AWS Security Checklist Report

AWS Security Checklist - AWS Elastic Beanstalk

Item	Description
Use IAM roles to control access to AWS Elastic Beanstalk resources	Using IAM roles enables you to control which users and applications have access to AWS Elastic Beanstalk resources and what actions they can perform.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit network access to Elastic Beanstalk resources	Limiting network access helps prevent unauthorized access and limits the impact of security breaches.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your Elastic Beanstalk environments.
Regularly update your Elastic Beanstalk environments and their components	Regularly updating your Elastic Beanstalk environments and their components helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Implement function-level access control	Use AWS Identity and Access Management (IAM) policies to control access to your Elastic Beanstalk environments. Restrict access to only the actions and resources that are necessary for the environment to perform its intended actions.
Implement secure deployment practices	Implementing secure deployment practices helps ensure that your Elastic Beanstalk environments are deployed securely and that your applications are not vulnerable to security breaches.
Use WAF to protect against web-based attacks	AWS WAF (Web Application Firewall) can be used to protect against common web-based attacks such as SQL injection and cross-site scripting.
Implement access and authentication controls for applications	Implementing access and authentication controls for your applications helps ensure that only authorized users can access sensitive information or perform privileged actions.
Implement data protection controls for applications	Implementing data protection controls for your applications helps ensure that sensitive information is protected from unauthorized access or disclosure.