Now

Or Book a Briefing with One of Our Experts

Get tailored guidance on how your organisation can meet TSA compliance and strengthen network resilience

Schedule Briefing

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) 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-EB-14178-EN-01 Nov 2025