CMS
IT SERVICES
Reliable I Robust I Secure

Case Study: Identity & Access Management integrated with SOC Services for a Telecom Tower Company

Executive Summary

This case study is an excellent example of successfully streamlining the identity and access governance at one of the largest Telecom tower companies in the world. Our comprehensive identity and access solutions, and managed cybersecurity solutions, accelerated the customer's digital transformation and centralized outcome-based control over accesses and authorisation processes.

The result was the **digital transformation of the complete IT ecosystem fortifying the customers' cyber defences.**

The Customer

With over 185,447 telecom towers in 335,791 locations in all 22 telecom circles in India, customer is one of the largest telecom tower companies in the world. For various mobile operators and all wireless telecommunication service providers, Customer deploys, owns, and manages telecom towers and communication structures. The Company has been the industry pioneer in adopting green energy initiatives for its operations and more than 74,353 are green sites. To achieve an aggressive 99.96% average uptime at the sites, 90% of front-line field force operates on the ground and is responsible for maintaining network connectivity. one of the sets of outcomes they strive for consists of robust corporate governance structure, innovative mechanism, and processes to empower cost effective solutions for our customers, technology-powered applications, seamless information flow and real-time decision making, and automation of operational services.

The Challenge

1. Continual configurations of account policy, access rights and password control, and controlling/ preventing unauthorized access to application and segments in the IT environment was a big challenge.

2. Visibility on the applications’ access and privilege accesses was minimal and discovery, the incident response was weak.

3. Governing identities and access across their hybrid IT landscape was difficult.

4. Compromised visibility across the ecosystem made it hard to govern access to critical applications efficiently.

5. Time-consuming manual processes and sometimes, cumbersome user experience also acted as barriers to their cloud strategy.

CMS
IT SERVICES
Reliable I Robust I Secure

Case Study: Identity & Access Management integrated with SOC Services for a Telecom Tower Company

The Solution

As a cornerstone of the holistic managed cybersecurity services, digital forensics, incident response, identity & access management with integrated privilege identity and access monitoring and management streamlined the identity and access governance. This helped lay a strong foundation to accelerate their digital transformation. Key aspects include:

1. Streamline the policies and controls for the identity and access management engine.
2. Monthly cadence for verification/ reconciliation of the users and their accessed to systems. Centralized control and monitoring of SoD conflicts, data use.
3. Validation/ re-validation of the business requirement of continued access of systems for privileged users, managing privileged user IDs and third-party user ids accessing the customer IT network.
4. Performing access and authorisation configurations reviews to discover and rectify inconsistencies and redundancies against security policy.

The Benefits

1. Centralized outcome-based control over access and authorisation processes adds efficiency and reduces IT/ HR hours.
2. Unprecedented access visibility keeps enterprise assets secure and ensures continuous compliance while eliminating redundant security procedures.
3. Improved efficiency helps the bottom line and enhances employee and customer relationships.
4. Seamless integration to the managed cybersecurity services fabric strengthens VOILA delivery framework- Visibility, Observability, Incident Response, Low-code integration, and Automation and analytics- and catalyses customer's digital transformation.

Contact Us for Best in Class Cyber Defence