

CMS IT Services' Holistic Identity and Access Management fortifies critical data access and reduces operations and compliance costs by at least 20% for Fortune Global 500 corporation's associate enterprise



CUSTOMER

A Fortune Global 500 corporation's associate undertaking with a legacy of more than 90 years and operational coverage of over 80% in India with six regional offices and two state-of-the-art manufacturing facilities, the customer engages over 11 lakh dealers and more than 15,000 farmers for 5 iconic brands in the Indian market. The organisation acknowledges data risks and understands that the loss or misuse of sensitive information, or its disclosure to outsiders, including competitors and trading partners, could potentially have a significant adverse impact on the business operations and/or give rise to legal liability. Information Technology and Digitisation have been their prime enablers in business growth.

THE CHALLENGE

The customer had an uncontrolled growth in Privileged User IDs. Privileged users were able to install or remove software, upgrade the operating system, or modify system or application configurations, and have access to files that are not normally accessible to standard users. Root and administrator or superuser accounts (typically used for installing and removing software and changing configuration), service accounts (used for running processes, such as web servers, database servers, and application servers), and system accounts (used for running operating system components and owning related files) are the various kinds of privileged accounts. Privileged users are a necessity, but the power they wield across managed systems makes them a security risk. This prompted the company to introduce a system to continuously monitor their use.

And, to make matters worse, there was no access control on Privileged Users. Access control (or authorization) is the application of constraints on who (or what) can perform attempted actions or access resources that they have requested. With a broken access control unable to regulate Privilege Users, adversaries or insiders would have been able to circumvent existing cybersecurity implementations and mechanisms to gain higher-level permissions, take full control and command, and exploit the business systems. This was a huge open attack surface and an unmitigated risk.

There were no audit trails or log monitoring. Shared passwords and multiple gateways in a dynamic organization structure were detrimental to risk governance and compliance.


The firm wanted to eliminate inefficient and error-prone, manual processes for managing privileged accounts, bring all systems and their privileged users under a single integrated administration, and bring in structured granular role-based privileged access while integrating the entire system into their Security Operations Centre.

THE SOLUTION

To bolster the customer's security posture and Identity and Access Management (IAM) program to protect confidential information, CMS IT delivered a robust Privilege Access Management solution hallmarked by faster deployment, lower set-up cost, and higher efficiency. The solution not only helped the customer ensure robust monitoring of the privileged users, password management, and complete the audit trails of privileged sessions but also, attain the desired compliance level by providing a solution that would seamlessly monitor privileged access.

Before establishing firm Privilege Access Management controls on each target system and linking privileged users with specific devices, CMS IT Services conducted a scan of the customer's user accounts, including privileged users, and all systems in the organization. The scan became the basis for mapping out connections between privileged users and privileged (administrative) accounts on each system. While integrating with Active Directory servers, CMS IT configured custom policies, workflows, and controls in the solution to cater to the defined functional requirements. The solution was seamlessly integrated into the Security Operation Centre's IT and operations' architecture.

BENEFITS




20% reduction in manual operation costs by using a central console for Privileged Account Management



Multi-format Logs and Audit Trails enhanced risk governance, mitigation, and compliance



Interoperable workflow design helped seamless integration with Security Operations Centre






Seamless single-sign-on to mission-critical applications and increased security for access to shared IT equipment brought a significant reduction in managing account credentials and improved the ability to administer systems using individual identities



100% Customer Satisfaction through best practices implementation in Identity and Privileged Access Management



We are a leading provider of System Integration and Managed Services. As one of India's top IT Services firms, we offer an integrated portfolio of products, solutions and services, built around Automation, Cloud, Cybersecurity & Digital. Currently, CMS IT Services has over 6500 employees and serves more than 300 leading enterprises across key industries.

-  www.cmsitservices.com
-  inquiry@cmsitservices.com
-  +91 80 4550 0300