Cloud Security for Bromma SMS.

A BROMMA WHITE PAPER

SEPTEMBER 2023

BROMMA

A Tradition of Innovation

CONTENTS

Cloud Security for Bromma Spreader Monitoring System.

Executive Summary.

Bromma Spreader Monitoring System (SMS) is a tool for condition based monitoring of your spreader fleet that gives you an easy to use overview of your spreader health and other key statistics. Enabling you to take action on real-time information, that will help improve your overall operations immediately. Bromma SMS turns data into spreader health analysis with highlighted actionable recommendations and solutions.

As Bromma SMS collects, stores, and processes data critical to its customers' operations, it is of utmost importance for us at Bromma, to make sure that your data stays secure.

Bromma SMS has been built with information security in mind from the start. This whitepaper explores the security decisions and processes made to ensure that data is and remains secure.

1 Introduction to Cloud Security and Bromma SMS architecture.

Bromma SMS is a cloud-native application built for processing operational IoT data on a large scale. To support the performance, scalability, and security expectations of our customers, the application is built on Amazon Web Services (AWS) using some of the most advanced capabilities available on AWS.

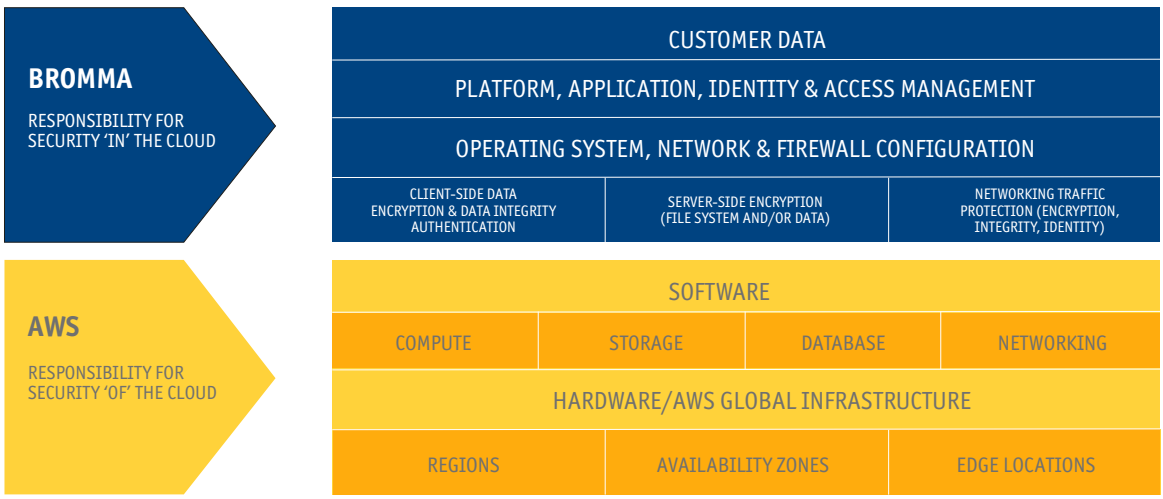
Bromma SMS takes advantage of **the shared responsibility model** of AWS where security and compliance activities are shared between AWS and Bromma. The model is described as follows:

...Bromma SMS takes advantage of the shared responsibility model of AWS where security and compliance activities are shared between AWS and Bromma.

