Cloud encryption and secrets management for cloud-based digital services

Consultancy and support for handling highly sensitive information in the cloud securely. Adhering to legal and regulatory frameworks for data, including data sovereignty requirements. Cryptography and secrets management are handled by our experienced security experts, ensuring data is protected appropriately without teams having to manage complex cryptography.

As part of planning and implementation efforts, careful consideration must be given to the secure storage, management, operation and use of secrets and encryption within the selected cloud provider. Within the Shared Responsibility Model, users are responsible for the security of their own data within the cloud and our service helps to achieve this.

Our service is recommended for any public sector organisation seeking to adopt, or already using, cloud services. Our service provides strong security protection for secrets such as credentials, encryption keys, access tokens, and other sensitive data that must be carefully protected through controlled access, with reliable auditing mechanisms to detect malfeasance.

Our consultants analyse existing designs and/or implementations and identify gaps in the security surrounding these sensitive assets. Using this gap analysis, we design a secrets management solution that defends against the threats posed to the organisation. We go beyond the technical controls, examining user interaction and offline processes that may have an impact on the secure handling and management of secrets, to provide a holistic approach to security.

Our security consultants have in-depth, hands-on experience and expertise in designing, implementing and operating secrets management solutions in a variety of environments, bringing industry experience from a wide range of sectors including regulated industries such as finance and banking.

Features

- Strong policy definitions to control access to secret artefacts
- Audit log of activity related to access, modification of secrets
- Supports high availability deployments
- Cloud agnostic and supports multi-cloud deployments

- Supports automatic key rotation
- Powerful and flexible capability to revoke access in an emergency
- Integrates with existing identity providers
- Integrates with existing logging platforms and SIEM solutions
- Full API for custom workflows, integrations and automation
- Effective knowledge and skills transfer to teams

Benefits

- Delivered by expert security consultants with government experience and clearance
- Able to respond rapidly in case of an emergency
- Reduces the risk of leaking sensitive data
- Keeps secret material within secure environments
- Thoroughly documented threat model and risk analysis
- Reduces operational cost through secure self-service by delivery teams
- Supports migration paths from existing secrets management systems
- Supports zero downtime deployments and migrations
- Removes the need for super-admin with access to secret material

Our approach to cloud encryption and secrets management

Equal Experts consultants are highly experienced in modern agile and lean practices. They bring with them experience of a wide range of business domains and industries, including many industries that face strong regulation around security, such as banking and finance. They excel at communicating with senior stakeholders and delivery teams across the organisation, using plain language that is easily understandable to non-security specialists.

Our approach aligns well with the five core functions of the NIST Cybersecurity Framework:

- Identify
- Protect
- Detect
- Respond
- Recover.

Our consultants work closely with a client to identify and establish a shared understanding of the cybersecurity risks surrounding encryption and secrets management in cloud environments, with particular emphasis on the specific environment. This is driven from a

wide variety of inputs, such as the business context, delivery approach, resources available, as well as any existing risk management policies created by the organisation.

From this shared understanding, we create a design and develop an encryption and secrets management solution to protect these sensitive assets within the cloud environment. This is driven by mature security threat modelling exercises that point towards areas of risk, which our consultants then use to define and document suitable controls to mitigate those risks. We take a holistic approach to security, resulting in comprehensive coverage of security concerns beyond just the technical controls available.

We also consider human factors in security, creating usage patterns that fit with real-world scenarios to ensure that security models are fit for purpose and pragmatic.

Based on the system design and the environment in which it operates, we determine appropriate activities to detect a cybersecurity incident. Our consultants are experienced at integrating the encryption and secrets management solution with existing monitoring tools, providing audit feeds of all activity within the system. From these audit feeds, we implement monitoring and alerting events to notify of any abnormal patterns of behaviour within the system and facilitate a rapid response.

Our consultants bring significant expertise in helping to respond in the event of a security incident. We define suitable incident response procedures that can be followed when an incident has been detected. However, we are also happy to use any existing incident response plans the organisation may already have. The incident response procedures include clear guidance and activities that should be followed to limit the damage that can be caused in the event of a security incident, and to coordinate the teams involved in the response.

Finally, we provide clear steps to help recover after an incident. Our security consultants provide guidance on how to use the audit event data to establish the scope of the incident and use fine-grained controls to reset or rotate any secrets that may be at risk, without impacting those that are known not to have been compromised.

Examples of cloud secrets management in action

We have previously implemented a cloud encryption and secrets management solution for a major UK government department, which operates a large microservices architecture running in the cloud, supporting hundreds of microservices.

A team of Equal Experts security consultants followed the approach outlined above in order to deliver significant improvements to the secure management of secrets in the cloud, while maintaining the department's excellent track record of high availability and frictionless deployments to production.

Our consultants analysed the existing approach to secrets management and identified areas of risk that needed to be addressed in order to satisfy the department's security requirements. We then proposed a new secrets management system with clearly defined roles and responsibilities and self-service capabilities provided to delivery teams, ensuring that this new design satisfied the requirements identified in the previous exercise. We performed multiple threat modelling exercises to validate the design and ensure that there were no gaps in the security model.

Our team led the delivery of this new secrets management system, coordinating the work among multiple participating teams all working on the government department's platform, including infrastructure, telemetry, build and deployment tooling, and many others.

We faced several challenges in this project, particularly:

- The government department had more than 50 teams working in geographically dispersed locations that all needed to use the new secrets management solution
- The platform was already running many hundreds of microservices in production and required zero-downtime deployments and minimal disruption to the ongoing development of microservices

A phased delivery approach was adopted to bring security benefits as early as possible while minimising the impact on delivery teams building microservices on the platform and maintaining zero-downtime deployments. This ensured that we were able to replace the legacy approach to secrets management with the new and secure solution without any service or platform downtime.

Our security consultants leveraged existing platform tools that had been built internally in order to dynamically generate fine-grained access control policies for the numerous teams and microservices running on the platform. These policy generation tools consumed data from internal APIs to identify the services running in each environment and the teams that owned them, ensuring that teams were only given permission to configure secrets for their own services. This allowed us to generate policies dynamically in response to various events, such as the creation of a new microservice. This gave the department flexibility in

responding to rapid changes in the environment and provided a solid foundation for automating the creation and testing of access control policies.

As a result of this new solution:

- Teams are able to manage the secrets for their own microservices in all environments, without having to coordinate this through a central team. This allows the department to maintain its alignment with our DevOps philosophy, ‘you build it, you run it’. It ensures the people with the best knowledge of any given service - those that develop and operate it - are able to manage all aspects of their service without bottlenecks being introduced unnecessarily.
- Secrets are now more securely controlled, removing numerous single points of compromise in the previous system. The platform teams no longer have access to secrets for any services, and service delivery teams can give strong security guarantees on the confidentiality and integrity of their secrets to their stakeholders.
- Secrets management is now a completely transparent process. All of the work behind the new solution (e.g. requirements, threat models, security controls, access control policies, roles and responsibilities, etc.) is open for anyone within the department to view and contribute to - ensuring that any security issues can be brought to light as quickly as possible.
- Strong audit trails exist for every activity in the secrets management system, giving the department visibility it didn’t previously have. This allows them to identify when unusual behaviour takes place and respond accordingly.
- The department is able to respond far more rapidly to security incidents now than they were before, and with more data to support any investigations that may follow.