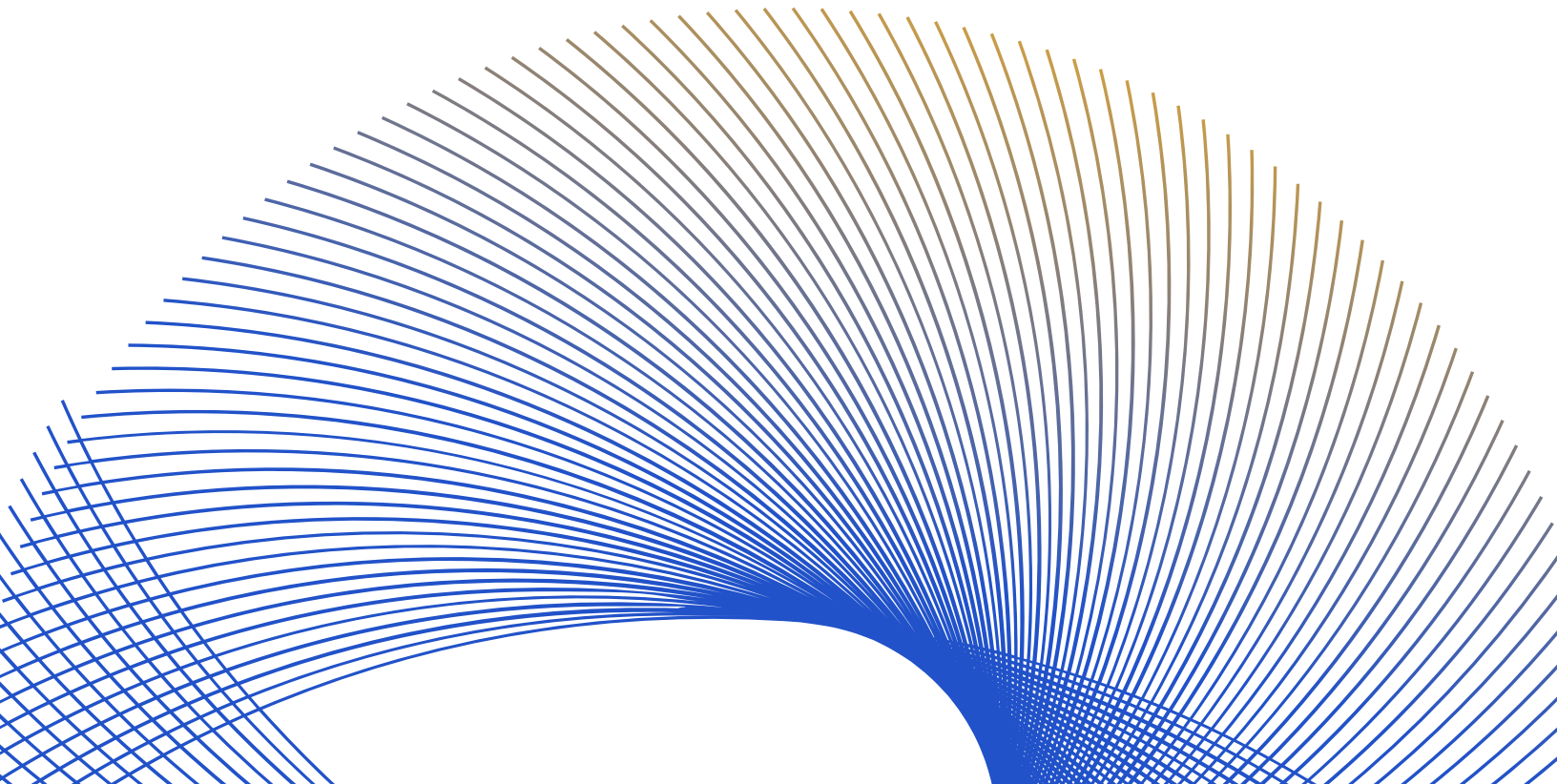
ThreatModeler® | aws

5 Steps to Building a Scalable Threat Modeling Program for AWS

Contents



Introduction

As technology evolves, companies face the challenge of making decisions regarding the security of their data. Cloud computing has experienced rapid growth in the last few years, despite the lack of knowledge on cloud adoption and the process behind it. According to Forbes, digitally transforming enterprises (63%) is the leading factor driving greater public cloud engagement or adoption followed by the pursuit of IT agility (62%). The main reasons organizations are moving to the cloud are: flexibility, reduced costs, scalability and improved collaboration. Cloud services give CIOs and IT directors the flexibility to scale their cloud capacity, giving organizations a competitive advantage over their competitors. Cloud computing significantly saves on expenses required from traditional computing reducing overall costs and allowing teams to access data from anywhere having full visibility of their collaborations.