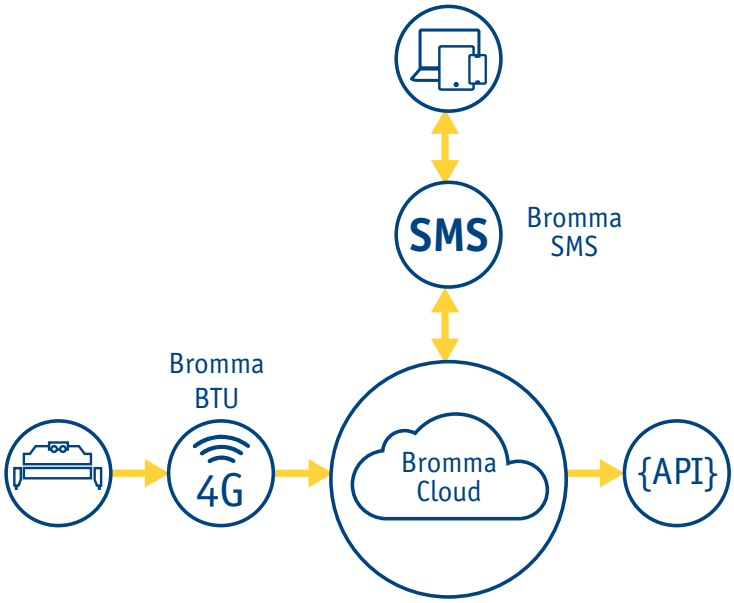
"Security of the Cloud" **-** AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. AWS operates, manages and controls the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the service operates.

"Security in the Cloud" – Bromma's development and operations teams are making sure that the services and technologies in the cloud are taken into use, integrated, and operated securely. This includes all the application components that Bromma SMS consists of.

Amazon data centres are designed and built with high security requirements in mind. Security is considered in multiple layers from the physical perimeter to infrastructure, data, and environmental aspects. As a result, the most highly regulated organisations in the world trust AWS every day.



A high-level architecture of Bromma SMS is as follow:



Key components in the architecture are:
Bromma Telematic Unit (BTU), the device installed on spreaders that reads operational data and transmits that data to the Bromma Cloud.
Bromma Cloud, the cloud platform used to store and process data from a spreader for operational analytics purposes.
Bromma SMS, the cloud application that Bromma customers use to access and analyse operational data from their spreaders.

Bromma SMS and Bromma Cloud consists of software and services on the Amazon Web Services (AWS) cloud platform, taking advantage of high-quality AWS technologies and services as much as possible. These include as an example:
Amazon Elastic Container Service (Amazon ECS) for orchestrating container workloads in the cloud.
Amazon Relational Database Service (Amazon RDS) for storing and processing data in the cloud.
Amazon Simple Storage Service (Amazon S3) for storage service with industry-leading scalability, data availability, security, and performance.

In addition to Amazon Web Services, Bromma SMS includes custom user access management system where each user can only access data they are authorised to. The user's identity is verified using multi-factor authentication. Communication is protected using TLS encryption. Secure authentication is essential for enterprise applications.

2 Security design.

It is our duty to protect Bromma SMS customer's data and business. This has been our guiding principle in creating the security design for our cloud-based offering. We believe that we are able to offer the best service for Bromma customers regarding the reliability and security of condition based monitoring and spreader data analytics.

...It is our duty to protect Bromma SMS customer's data and business. This has been the guiding principle in creating the security design for our cloud-based offering.

