MEETING THE
UK TELECOM SECURITY ACT (TSA)
WITH KRON NETWORK PAM

Securing Remote Privileged Access For Telecom Network Infrastructure:

Meeting The UK Telecom Security Act (TSA) With Kron Network Pam

As the UK's **Telecom Security Act (TSA)** reshapes how telecom providers manage cybersecurity, one requirement stands out as both urgent and complex: **telco-operator-controlled, secure, and auditable remote access to critical network infrastructure.**

Traditional PAM solutions — often retrofitted to support telecom environments — fall short when faced with the scale, diversity, and operational realities of telecom networks.

That's where **Kron Network PAM** comes in, purpose-built for this exact challenge. Designed with telecom infrastructure at its core, **Kron Network PAM delivers secure, identity-bound, on-prem privileged access,** even for remote users — with zero compromise on compliance or performance.

Understanding the Telecom Security Act (TSA) and Its Real- World Implications

The **UK Telecom Security Act** doesn't explicitly state that Privileged Access Management (PAM) solutions must be deployed on-premise. However, the **Telecom Security Requirements (TSRs)** — the detailed technical guidance enforced by **Ofcom** and aligned with **NCSC** principles — effectively lead many UK telecom operators to that conclusion.

Kron TECHNOLOGIES

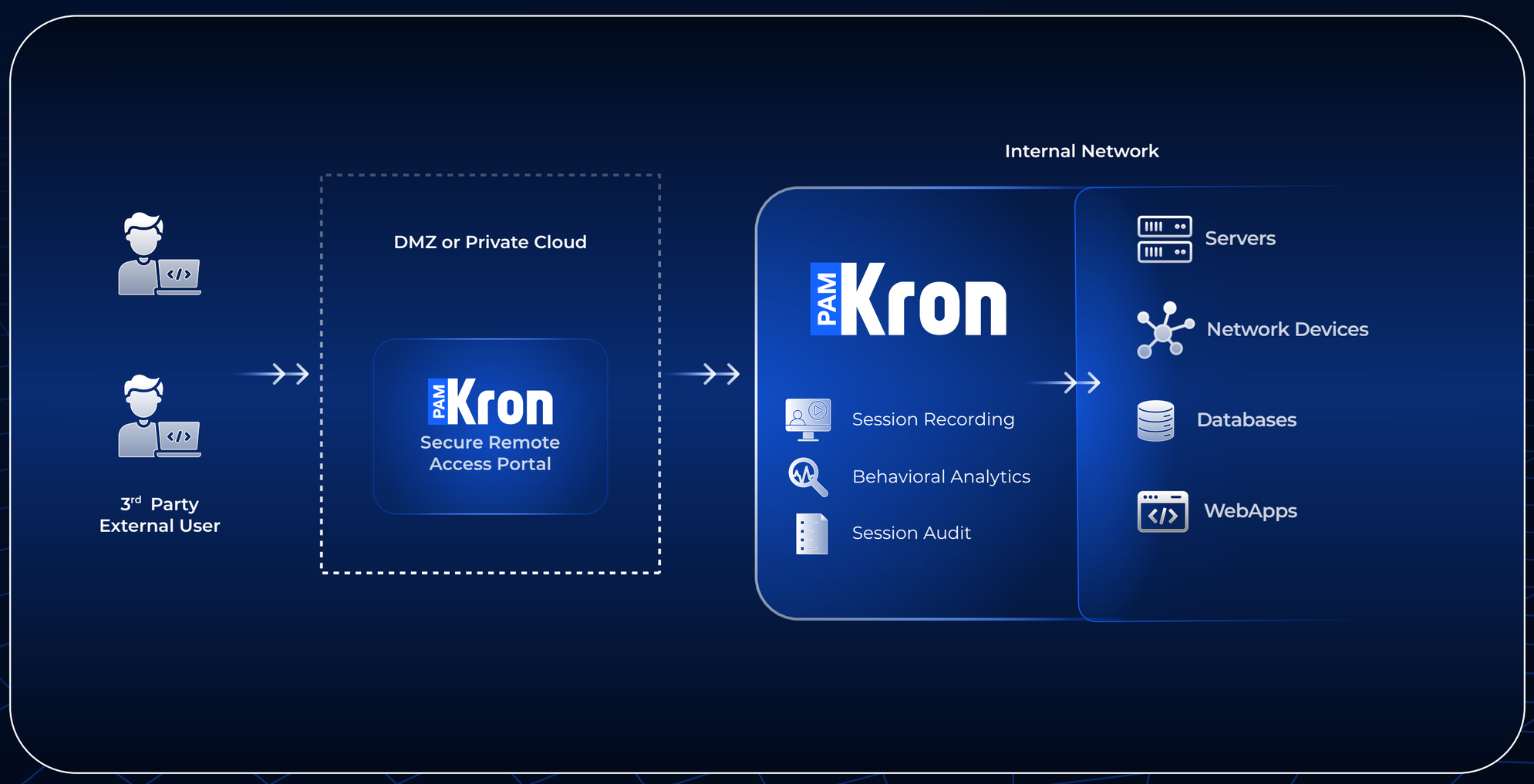
Secure Remote Access Requirements

The TSRs mandate that:

- Remote privileged access must be **strongly authenticated, centrally controlled, and fully auditable**
- Access paths must be **minimized and justified**
- Operators must have **full control** over logs, credentials, and access workflows
- Suppliers and third parties must access systems only through **approved, controlled methods**

This creates significant challenges for **SaaS-based PAMs,** especially when it comes to:

