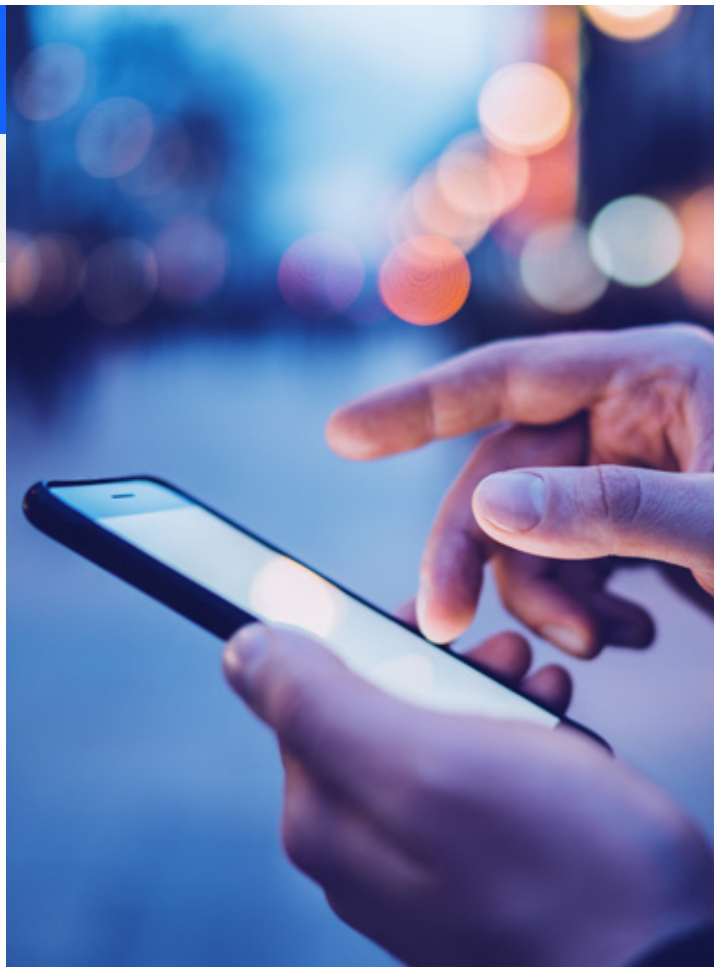
Single Connect Krontech

Large Telecom Operator chooses Krontech Single Connect to protect their systems

Large Telecom Operator from APAC Region



CHALLENGE

The company was using a customized Privileged Access Management application. With the highest quality standards and expectations in mind, the company was looking for a PAM product to meet its needs and completely replace this custom application.

The company needed a solution to manage privileged access in and between the IT and network worlds' under one roof, securely store privileged credentials in vaults compliant with FIPS standards and manage the increased traffic with high availability. They understood that unified governance would bring tremendous productivity benefits by managing all policies from a single solution and thus minimizing administrative costs. Performing audits through a single system would prove beneficial for regulatory processes and compliance. This PAM solution had to fully support the requirements of the IT and network world.

SOLUTION

After starting a POC process, the company tested Single Connect and other PAM products in all required scenarios, from the simplest to the most comprehensive. At the end of this meticulous process, the company finally decided that Single Connect was the PAM solution they were looking for. It purchased the Single Connect Privileged Session Manager (SSH Proxy, RDP Proxy, HTTP Proxy, SFTP Proxy), Dynamic Password Controller, Privileged Task Automation, Mobile Application, Reporting, and Multi-Factor Authentication modules.

- The company started to manage all privileged accounts of telecom vendor products (Ericsson, Huawei, ZTE, etc.) with Single Connect. They now control, restrict, and authorize all access to these products without exposing credentials while logging all audit records.
- The company manages more than 1300 endpoints via proxies in the Privileged Session Manager module. With Single Connect's auto-login feature, the company supports more than 50 privatized telecom providers accessing web portals through the HTTP proxy.
- The company wanted to restrict access to applications with privileged credentials. With Single Connect, the company can determine which privileged accounts have access to applications based on user groups and enable automatic login for privileged accounts without requiring users to expose their credentials.
- Company-wide cybersecurity service with an effective privileged access management solution.

- The company can now record audit logs and video sessions and apply OCR to video recordings to create searchable indexes from the video recordings. The Single Connect Privileged Session allows company to manage all these applications according to PAM principles. Various database clients and other applications, EMS nodes, and apps were supported as part of this project.

- The company assigns significant importance to access security. To elevate security to the highest level, the company applies various trusted mechanisms at each authentication and authorization step. They also use MFA for approvals and reservations and configure multi-level managerial approval processes.

- The company uses applications with X11 support, and now they can access these applications via Single Connect's RDP.

- The company uses a highly effective and advanced reporting infrastructure at all levels for executive and operational management teams. They wanted to maintain this reporting system through Single Connect. They now create dashboards, export PDFs, and distribute these reports to appointed audiences on a schedule. Krontech created a reporting stream for this project and developed dashboards and more than 70 new reports exclusively at customer's request.

- The company can now automatically configure OS settings on Windows and Linux servers using the Privileged Task Automation module. Because only privileged accounts can set OS configurations on Windows and Linux devices and execute configuration commands, the company abandoned manual configuration processes. They automated the processes by using Single Connect's PTA module, preventing disclosure of privileged account credentials while logging all configuration operations in Single Connect.

- The company uses numerous devices and applications. Now they use Single Connect to manage the onboarding and password randomization of privileged accounts used to access these devices and applications. With API integration, Single Connect can automatically onboard these accounts via Rest and Soap APIs, randomize passwords, and securely store them in the vault after use via the APIs.

- Password protection, confidentiality, and logging of access to privileged credentials are high priorities for the company. The SAPM module ensures that users have access to devices without having to share privileged credentials. They can also share the credentials with their respective teams with managerial approvals. All approvals and accesses are logged.

- Recognizing the importance of securing privileged accounts and devices, Krontech implemented 360° on boarding of company's infrastructure. Krontech also consulted to the company on best practices for managing privileged access, including syntax configuration for ease of use, password rotation strategies, approval workflows, dashboard views, and critical reports to provide comprehensive insight into customers access security.

- To ensure the service continuity for critical IT infrastructure and uninterrupted access to company IT users, Kron provided a comprehensive redundancy plan. This plan included geo-redundancy by deploying multi-site clusters, and cluster level redundancy by having multiple instances in each cluster with runtime replication across all instances and clusters. Backup of privileged credentials is managed at regular intervals for offline restoration via break glass method. Rotation of privileged user accounts from super users is also in place to ensure continued access to devices in worst-case scenarios.

- Krontech deployed a separate instance of lightweight PAM with minimal services in the DMZ. It exposes the companies external-facing services to the untrusted network, allowing users to perform required tasks such as 2FA authentication and connection approval from their own devices while reducing the public footprint of the company network directly to the production PAM environment.

RESULT

The company now manages its IT and network devices, applications, web portals - its entire ecosystem using multiple access technologies - through a single PAM solution. The company can report and list all access logs at will, restrict users based on the principle of least privilege, change privileged account passwords regularly, and control 1500 endpoints and 500 privileged users.

KEY BENEFITS

- Improving cybersecurity posture with an effective privileged access management strategy.
- Unified and centralized Privileged Access Management, bringing the company-wide IT and network worlds together.
- Simplified access permission management with smooth, flexible, and auditable approval and reservation workflows.
- Auditing privileged user activities and meeting compliance and standard requirements.
- In-Session Least Privilege Management.