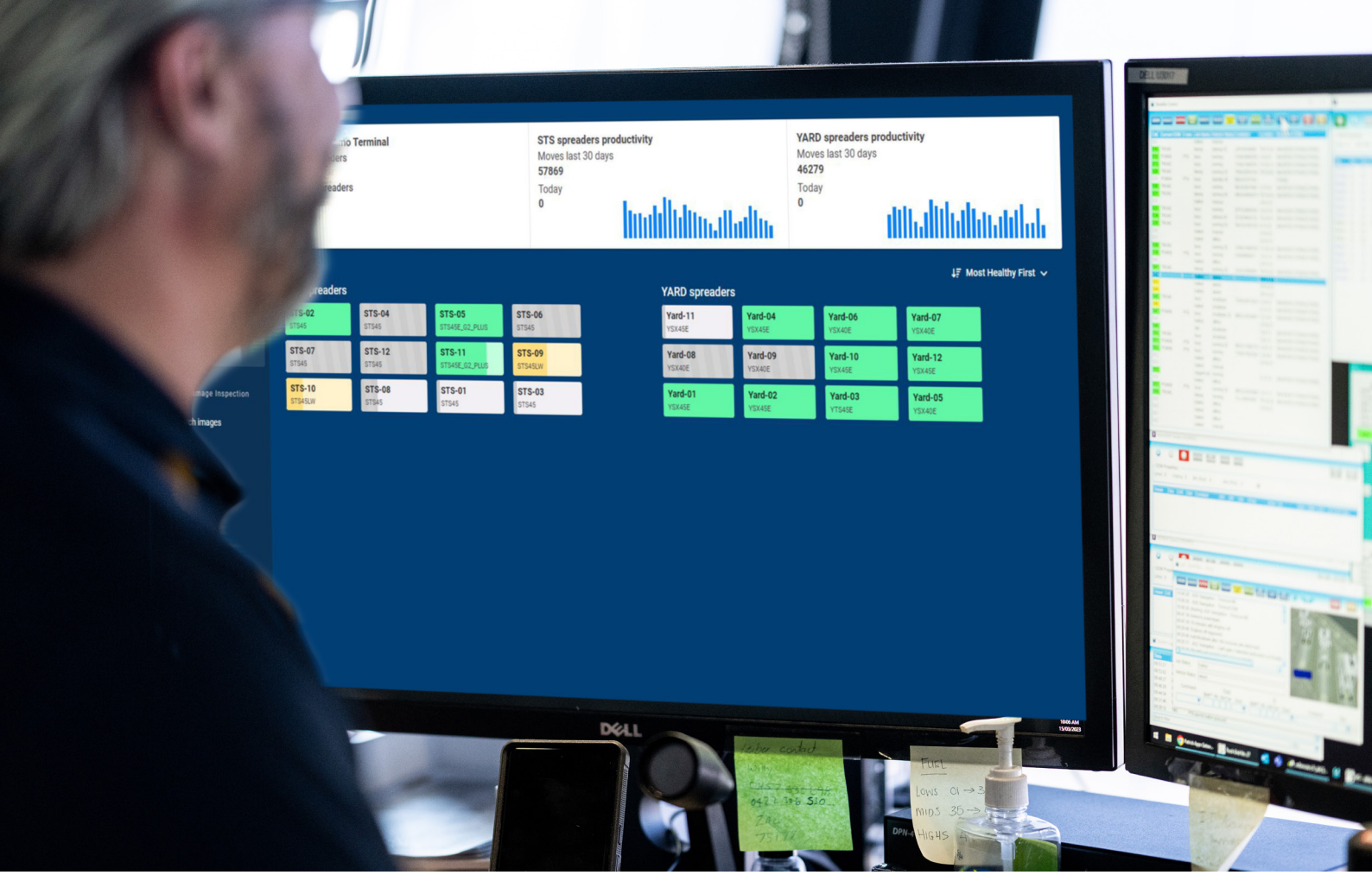
The Bromma SMS application and Bromma Cloud platform are built on serverless computing, microservices, and containerisation. This design approach makes the application inherently more **resilient, scalable, and secure** than traditional monolith systems. We believe that this design approach and cloud-native use of Amazon services provides the best possible technology solution to our customer's needs.

The Bromma SMS application and Bromma Cloud platform is founded on a resilient architecture based on Docker containers. The containers are run on Amazon Elastic Container Service for performance and security. As a containerised application, Bromma SMS is more capable of dealing with cyberattacks than a traditional web application design. A possible breach in a microservice container does not inherently affect the entire system as in monolith designs. Instead, this allows our security operations to **detect the misuse and respond accordingly** before the attacker is able to move laterally to access confidential data storage or sensitive functionality.

The Bromma data platform contains many internal services and APIs. These are never exposed to the public networks. To protect these APIs, they are placed on Amazon Virtual Private Clouds (VPC) making the pools of computing and storage resources logically isolated from other pools and the public networks.

The infrastructure of the Bromma SMS application and platform is expressed using code instead of through manual processes. This allows us to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for Bromma SMS. This approach called Infrastructure as Code (IaC) is considered the best practice in building secure, auditable platforms in the cloud.