- **Log data sovereignty**
- **Credential storage and injection**
- **Operator control over access sessions**



Kron TECHNOLOGIES

Preference for On-Premise or Private Cloud

While not technically forbidden, public cloud or SaaS PAMs raise red flags. In practice, most UK telecom operators adopt a **risk-averse interpretation**, meaning:

- **On-premise or private cloud PAM deployments** are strongly preferred
- This ensures complete control, **data residency**, and **supplier accountability**
- It also simplifies assurance under internal audits and NCSC guidance

Ofcom & NCSC Guidance

Both Ofcom and the NCSC emphasize the need for:

- **Tight administrative access control**
- **Strong protection of sensitive data**
- **No exposure to unintended third parties**

So while the letter of the law may not hard-code “on-premise PAM,” the **spirit of compliance clearly points in that direction** — especially for remote privileged access use cases.

Kron TECHNOLOGIES

PAM Kron

KRON NETWORK PAM: PURPOSE- BUILT FOR TELECOM-GRADE COMPLIANCE

This is where Kron Network PAM stands out — not as a retrofitted IT tool, but as a network-native, compliance-aligned solution for today's telecom operators.

Here's why Kron Network PAM is the natural choice for securing privileged access in line with the TSA and TSRs:

1. Fully On-Premise Deployment - Aligning with TSA Realities

Kron Network PAM offers **lightweight, redundant on-premise deployment** — no third-party cloud dependencies, no external log repositories, and no SaaS risks. The entire stack, including session brokers, AAA engines, and audit logging, can be run within your network perimeter — even on just two virtual machines.

This ensures full **data sovereignty, session control, and compliance alignment** — a challenge most traditional PAM vendors can't easily overcome.

2. Agentless, Scalable, and Vendor - Agnostic

Kron Network PAM is **fully agentless** and supports **all major network vendors** — including Cisco, Ericsson, Huawei, Nokia, ZTE, and more. It's already operating at **telecom scale**, securing:

- 160,000+ network devices
- Globally distributed environments
- Access for both internal admins and third-party engineers

The system has been field-proven to handle **5,000+ transactions per second per node,** making it suitable even for Tier 1 backbone providers.

Kron TECHNOLOGIES

3. Secure Remote Access - Protocol-Level Control, With or Without VPN

Kron Network PAM provides **flexible deployment options** for secure remote access — whether your operations prefer a **VPNless approach** for speed and simplicity, or a **VPN-based setup** for layered network segmentation.

In both cases, Kron Network PAM brokers access through its **protocol-level proxy gateway,** eliminating the need for legacy jump servers and ensuring full visibility and control over every session.

Key capabilities include:

- ✓ **Strong MFA enforcement** across CLI and GUI access, regardless of connection method
- ✓ **Session brokering via Kron's secure Session Manager**, supporting both direct (VPNless) or VPN-tunneled access
- ✓ **Time-based, IP-based, and geolocation-based access restrictions**
- ✓ **Full session recording, real-time monitoring, and immediate termination capabilities**

Access is always **identity-bound**. Users authenticate using **corporate credentials** (via AD, Entra ID, SAML, etc.), while Kron Network PAM handles credential injection and **command-level policy enforcement** behind the scenes.

Whether your organization uses **dedicated VPNs** for third-party engineers or embraces a **VPNless Zero Trust model**, Kron Network PAM adapts to your architecture — without compromising on compliance, control, or usability.

Kron TECHNOLOGIES

4. Integrated TACACS+, RADIUS, and AVP Control - Telecom-Grade AAA

Kron Network PAM doesn't rely on external AAA systems. It includes:

- Built-in **TACACS+** and **RADIUS** servers
- Support for **AVP-based authorization**
- Built-in **2FA support for CLI access** on legacy and modern devices

This closes one of the biggest security gaps in telecom infrastructure — **legacy protocols with no native MFA support, or a legacy network element that supports only TELNET.** With Kron Network PAM, even a 10-year-old router can participate in a **Zero Trust access model.**

5. Auditing, Monitoring, and Compliance - Built In

Kron Network PAM captures:

- Full session logs and keystroke-by-keystroke playback
- Command-level filtering and policy enforcement
- Alerts for unusual behavior or policy violations

Logs are retained in **tamper-evident formats**, exportable to your SIEM, and available instantly for compliance audits — aligning perfectly with **ISO 27001, NIS/NIS2, PCI DSS 4.0,** and of course, **UK TSA** controls.

Kron TECHNOLOGIES

Final Thoughts:
The Right PAM for the Telecom Security Act Era

UK telecom operators face a clear challenge: secure remote access **without losing control.** While many PAM platforms talk a good game, only a few were designed with **network infrastructure and Telco** in mind — and even fewer can meet the **on-premise, operator-controlled, telecom-scale** requirements dictated by the UK's Telecom Security Requirements.

Kron Network PAM is the right tool for this job — because it was purpose-built for it - **Not Bolted On Later**

- **Natively multi-tenant**, designed to meet the needs of multi-divisional and complex telecom environments.
- **Born in Telco**, not a patchwork solution from mergers or acquisitions.
- **Granular protocol-level control** across TACACS+, RADIUS, SSH, TELNET, and more.
- **Frictionless for network teams,** with zero disruption to daily workflows.
- **Fully aligned with NCSC, Ofcom, and TSA compliance requirements.**
- **Proven at scale**, trusted by Tier 1 telecom operators.

> If you're interested in learning more about how Kron Network PAM can support your compliance efforts while modernizing access security across your telecom infrastructure.

Kron
TECHNOLOGIES