WHITE PAPER

SECUREKI

SecureKi Secret Management

www.secureki.com

Introduction

In today's digital age, data is one of the most valuable assets for any organization. This includes sensitive information such as login credentials, financial data, customer information, and intellectual property. As the amount of data generated and stored by organizations grows, it becomes increasingly challenging to manage and secure this data. This whitepaper discusses a secret management solution that can help organizations manage and secure their sensitive data effectively.

Secret management is essential for organizations of all sizes and industries in today's digital landscape. As businesses increasingly rely on technology to store and process sensitive information, the risks associated with compromised secrets have become more significant. Data breaches can result in financial losses, reputational damage, legal action, and compliance violations.

Effective secret management is essential for mitigating these risks and ensuring that sensitive information remains secure. Proper secret management practices help organizations to:

- Reduce the Risk of Data Breaches: Effective secret management practices can help reduce the risk of data breaches by ensuring that sensitive information is stored securely and only accessible to authorized users and systems.

- Meet Compliance and Regulatory Requirements: Many regulations, such as GDPR, HIPAA, RMIT, and PCI DSS, require organizations to protect sensitive information, including secrets. Effective secret management practices can help organizations comply with these regulations and avoid fines and other legal action.

- Improve Operational Efficiency: By automating secret management processes and providing centralized control over secrets, organizations can improve operational efficiency and reduce the risk of human error.

- Enhance Security Controls: Effective secret management practices can enhance an organization's security posture by providing stronger access controls, encryption, and monitoring capabilities.

Challenges in Secret Management

a. Lack of visibility into secrets: One of the primary challenges organizations face in managing secrets is a lack of visibility into where secrets are stored and who has access to them. This can occur when secrets are stored in different systems and applications or when they are managed manually. Without clear visibility into secrets, organizations may struggle to detect and respond to security incidents such as unauthorized access or data breaches.

b. Difficulty in detecting unauthorized access: Another challenge in secret management is detecting unauthorized access to secrets. Attackers can use various techniques to obtain unauthorized access to secrets, such as phishing, malware, and social engineering. Organizations may struggle to detect these attacks, particularly if they lack the necessary security controls or their monitoring and alerting systems are not configured correctly.

c. Limited control over secrets: Organizations may face challenges controlling access to secrets, particularly in complex environments with many different users and systems. Without clear control over secrets, organizations may struggle to ensure that secrets are only accessible to authorized users and systems. Additionally, if secrets are not properly controlled, they may be inadvertently disclosed, resulting in a data breach.

d. Human error and negligence: Another challenge in secret management is the risk of human error and negligence. Humans may accidentally disclose secrets, forget to rotate secrets, or fail to follow best practices for secret management. This can occur due to a lack of training, insufficient awareness of security risks, or simply carelessness. Human error and negligence can result in data breaches and other security incidents.

e. Compliance and regulatory requirements: Finally, organizations may face challenges managing secrets due to compliance and regulatory requirements. Many regulations, such as HIPAA, GDPR, and PCI DSS, require organizations to protect certain types of sensitive data, including secrets. Failure to comply with these regulations can result in fines, legal action, and damage to an organization's reputation. However, compliance with these regulations can be challenging, particularly in complex environments with many systems and applications.

Secret Management Tools & Technologies

Secret management tools and technologies help organizations securely store, manage, and control access to secrets. These tools can manage various types of secrets, including passwords, keys, certificates, and API tokens.
Here are some examples of secret management tools and technologies:

Password Managers: Password managers allow users to store and manage passwords for different applications and services securely. Password managers can also generate strong and unique passwords, reducing the risk of password reuse or weak passwords.

Key Management Systems: Key management systems are designed to store and manage encryption keys to protect sensitive data securely. Key management systems can also generate and rotate keys automatically, ensuring that encryption keys are changed regularly to reduce the risk of compromise.

Secrets Management Systems: Secrets management systems are designed to manage all types of secrets, including passwords, keys, certificates, and API tokens. Secrets management systems provide centralized control over secrets, making managing access and monitoring usage easier. These systems can also automate the process of generating, rotating, and revoking secrets.

Cloud-Based Key Management Services: Cloud-based key management services are offered by cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. These services allow users to manage encryption keys securely in the cloud. Cloud-based key management services can also manage other types of secrets, such as API tokens.

When evaluating secret management tools and technologies, organizations should consider the following factors:

Security: Secret management tools and technologies must provide strong security controls to protect secrets against unauthorized access and disclosure. This includes encryption of secrets at rest and in transit, access controls, and auditing and monitoring capabilities.

Integration: Secret management tools and technologies must integrate with existing systems and applications to ensure that secrets can be easily managed across the organization.

Scalability: Secret management tools and technologies must scale to meet the organization's needs, particularly as the number of secrets and users grows.

Usability: Secret management tools and technologies must be easy to use and manage to ensure that users can effectively and efficiently manage secrets.

Best Practices in Secret Management

The best practices that organizations can adopt to manage secrets effectively:

- Centralized Management of Secrets: Effective secret management requires centralized control over the storage and access to secrets. A centralized approach allows for easier management and monitoring of secrets, reducing the risk of unauthorized access or disclosure. Organizations should use dedicated tools or services designed for secret management, such as password managers, key management systems, or secrets management systems.