Applications need password, API keys, and other secrets throughout their lifecycle. As a design principle, our code or configuration never contains passwords or other secrets [hidden files] that a criminal hacker might gain access to. Instead, we use the **AWS Secrets Manager**



service that helps us protect those secrets. With Secrets Manager, applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

The APIs of the Bromma Cloud are protected using authentication. Authentication is used to ensure that access to APIs are limited to authorised applications. Throttling prevents malicious applications from brute forcing access credentials or consuming excess amounts of capacity or bandwidth from the platform. Bromma SMS uses Amazon Elastic Load Balancing to provide resilience and high availability against potential network attacks that would otherwise degrade the performance of the application.

Services used by the Bromma SMS application are located in Amazon's European data centres. This is to ensure our applications and data stored benefits from the European data protection regulation.

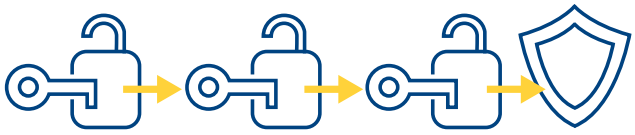
The following chapters will take a close look at some of the security aspects of Bromma SMS and Bromma Cloud.

3 Authentication.

One of the security basics on any application is getting the authentication right. Bromma SMS includes a custom user access management system where each user can only access data they are authorised to.

The application also provides API access for integrating directly to the Bromma Cloud. We protect all the application APIs using OAuth2.0 standard protocol.

The Bromma Telematic Unit (BTU) is the device by which data is collected from the Bromma spreader and transferred to the Bromma cloud platform. Bromma Gateways are authenticated by a MQTT data broker using a combination of a device certificate and key before being allowed to transmit data.



4 Encrypting data in transit.

Encrypting data in transit is a way of protecting it from malicious access during transmitting. The Bromma SMS user interface and BTU Gateway use the industry standard TLS encryption for protecting confidentiality and integrity of all communications.

5 Encrypting data at rest.

Encrypting data at rest is an important mechanism to protect data while it is stored. Encryption gives us confidence that anyone can't access the data by circumventing Bromma Cloud APIs such as by breaching a data centre. We use Amazon-provided data encryption in both our storage services; in S3 storage and in RDS database.

6 Secure coding.

We take software quality and security seriously and have taken into use procedures, tools, and training to achieve as high a standard on both as possible. Bromma has a modern DevOps culture and ways of working across various teams, allowing us to take advantage of up to date best practices when it comes to building security into our applications.

The Bromma DevOps team identifies beforehand planned changes that will have a security implication. Those changes are subjected to threat modelling. Threat modelling is a procedure for discussing the security requirements and planned design of the change so that there is no oversight in the security features.

...A key activity in coding is to keep track of vulnerabilities in open source libraries included in a project.

Source code changes are subjected to code reviews. This is a practice where another developer will review the committed change to verify its well-formedness and validity before the code is integrated into the main build. Code review practices enable us to detect human mistakes and bugs before the code is ever made part of the product.

A key activity in coding is to keep track of vulnerabilities in open source libraries included in a project. The DevOps team at Bromma uses a commercial tool to track 3rd party libraries and their licenses, and alert in case insecure dependencies are detected. This way we can be sure that any known insecure component will be replaced from our application as soon as possible.

Our DevOps team is trained and up to date on secure coding practices and design patterns. For example, they take advantage of OWASP Top 10 projects' documentation and guidance to make sure that Bromma SMS will not suffer from that kind of critical web application vulnerabilities.

7 Security testing.

Security testing is the mechanism which ensures that there are no vulnerabilities, configuration mistakes, or otherwise unwanted security exposure. Security testing for Bromma SMS takes place systematically and regularly.

Firstly, the build and integration pipeline for various software components of Bromma SMS have automated testing included. This automation helps us detect potential mistakes as the software is being developed. Making sure any potential mistakes are detected and remedied much before the affected version is ever deployed in production.

Secondly, we undertake a regular review using AWS Well-Architected Framework to detect areas where we need to improve. This framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimisation. By applying this structured approach, we ensure our way of making use of Amazon services follows the best practices and guidance available.

