T-Mobile ABM Plan – FY26

Account Overview

What We Heard Last Time

- Pain: Persistent SSH keys and root-level access across infrastructure.
- Urgency: Actively prioritizing cyberattack prevention.
- Outcome: Closed/lost due to a competing initiative with executive backing that addressed overlapping areas.

What's Changed (Based on 10-K)

- Credential misuse and unauthorized access are still top security concerns.
- Continued references to breaches and infrastructure gaps, particularly involving third parties and internal identity governance issues.
- No mention of a named vendor or solution that resolves machine identity, short-lived credentials, or cloud-native governance—indicating the selected tool may be incomplete.
- The company is investing heavily in automation, AI, and multi-cloud scale, introducing new pressures on identity management and privileged access control.

Strategic Interpretation

It appears the original initiative selected may not fully address their evolving infrastructure needs:

- They likely deployed a traditional PAM or secrets vault that does not support ephemeral access, JIT workflows, or workload/machine identity at scale.

- Security and engineering teams are likely still struggling with operational friction and lack of visibility across hybrid and cloud environments.

- Given their roadmap and breach history, they may now be more receptive to tools that *augment* existing solutions with zero trust enforcement and developer-aligned workflows.

Updated Positioning for Re-Engagement

Pain Reframing

- Access risk still persists across machines and humans.

- Credentials and over-permissioning remain the most likely root cause of breaches.

- Legacy PAM or identity bolt-ons may not scale with AI, Kubernetes, or multi-cloud growth.

Hypothesis: Where T-Mobile Is Now

T-Mobile likely moved forward with a **legacy or compliance-oriented PAM solution** last year to address audit gaps and basic access control. However, based on their latest 10-K disclosures, they are still **struggling with credential-based risk**, **unauthorized access**, and **identity governance across cloud and hybrid systems**. With infrastructure complexity accelerating—driven by **AI, multi-cloud growth, and automation initiatives**—that existing solution is likely **insufficient for engineering velocity or machine identity coverage**.

Their initial solution likely:

- Addresses static credentials and human access governance

- Does not solve for **ephemeral access**, **non-human identity**, or **developer-native workflows**

- Introduced **workflow friction** or **coverage gaps** as infrastructure scaled

Breaking In

Position Teleport as a complementary modernization layer that addresses the exact gaps they likely still face:

- **Eliminate persistent credentials**, not just vault them
- **Extend zero trust to machines, CI/CD, Kubernetes, and AI workflows**
- **Deliver engineering velocity** through ephemeral, policy-based access

Approach should focus on:

- **Security leaders** frustrated by residual risk and audit blind spots
- **Platform or DevSecOps teams** under pressure to scale secure access without adding friction
- Emphasizing **low-overhead layering** alongside their current stack, not a rip-and-replace

Messaging

"It's clear that T-Mobile is still under pressure to reduce credential risk and enforce least privilege. If the previous solution addressed only part of the problem, we may be able to help close the gaps—without requiring a rip and replace."

"Teleport helps teams evolve beyond persistent credentials by eliminating them entirely—introducing cryptographic, short-lived identity for both engineers and workloads. Think zero trust access, aligned to how your infrastructure and teams actually work."

Email Campaign

Subject: Eliminating root access and persistent credentials

Email #1

Hi {{first_name}},

I'm reaching out as a new point of contact for T-Mobile here at Teleport. Our teams spoke last year as you guys were prioritizing root privilege reduction and eliminating persistent keys. From my understanding, another solution was selected at the time due to overlapping capabilities it provided to another project happening.

Since then, T-Mobile has publicly reinforced that credential-based threats and access governance remain ongoing challenges—especially across cloud, AI, and hybrid environments.

If your current stack isn't addressing things like short-lived credentials, machine identity, or JIT access at scale, might it be worth a reconnect?

Best,
Grace

Email #2
Subject: Following up on identity risk at T-Mobile

Hi {{first_name}},

Wanted to follow up on my last note.
From what we're seeing across telecom and enterprise infra, a lot of teams are finding gaps between what traditional PAM/secrets management covers and what's needed for things like non-human identity, JIT access, or automated workload governance.

Has your team run into any of that as your cloud and AI environments expand?

Would be happy to compare notes.

Best,
Grace

Email #3
Subject: Where Teleport fits with existing tools

Hi {{first_name}},

Just a quick follow-up. Many of the teams we are working with already have legacy PAM or vaults in place.
We often come in to help with the gaps those tools cannot solve, such as eliminating static credentials entirely, introducing short-lived identity, and improving access governance for non-human users and modern infrastructure.

If your team is still focused on reducing credential-based risks, happy to share how others are layering Teleport into their existing stack.

Best,
Grace

Email #4
Subject: Root access and credential risk

Hi {{first_name}},

Last year your team was focused on reducing root privileges and persistent credentials. That remains one of the most common weak points we are seeing in breach cases today.

If your priorities around reducing credential-based risk are still active, I would be happy to share how teams are solving this with ephemeral identity and better controls across cloud and hybrid environments.

Would you be open to a short chat?

Best,
Grace

Email #5
Subject: Reducing attack surface as infrastructure evolves

Hi {{first_name}},

I wanted to check in again.
As infrastructure expands across AI, cloud, and hybrid models, we are seeing more teams revisit how they enforce identity and access controls. The risks tied to persistent keys and standing privileges tend to grow with that complexity.

If this is coming back on the radar for your team, I would be happy to share some recent examples from other large infrastructure organizations.

Best,
Grace

Email #6
Subject: A quick check-in on priorities

Hi {{first_name}},

I know timing is everything. Since your team had selected another solution last year, I wanted to check whether priorities around identity risk reduction or cloud security posture have shifted.

If there is a new owner or if this is something we should revisit, happy to connect at the right time.

Best,
Grace

Email #7
Subject: Open to a quick chat this quarter?

Hi {{first_name}},

As your environment continues to grow more dynamic, especially with the AI and cloud-native initiatives mentioned in your 10-K, I thought this might be a good time to revisit how Teleport helps teams eliminate persistent credentials and scale secure access.

If this is worth a quick conversation this quarter, just let me know.

Best,
Grace

LI Messages

LinkedIn Connection Request
Hi {{first_name}}, I work with Teleport. Saw that your team had previously looked at eliminating persistent keys and improving privilege management. Would be great to connect and share where we are seeing teams make progress here.

LinkedIn Follow-Up 1 (after connect)
Thanks for connecting, {{first_name}}. Given the ongoing focus on credential-based risk in your latest filings, thought this might be a good time to revisit where Teleport fits alongside existing tools. Would you be open to a quick chat?

LinkedIn Follow-Up 2 (if they go quiet after connect)
Just wanted to follow up here, {{first_name}}. We are seeing a lot of teams revisit static credential risks as cloud and AI workloads expand. If that is relevant for your team right now, happy to share a few quick examples.