- Encryption and Decryption of Secrets: Encryption is a crucial aspect of secret management. Sensitive information, including secrets, should be encrypted at rest and in transit. Encryption helps to protect secrets from unauthorized access, even if they are compromised. The decryption of secrets should only occur when necessary, and access to decrypted secrets should be strictly controlled.

- Access Controls and Permissions: Access controls and permissions are essential for managing secrets effectively. Access to secrets should be granted on a need-to-know basis, with only authorized individuals or systems allowed to access them. Organizations should implement role-based access controls, which grant permissions based on the user's role within the organization. Furthermore, access to secrets should be granted on a least-privilege basis, meaning that users are only granted the minimum permissions necessary to perform their job functions.

- Regularly Rotating Secrets: Regularly rotating secrets, such as passwords and encryption keys, is a best practice for secret management. Rotating secrets can help mitigate the risk of unauthorized access, particularly if a secret has been compromised. Organizations should set up automated processes for regularly rotating secrets, reducing the risk of human error or oversight.

- Monitoring and Auditing of Secret Access: Organizations should regularly monitor and audit access to secrets. This helps to identify potential security breaches and ensure that access is granted only to authorized individuals or systems. Monitoring and auditing can also provide valuable insights into user behavior, helping organizations to identify areas where additional training or security controls may be needed.

- Automated Secret Management: Automated secret management processes can help reduce the risk of human error and ensure that secrets are managed consistently and effectively. Organizations should use dedicated tools or services designed for secret management to automate processes such as secret generation, rotation, and revocation

Effective secret management requires a comprehensive approach that includes centralized management, encryption, access controls, regular rotation, monitoring and auditing, and automation. By adopting these best practices, organizations can better protect their sensitive information, reduce the risk of data breaches, and meet regulatory and compliance requirements.

Case Studies

Below are examples of organizations in South Korea that have implemented effective secret management practices and how it has helped them to enhance their security posture.

KB Kookmin Bank

KB Kookmin Bank is a subsidiary of KB Financial Group. It is one of the top banks in South Korea. It was founded in 1963, around 59 years ago. Its headquarters is located in Seoul. It has over 1,100 branches nationwide, serving about 30 million customers. It also has 3,000 ATMs all over the country.

KB Kookmin Bank has implemented a comprehensive secret management strategy to protect sensitive information. The company uses a secrets management system solution that allows them to securely store and manage privileged account credentials, certificates, and other sensitive information. The system provides strong access controls, auditing capabilities, and automated secret rotation, which has helped KB Kookmin to reduce the risk of unauthorized access to sensitive information and meet compliance and regulatory requirements.

Shinhan Bank

Shinhan Bank is one of the top banks in South Korea. It was established in the year 1982, around 35 years ago. They have about 13,400 employees working here. They have a presence in over 19 countries. Only in South Korea, Shinhan Bank has over 900 offices. Shinhan Bank is the main subsidiary of Shinhan Financial Group.

Shinhan Bank has implemented an effective secret management strategy and solution to protect its digital assets. The company uses a secrets management system that allows them to securely store and manage secrets like API keys, database credentials, and certificates. Vault provides strong access controls, auditing capabilities, and automated secret rotation, which has helped Shinhan Bank to reduce the risk of data breaches and meet regulatory requirements.

NongHyup Bank

NongHyup Bank (NH) is a subsidiary of NongHyup Financial Group. NongHyup Financial Group is owned by the National Agricultural Cooperative Federation (NACF). NH Bank has around 1200 branches in South Korea, focusing on commercial banking services.

NongHyup Bank has implemented an effective secret management strategy to protect its customers' financial information. The company uses a secrets management system solution that allows them to securely store and manage privileged account credentials and other sensitive information. The system provides strong access controls, auditing capabilities, and automated secret rotation, which has helped NongHyup Bank to reduce the risk of unauthorized access to sensitive information and meet compliance and regulatory requirements.

Overall, implementing effective secret management practices is critical for the financial services industry to protect their customer's financial information and mitigate the risk of data breaches. By adopting best practices like encryption, access controls, regular rotation, and monitoring and auditing, organizations in the FSI sector can better protect their sensitive information and enhance their security posture.

Conclusion

The white paper on secret management emphasizes the importance of implementing effective secret management practices to secure an organization's digital assets. The paper identifies various challenges organizations face in managing secrets, such as a lack of visibility, difficulty detecting unauthorized access, limited control, human error, and compliance requirements. This paper discusses several best practices organizations can adopt to effectively manage secrets, including centralized management, encryption, access controls, regular rotation, monitoring and auditing, and automated secret management.

This paper also highlights the importance of implementing these best practices to reduce the risk of data breaches, protect sensitive information, and meet regulatory and compliance requirements. It also provides examples of organizations, such as KB Kookmin Bank, Shinhan Bank, and NongHyup Bank: that have implemented effective secret management practices and have improved their security posture as a result.

To conclude, this white paper emphasizes that effective secret management is critical for securing an organization's digital assets and mitigating the risk of data breaches. By implementing best practices and using modern secret management tools and technologies, organizations can better protect their sensitive information and maintain the trust of their customers and stakeholders.