8 Security operations.

Security operations are the set of processes and procedures to ensure that the production environment stays protected. An essential element of security operations is privileged access management. Privileged or administrative access must be shielded from attackers. With Bromma SMS, we follow Amazon best practice guidance in organising our AWS subscription and privileged accounts.

As the application uses the infrastructure as code technology, security operations benefit from being able to detect any unexpected changes on the services. This feature, called drift detection, will alert Bromma SMS security operations staff in case there are unexpected changes on the services. For example, these kinds of changes could happen due to criminal hacking or operational mistakes. Because of drift detection the changes will be caught and investigated as they occur.

At times, there are security patches available to operating systems, libraries, and other components at the foundations of Bromma SMS. Making sure these patches are installed in production as soon as possible is a basic security posture in enterprise applications. Our security operations team monitors used components for patches and initiates testing and roll-out activities based on availability.

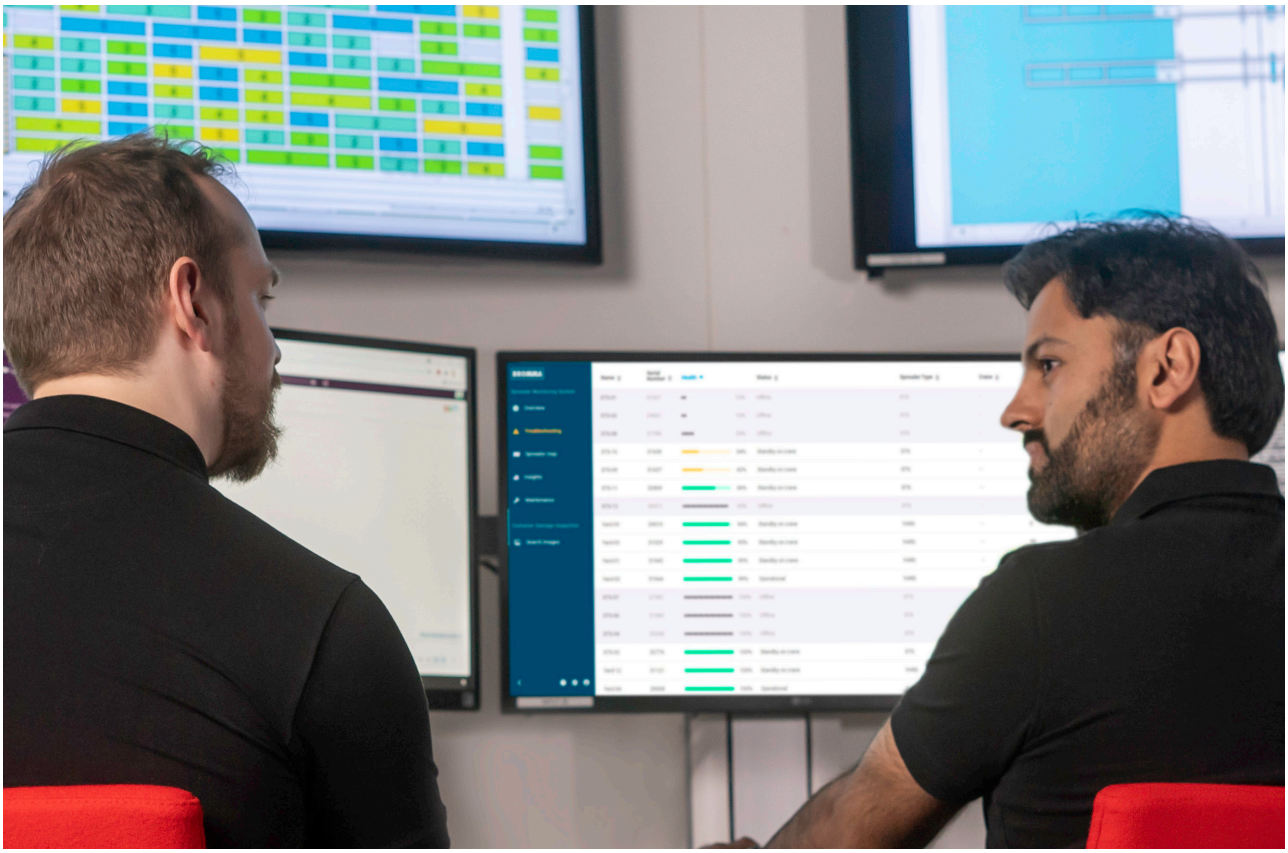
Our security operations use Cloud Security Agents to continuously monitor our cloud workload for malicious activity and unauthorised behaviour. The agents uses anomaly detection, and integrated threat intelligence to identify and prioritise potential threats. This enables our operations to detect malicious behaviour and act appropriately to respond to emerging incidents.

