CASE STUDY: A Leader Finance Organization from Malaysia improves its Security Posture with Single Connect

ABOUT THE COMPANY

As Malaysia's online equities broker, our client offers trading on Bursa Malaysia through a FinTech platform that makes investment management a complete online experience. Just after their first year, the company was named the 2018 FinTech Company of the Year by the Malaysian Communications and Multimedia Commission (MCMC). It holds a restricted capital markets services license from the Securities Commission Malaysia, which allows the company to trade listed securities and offer investment advice.

CHALLENGE

Customers need to make informed decisions fast

As a leading investment management company that develops technologically fast and secure solutions with customer-centric strategies, the company was looking for a PAM solution that was as fast and adaptable as its approaches. Because its customers make investment calls every day, the company provides applications that enable its customers to make informed decisions quickly by ensuring secure and fast access to the information they need.

Protect credentials against internal and external actors

To protect privileged credentials against credential theft by internal and external actors, the company needed to:

- Store the passwords in an encrypted vault
- Change the passwords regularly
- Enforce password policies with a high-security level

Because changing passwords placed a heavy workload on operations teams in the absence of a PAM solution, the company's administrators used shared passwords, even though they knew that such a situation was risky in the event of an attack.

Manage all processes and record all activities

The company primarily needed to establish secure access management to govern and restrict access to target systems, prevent unsupervised access by internal actors, and detect misuse by legitimate users. All of these requirements called for:

- Implementing processes to request and access sessions
- Tracking and monitoring of user sessions and enabling live session monitoring
- Creating tamper-proof session log records
- Reporting and/or preventing unwanted user behavior, detecting misuse by legitimate users

The company also wanted to log all activities, comply with sectoral regulations, and prepare internal/external audits without adding additional effort to day-to-day operations.

Enforce the least privilege principle

Our client wanted to restrict privileged account access based on the least privileged principle, which enforces granting administrators only the permissions they need to perform their tasks.

The company was aware that users were being granted more than the required level of privileges or that privileges granted temporarily were not subsequently removed, which in turn increased the attack surface. The company needed to limit administrators' access to:

- A small number of necessary systems and applications
- Necessary operations and data only (e.g., application isolation, command blacklist, context-aware)

SOLUTION

Single Connect accompanies the company's dynamism and addresses its securely managed access management needs

Kron offered the Single Connect PAM solution. **The Privileged Session Management, Secret Management** and **Reporting** modules covered the company's needs, and the solution's trust mechanism and governance capabilities met its dynamic requirements.

Complete control over privileged access

Single Connect gave the company the ability to grant or restrict privileged account permissions whenever and however they needed. It provided controlled access to the target systems without revealing the system credentials and removed personal administrative rights because they could be used to retain access or be shared without permission.

Single Connect enabled a highly developed trust and accountability structure in the company's environment, ensuring that privileged accounts are used for legitimate business purposes only.

Now that the company has a privileged access management system in place with Single Connect, user accounts are given the minimum permissions required to perform an intended function to minimize the attack surface for privileged access and operations.

Password rotation

Single Connect also started to automatically change all privileged credentials at regular intervals on target systems and applications to prevent password sharing among colleagues.

Logging and tamper-proof reporting of all activities

Single Connect logs all activities of the company's admin users. Auditors can access these activities as video records, search the sessions' human-readable indexed log records, detect risky commands, and see violation attempts.

Thanks to Single Connect's ready-to-use set of reports and dashboards, the company can now report all activities for auditing and regulatory compliance purposes with tamper-proof records.

RESULT

The company strengthened its security posture and reduced the attack surface related to privileged accounts

Deploying the Single Connect PAM solution gave the company a broader granular view of what is happening within privileged sessions from a single pane of glass: a) who is the owner of the privileged accounts/credentials, b) who wants to access the credentials when and why, d) who approves these access requests, e) what are the role-based access policies, f) which privileged users attempted to violate which policies.

The company's privileged users can now log in to the system with their personal LDAP accounts and access authorized devices/applications/privileged accounts from a web portal. Single Connect can securely inject the privileged credentials into the sessions without credential exposure.

The security team started working immediately

Single Connect is recognized as the fastest to deploy PAM solution. The company's security team was able to set up Single Connect quickly and easily and can use Single Connect effortlessly.

Taking the workload off IT teams

User, server, session policies, and account password management are now easy to govern and no longer burden the company's IT teams. Single Connect changes the passwords of server accounts regularly in specified intervals, making accounts even more secure against password sharing.

Automatic device and account discovery

Single Connect's Account and Device Discovery module allowed the company to import their inventory into PAM quickly. Through Active Directory integration, admins have seamless authentication to PAM.

Native client support with PAM

Kron's Single Connect allows privileged users to use their preferred native clients while accessing through their devices. Kron believes that a PAM solution should allow privileged users to do their jobs without slowing the process or without changing their work habits. The company's privileged users can now use their preferred native clients in this secure access management lifecycle.

Easy to integrate

Thanks to Single Connect's ready-to-use integration support, the company can plug and play all applications in its ecosystems with integrations.

Reporting vulnerability factors

Single Connect's reporting abilities have allowed the company to create audit reports on the server accounts and detect any security vulnerability instantly.

KEY BENEFITS

- Managing all types of privileged access
- Secure vaulting
- Automated Discovery and Onboarding for privileged accounts and devices
- Compliance with the regulations
- Providing comprehensive Audit Reports and Dashboards
- Fastest to Deploy PAM solution
- Zero Trust Privileged Management