silverlake
SYMMETRY AT WORK

masterSAM

Silverlake MasterSAM Telecommunication Sector

- Unique Challenges in the Telecommunication Sector
- How PAM Helps Strengthen Telecom Security

Unique Challenges in the Telecommunication Sector

The telecommunications industry is a major part of modern society, but it faces serious cybersecurity threats. These threats make strong Privileged Access Management (PAM) solutions essential.

In 2025, Europe operator confirmed a cyber-attack that compromised the personal data of 6.4 million customers. In 2024, hacker alleges to have stolen a Malaysia telco's customer database with 'nearly 20 million effective user data'.

a. Wider Attack Surface

As telecom companies adopt cloud services, 5G, and IoT technologies, they become more vulnerable. With more systems connected and more access points created, attackers have more opportunities to break in. A single compromised privileged account can lead to massive damage because it grants attackers elevated access to an organisation's most sensitive systems and data, potentially leading to data breaches, system disruptions, significant financial losses, reputational damage, and operational downtime.

b. Risks in 5G Networks

Cyber Risks Caused by 5G Technology

The main cybersecurity and access security risks to be faced by organisations with the use of 5G technology can be grouped under three main headings.

- Complexity of Network Architecture: 5G networks rely on a more complex architecture, incorporating virtualisation, edge computing, and network slicing. This complexity introduces potential security gaps that attackers may exploit.
- New Protocols and Standards: 5G introduces new protocols and standards, some of which may not have been thoroughly tested for security flaws. As these technologies are deployed at scale, attackers will likely discover and exploit previously unknown vulnerabilities.
- Supply Chain Risks: The construction of 5G networks involves a global supply chain with multiple vendors providing equipment and software. Any compromise or tampering in this supply chain could lead to security issues within the network infrastructure.

Unique Challenges in the Telecommunication Sector

c. Third-Party and Remote Access Risks

Telecom relies heavily on remote staff and vendors. Granting them secure, temporary access is difficult. Traditional methods like VPNs are outdated, hard to manage, and can slow down operations.

d. Insider Threats

Employees can pose risks, either by accident or intentionally. Common issues include:

- Forgotten or unused accounts
- Over-privileged users
- Shared passwords
- Credentials stored in unsecured files or hard-coded into software

e. Legacy Systems and Digital Transformation

Many telecom systems are outdated and need to modernise to support 5G. Moving to cloud-based platforms introduces new security needs. With thousands of privileged accounts, manual management is no longer practical.

f. Tough Compliance Requirements

Telecom operators must follow strict regulations like ISO, GDPR, QoS standard, and more. Failing to comply can lead to heavy penalties and reputational damage.
Privileged Access Management (PAM) plays a key role in helping telecom companies tackle complex cybersecurity threats. It provides a structured, automated way to control and monitor elevated access across the organisation.

How PAM Helps Strengthen Telecom Security

1. Enforces Least Privilege Access

PAM ensures users only get the minimum access needed to do their job—nothing more. This reduces the chance of attackers misusing high-level access. It also helps meet security standards like GDPR, ISO 27001, HIPAA, and PCI-DSS.

2. Centralised Credential Management

All privileged accounts are stored in one secure vault. This prevents unsafe practices like:

- Keeping passwords in spreadsheets or shared documents
- Using hard-coded credentials in apps or devices

PAM also rotates passwords automatically, making them harder to crack.

3. Monitors and Audits Privileged Sessions

PAM tracks and records everything users do with privileged access. This allows:

- Early detection of suspicious activity
- Clear records of who did what, helping with investigations
- Proof for auditors and regulators

This is especially helpful when credentials are shared, as PAM ensures full accountability.

4. Just-in-Time (JIT) Access

Instead of giving users permanent access, JIT gives access only when needed—and removes it right after the task is done. This shortens the time attackers could exploit access and helps prevent misuse.

How PAM Helps Strengthen Telecom Security

5. Secures Remote Access

With remote staff and vendors, PAM enables secure, easy-to-manage access without needing VPNs or extra software. All remote activity is tracked and controlled in real time.

6. Protects Cloud and 5G Environments

As telecoms shift to cloud and 5G, PAM helps:

- Manage access to cloud platforms
- Control credentials in fast-moving environments
- Secure virtual components used in 5G systems

7. Supports Compliance and Audit Readiness

PAM keeps detailed logs and reports of all privileged activities. **How PAM Supports** Telco in driven to meet QoS standards:

By controlling privileged accounts, PAM prevents unauthorised access or misconfigurations that could disrupt QoS policies and degrade service quality. It ensures the stability of the network devices and platforms responsible for traffic prioritisation and resource allocation, which are fundamental to QoS. A robust PAM solution helps telcos maintain compliance with regulatory requirements by providing a secure environment for network operations.

Summary: Why PAM Delivers High ROI in Telecom

- Reduces costly breaches
- Meets tough regulatory demands
- Saves time through automation
- Improves accountability and visibility
- Supports secure digital transformation (5G, cloud)

Bottom Line: PAM pays for itself by **reducing risk, saving time, and avoiding regulatory costs**—a high-ROI cybersecurity investment for telecom operators.