9 Logging and monitoring.

Logging and monitoring security events provide valuable input and enabled security operations. Additionally, they help to identify misuse and attacks against the application and data. In Bromma SMS, we produce numerous logs from all sort of events, including security events, such as authentication and access. All authentication activities on our APIs, access to S3 storage, and RDS database access are logged and stored.

Bromma SMS uses **Amazon CloudWatch Service**, which enables us to collect, access, and correlate this data our AWS resources, applications, and services. CloudWatch helps us gain system-wide visibility and quickly resolve issues.

In addition to user activities, we are logging privileged access, also known as administrative access, and changes made to our configurations and services. This audit trail gives us confidence is our ability to detect misuse of our privileged accounts and react to harmful changes in time to mitigate damages.



10 Data backups.

Making sure that business critical operational data is protected from a sudden loss is a key information security activity. Since Bromma SMS is natively built on cloud technologies, we are able to leverage the automated and powerful data and system backup services provided by Amazon. All data on Bromma SMS and Bromma Cloud are automatically protected against loss due to unlikely events of system or storage malfunction. Should the unexpected failure occur, the same services allow us to restore snapshots and backups automatically minimising the impact of any outage.

...Making sure business critical operational data is protected from a sudden loss is a key information security activity.

11 Personal data protection.

Bromma is committed to protecting the personal data of its customers and users. We follow the European General Data Protection Regulation in all our operations and services. In Bromma SMS, personal data processing activities are limited and low risk. Personal information processed is limited to the name and email addresses of our customers with access to the Bromma SMS application.

12 Product security incident response process.

Bromma and Cargotec have a product security incident response team (PSIRT) for managing security incidents related to its products across business areas.

There are several sources that might lead to a product security incident process being started:

- A customer contact
- An alert from Bromma SMS security monitoring
- An internal security assessment finding
- A contact from a security researcher
- Public disclosure of a security issue.

As a product security incident response process is initiated, the first step is to assess the magnitude of the finding and start activities warranted by the situation. The following topics are always a priority for Bromma and Cargotec in a security response:

- Making sure people are safe. Any threat that would put people's health in danger takes priority.
- Understanding the scope of the affected products and services. In order to initiate appropriate activities to remedy the situation, such as building and deploying a software patch, we will swiftly analyse the root cause of the matter and technologies involved. This will also help us to pinpoint which customers might be affected.
- Understanding the scope of the affected customers. It is our duty to make sure that our customers data is secure, and they will have continued trust in us. When it comes to our security and incidents, we commit to being open and timely when communicating any relevant information to our customers.

In any questions regarding Bromma and Cargotec product security, please contact Bromma customer support.

REFERENCES

Amazon Web Services: Shared Responsibility Model
https://aws.amazon.com/compliance/shared-responsibility-model/

Amazon Web Services: Overview of Security Processes
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Amazon Data Center Security
https://aws.amazon.com/compliance/data-center/data-centers/

AWS Secrets Manager
https://aws.amazon.com/secrets-manager/

AWS Well-Architected Framework
https://aws.amazon.com/architecture/well-architected/

OWASP Top 10, version 2021
https://owasp.org/Top10/

www.bromma.com
sales@bromma.com

BROMMA

A Tradition of Innovation