

An airline catering company deploys ARCON | PAM

overview







According to the latest (2018) Verizon report, cyber attacks on hospitality industry along with food services business have increased by one third comparing to that of the previous year. Almost 86% of breaches happening in catering industry stay unnoticed. In this backdrop, we would like to discuss about one of the Asian Catering giant who decided to take adequate security measures for their information assets and decided to deploy ARCON | Privileged Access Management (PAM) solution to secure their privileged accounts.

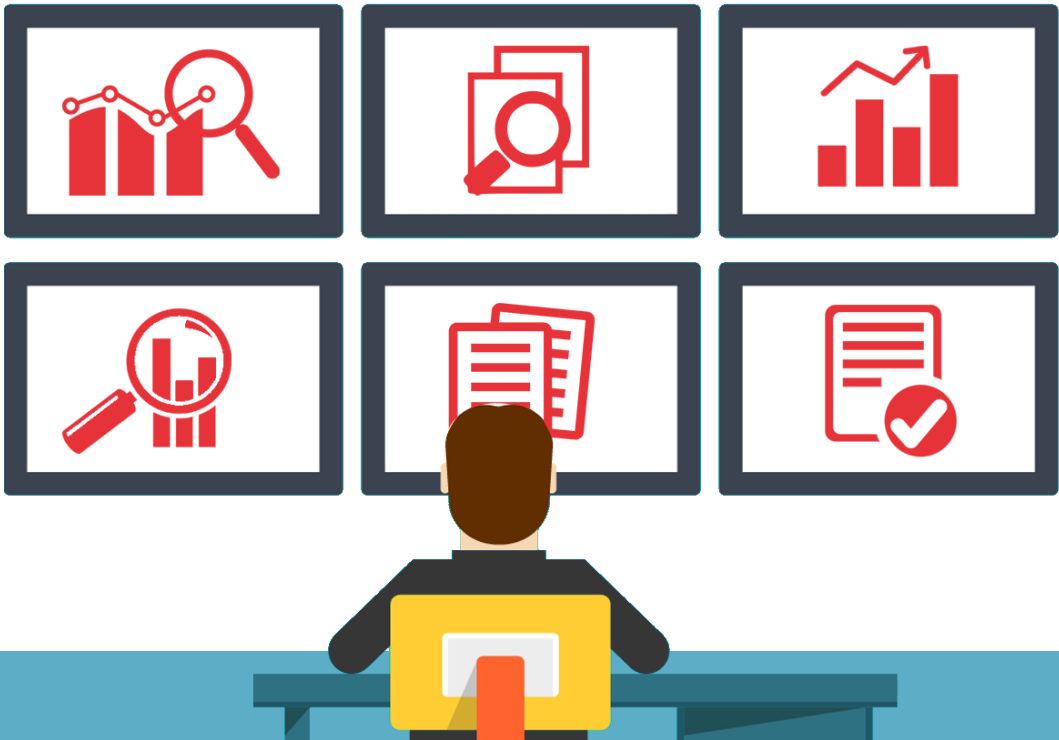
about the client

Based out of Dubai International airport region, this Aviation Catering giant provides pre-ordered foods to airlines, events, Jet catering and VIP catering. Our client's other services include laundry, food production and airport lounge food & beverage. The vastness of our client's hospitality services comprises of more than 11,000 employees who work continuously to provide almost 2.25 million meals everyday for more than 105 different airlines. In order to facilitate timely services and manage the huge demand, this airline food supplier maintains a 2.55km long electric monorail which transports meal carts, food plates and clean kitchen equipment's. The facilities also include a vacuum waste system to maintain the overall hygiene.

challenges faced

There are numerous data security challenges in aviation catering industry. Today catering companies maintain modernized technological structure to store and process a large amount of critical information. These information include supplier details, client details, employee details, airlines details, airlines passenger details, their personal identification number, payment details including credit card details, debit card details etc. These confidential information are normally accessed through multiple privileged accounts in an uncontrolled environment. As result, there is always a risk of malicious insiders or third party users compromising these data in unmonitored IT environment. Our client faced the following challenges:

	Lack of robust Access Control mechanism that could protect the huge database from malicious insiders and third parties.		No Reporting and audit of individual privileged user and privileged tasks.
	Absence of Authentication mechanism that would prevent unauthorized users from getting access to the privileged accounts.		No securing and randomizing privileged passwords for protecting confidential information from malicious insiders and suspicious third parties.
	No Real-time monitoring of the privileged user activities happening in the network.		Inadequate compliance measures that could not meet the global regulatory standards.



the solution

After elaborate and extensive technical evaluation, our client decided to choose ARCON | Privileged Access Management (PAM) that offered all of the above-mentioned security requirements under one roof. In order to diligently manage the operations of so many departments in aviation catering industry, our client had multiple privileged identities for managing various privileged tasks. These privileged accounts are the gateways to all the confidential information - mostly personal details of suppliers/ clients/ airline passengers including the payment details. In a typical shared and distributed environment where insiders and third parties have access to the privileged accounts, our client was looking for a tool that could continuously monitor all the user activities in real-time and detect suspicious activities (if any). ARCON | PAM helped in reinforcing the IT security mechanisms in the following ways:

Authorization:

ARCON | PAM helped the IT administrators to set up a unified centralized policy that offered a role based privileged access to the targeted system and authorized the user to access the system only on “need-to-know” and “need-to-do” basis.

01**02**

Channelize IT Operations

ARCON | PAM created functional groups for privileged users to access target systems based on the roles with the help of Virtual Grouping. It helped the IT team to segregate the various catering units and define their roles group wise, server wise and role wise

Access Control

With hundreds of users accessing database of various privileged accounts at any given point of time, ARCON | PAM monitors the privileged users who are accessing which account and for what purpose. It helped our client to mitigate unauthorized users from accessing key information.

03**04**

Multi-Factor Authentication

ARCON's Multi-factor Authentication worked as a robust validation mechanism. It acted as a strategic and genuine entry point to target systems and helped to manage the privileged users. The One-Time-Password (OTP) validation and biometric authentication assured the administrators about the authenticity of the users.

Fine-Grained Access Control

Fine-grained access control allowed our client to control the privileged users with role based centralized policy. It offered the IT administrators to ensure secure and authorized access to target systems and minimize the risk of uncontrolled user access.

05

Real time Session Monitoring

ARCON's Real Time Session Monitoring helped the IT administrators to spot any suspicious activity happening in the enterprise network. The Live Dashboard kept on giving real time update of all the activities in front of the IT admins. It captures all the logs in video and text format to offer a comprehensive security assessment.

07

Regulatory Standards

ARCON | PAM helped our client to meet the compliance like EU GDPR (General Data Protection and Regulation), PCI DSS (Payment Card Industry Data Security Standard), NESA (National Electronic Security Authority) etc.

09

06

Password Vaulting

ARCON's password vaulting helped our client to secure and randomize their privileged passwords. These passwords are stored in a highly secured electronic vault and thus could provide robust security to highly important privileged passwords.

08

Audit Trails

ARCON | PAM helped our client to generate comprehensive report of all privileged sessions. It worked as a tool to help the administrators in take wiser decisions related to the users and their activities.

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us     