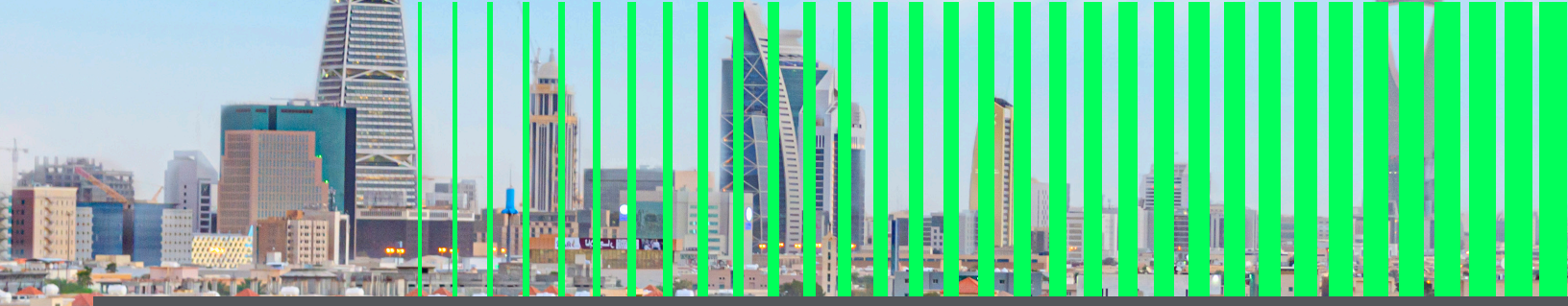

Delinea

SAUDI ARABIA MINISTRY **CASE STUDY**

Enhancing Cybersecurity for a Leading Saudi Ministry

MFA enforcement combined with secure vaulting secures a complex IT environment

Summary

A leading ministry in Saudi Arabia faced mounting cybersecurity challenges, especially in authenticating and managing privileged access to sensitive systems. To address these issues and comply with national cybersecurity mandates aligned with Vision 2030 — a government program launched by Saudi Arabia that aims to achieve increased economic, social, and cultural diversification, the ministry embarked on a digital transformation journey. By first deploying Cerebra mPass Multi-Factor Authentication (MFA) solution, and then integrating Delinea Secret Server for Privileged Access Management (PAM), the ministry achieved a robust security posture that not only fortified access controls but also streamlined administrative processes. This case study illustrates how combining Delinea with Cerebra laid the groundwork for a comprehensive, layered security strategy and great results for the ministry.

Challenges

As part of the security and modernization effort, the ministry has encountered some challenges, including:

1. **Authentication vulnerabilities:** The ministry's legacy authentication processes were inadequate in preventing unauthorized access, especially for high-risk administrative accounts.
2. **Compliance demands:** Adhering to Saudi Arabia's rigorous cybersecurity regulations required state-of-the-art, multi-layered security measures.
3. **Complex access environments:** Managing numerous privileged accounts across a sprawling network posed risks of human error and potential insider threats.
4. **Operational inefficiencies:** Manual authentication and password management processes hindered productivity and increased security risks.

Background

As one of Saudi Arabia's key ministries, the organization manages a vast and complex IT environment that supports thousands of employees and critical regulated and sensitive data. With sensitive systems and privileged accounts spanning multiple platforms, the ministry recognized an urgent need to upgrade its security framework. Initial assessments highlighted authentication weaknesses that left sensitive operations vulnerable. In response, the ministry opted to first enhance identity verification through Cerebra mPass MFA, ensuring that only verified users could access the system before reinforcing access controls with a robust PAM solution.

Solution

Phase 1: Cerebra mPass MFA: Strengthening the first line of defense

Recognizing that secure access begins with robust identity verification, the ministry implemented Cerebra mPass MFA as the foundation of its new security strategy based on several key features, including:

- **Adaptive authentication:** Leveraging contextual user behavior to tailor the authentication process.
- **Push notifications:** Simplifying the login experience while providing strong security via real-time verifications.
- **Broad compatibility:** Seamless integration with existing systems ensured rapid deployment without disrupting operations.

Phase 2: Delinea Secret Server: Fortifying Privileged Access

Once the authentication process was secured as described above, the ministry introduced Delinea Secret Server to safeguard and manage credentials. This PAM solution provided:

- **Automated password management:** Regularly rotating passwords to minimize exposure to breaches.
- **Secure credential vaulting:** Protecting sensitive credentials within a highly secure digital vault.
- **Session monitoring and recording:** Enhancing visibility into administrative activities for compliance and forensic analysis.
- **Discovery and remediation:** Streamlining the identification of unmanaged accounts and mitigating potential risks.

Implementation Process

1. **Planning & assessment:** Detailed evaluations were conducted to pinpoint vulnerabilities in the authentication process and privileged access management.
2. **Phased deployment:** Cerebra mPass MFA was deployed first to establish secure access, followed by the gradual integration of Delinea Secret Server starting with high-risk areas.
3. **Rigorous testing:** Comprehensive testing demonstrated that the new authentication and access controls functioned seamlessly together.
4. **Training & adoption:** IT staff and administrators received targeted training to smoothly transition to the new system and leverage its full capabilities.

Results

A Seamless, unified security ecosystem

The real power of the solution emerged from the integration of Delinea Secret Server with Cerebra mPass MFA. By leveraging SAML and Radius integrations, the ministry ensured that every privileged access attempt required not only verified identity through Cerebra mPass MFA, but also strict adherence to the PAM policies enforced by Delinea Secret Server. This dual-layered approach delivered enhanced security while maintaining operational efficiency for the ministry. Ultimately, the results that the ministry has been able to benefit from include:

- **Stronger security:** Unauthorized access incidents dropped significantly due to the enhanced verification and management processes.
- **Streamlined operations:** Automation of password management and session monitoring reduced administrative overhead and minimized human error.
- **Improved user experience:** The adaptive and user-friendly Cerebra mPass MFA solution elevated the user experience, resulting in higher compliance with security protocols.
- **Supporting regulatory compliance requirements:** The integrated approach has met and exceeded Saudi Arabia's stringent cybersecurity standards, aligning the ministry with Vision 2030.

This case study demonstrates how a strategic, phased approach, beginning with Cerebra mPass MFA, and advancing to a comprehensive PAM solution with Delinea Secret Server, empowered a major Saudi ministry to secure its critical assets effectively. The integration not only bolstered the ministry's security framework but also optimized operational efficiency, setting a benchmark for cybersecurity excellence in the region.

Delinea