University

A spate of security breaches involving some of the most prestigious global universities has brought to the fore an urgent need for safeguarding sensitive data. It has hastened the need for reinforcing the security architecture to protect confidential information.

Learn how ARCON Privileged Access Management helped a globally renowned university to attain the desired compliance level by providing a solution that would seamlessly monitor privileged access.

overview

Universities are an attractive target for compromised actors such as malicious insiders and third parties. As personal information sells on the web nowadays, this commercialization incentivises them to steal sensitive information.

Academic institutions collect, store and process a large amount of information such as Intellectual Property, personal details of alumni, faculty and staff members including other stakeholders. Threats of data breach always linger. Therefore, securing the critical information from an unauthorized access and compromised insiders and third parties is one of the biggest security concerns for academic institutions. In addition, stringent data protection regulatory standards such as the General Data Protection Regulation (GDPR) make it mandatory for them to deploy the essential safeguards to protect information assets.

Our client is one of the oldest educational institutions in the Middle East. It offers a full range of both undergraduate and graduate programs through nine colleges. With more than 14,000 enrollments, our client is a renowned name in the research-intensive academic world.

our client's requirement

The nature of the data and and the number of people that could get affected due to data breach can significantly jeopardize the prestige of this academic institution. Managing and protecting highly confidential information demands robust security measures.

Our client required an easy-to-deploy solution capable of mitigating the insider threat and unauthorized access to confidential information.

Our client has on-premises datacenter. It wanted to have a foolproof security for its application and database servers including network devices. Everyday, hundreds of privileged users access confidential information of the University. Our client wanted to authorize, authenticate, and monitor every privileged access to target devices.

our client's security objectives were:

- To have a secure gateway for accessing critical IT services of the organization
- Securing privileged passwords
- Comprehensive audit trails capability enabling the security team to log daily changes executed in secure and reliable way for daily system/administrative task

the solution

After a thorough technical evaluation, this academic institution chose ARCON Privileged Access Management (PAM). This feature-rich solution would allow our client to strengthen its security posture by providing additional defense layers against unauthorized access.

Objective-1: Our client had a challenge of managing and monitoring multiple privileged accounts. It wanted to ensure only the authorized person has an access to the confidential information. Therefore, they wanted to segregate and restrict privileged user based on job profile and inculcate the practice of user accountability and logical access control.

Solution: ARCON PAM provided a centralized policy engine to authorize privileged user access. The solution enabled our client's IT security team to segregate, elevate and control privileged account users based on their job profiles.

For instance, the access to Business Privileged User accounts for administering HR, faculty, alumni, financial records including IP was segregated and restricted based on individual privileged user's department and role. Likewise, IT Privileged accounts meant for administering network devices were assigned and authorized through Virtual Grouping. ARCON PAM's deepest level of granular level control further ensured that access to privileged accounts were controlled and restricted. Granular control allowed to enforce rule based access to target devices based on time/day/role, in addition to enabling the command filtering capabilities. It also ensured secure third-party access to IT systems. Further, it enabled our client to have a thorough authentication process. Now each access to target systems was made only after a multifactor authentication. The solution enabled our client to attain operational efficiency, apply the principle of Least Privilege; whilst ensuring access on "need-to-know and need-to-do-basis".

Objective-2: Our client required a robust vaulting to securely manage privileged passwords. Previously, our client had an unsecure and inefficient method to manage passwords. Passwords were managed manually in registers. The process was subject to human error and abuse. For instance, if the schedule to change the privileged password was missed, the password remained unchanged, raising the risk of a privileged password misuse.

Solution: ARCON Password Vaulting helped automate the password management process. Our client could now securely generate and change dynamic privileged passwords as per the schedule helping in meeting the desired compliance requirement. The information is encrypted, securely vaulted, and sent to the email address of the privileged user. Further, it also helped in forensic analysis as it enabled the security team to find out who has done what to passwords.

Objective-3: Our client required a detailed analysis of which individual user was accessing which privileged account and for what purpose through comprehensive audit reports.

Solution: ARCON PAM's advanced capabilities such as customized reporting, real-time alerts and analytics enabled the security team to improve upon privileged session monitoring and decision making. The solution allowed our client to capture each and every privileged session in a video and text format in real-time.

conclusion: benefits at a glance

- Formulate a centralized policy engine to authorize privileged user access to target devices
- Apply the principle of least privilege and logical access control
- Enforce granular level control over privileged users
- Control and monitoring of every privileged user and privileged session
- Secure third party access to privileged accounts
- Robust password vaulting
- Comprehensive audit report for each privileged session

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