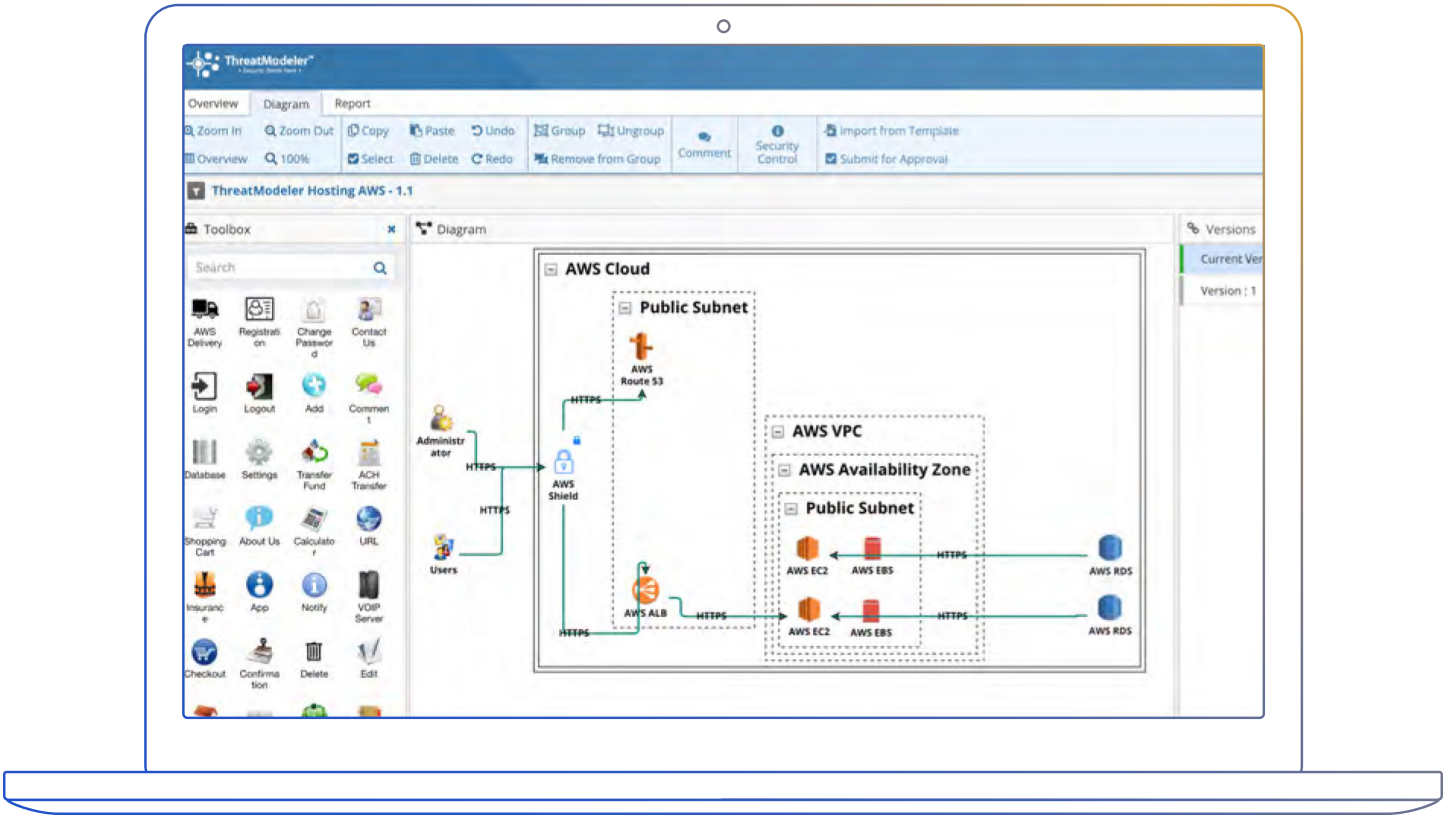
Amazon is the major player on the cloud market, establishing a secure cloud services platform – Amazon Web Services (AWS) — that offers compute power, database storage, content delivery and other features. Other key cloud computing platforms in the game are Azure, considered the second dominant player, followed by Google, Oracle and few others.

Although many organizations are making use of these platforms, they are still hesitant to move to cloud services without being aware of the security concerns. The Cloud Security Spotlight Report revealed that “90% of organizations are very or moderately concerned about public cloud security”. Some of the main security concerns in a cloud are: reduced visibility and control, lack of understanding of shared responsibility, lack of tools and technologies and lack of knowledge or SME. With all these mega breaches, the security of data in the cloud is a concern at 61% of companies.

Lift & Shift or Design Cloud Native with Security in Mind

Even though organizations are moving to the cloud with higher conviction, there are still lingering concerns around the migration to the cloud. The limited visibility into the controls securing cloud infrastructures and lack of knowledge of security threats in the cloud is a leading factor in some organizations still relying on traditional data centers.

This issue will keep progressing until there is a better understanding of the overall attack surface around the cloud eco-system and the relevant threats that may lead to security and privacy issues. Threat Modeling helps cloud architects analyze potential threats and design mitigation strategies, to evaluate solutions that will build a secure environment in cloud ecosystems.



Threat Modeling as a Preventive Approach

Threat Modeling has built a strong position in the cybersecurity industry as a well-known practice providing a deeper understanding of the various threats and an overall attack surface. By applying threat modeling to a cloud environment, organizations can understand their cloud architecture, the relevant threats and the overall attack surface. This enables, security teams to better understand the controls required to mitigate these threats and manage their overall risk exposure.

This white paper will highlight the most important steps for building a threat model for a cloud environment and establishing a scalable threat modeling process. Some of the most valuable key points discussed are:

Promotion of secure coding, requiring organization standards.

Creation of task lists to ensure that security controls meet compliance objectives.

Implementation of threat modeling as a self-service model by leveraging workflow integration.

Leverage security tools and technologies to reduce attack surface.

Meeting today's security challenges as well as being strategically positioned for tomorrow's opportunities, makes cloud security a must-have rather than a nice-to-have. Whether organizations are considering deploying a single application to the cloud, migrating their data or creating a complete serverless architecture, their cloud environment becomes a part of the organization's comprehensive attack surface. Therefore, organizations have the urge of an automated and scalable threat modeling program to fully understand and effectively address the potential threats in a cloud native architecture.

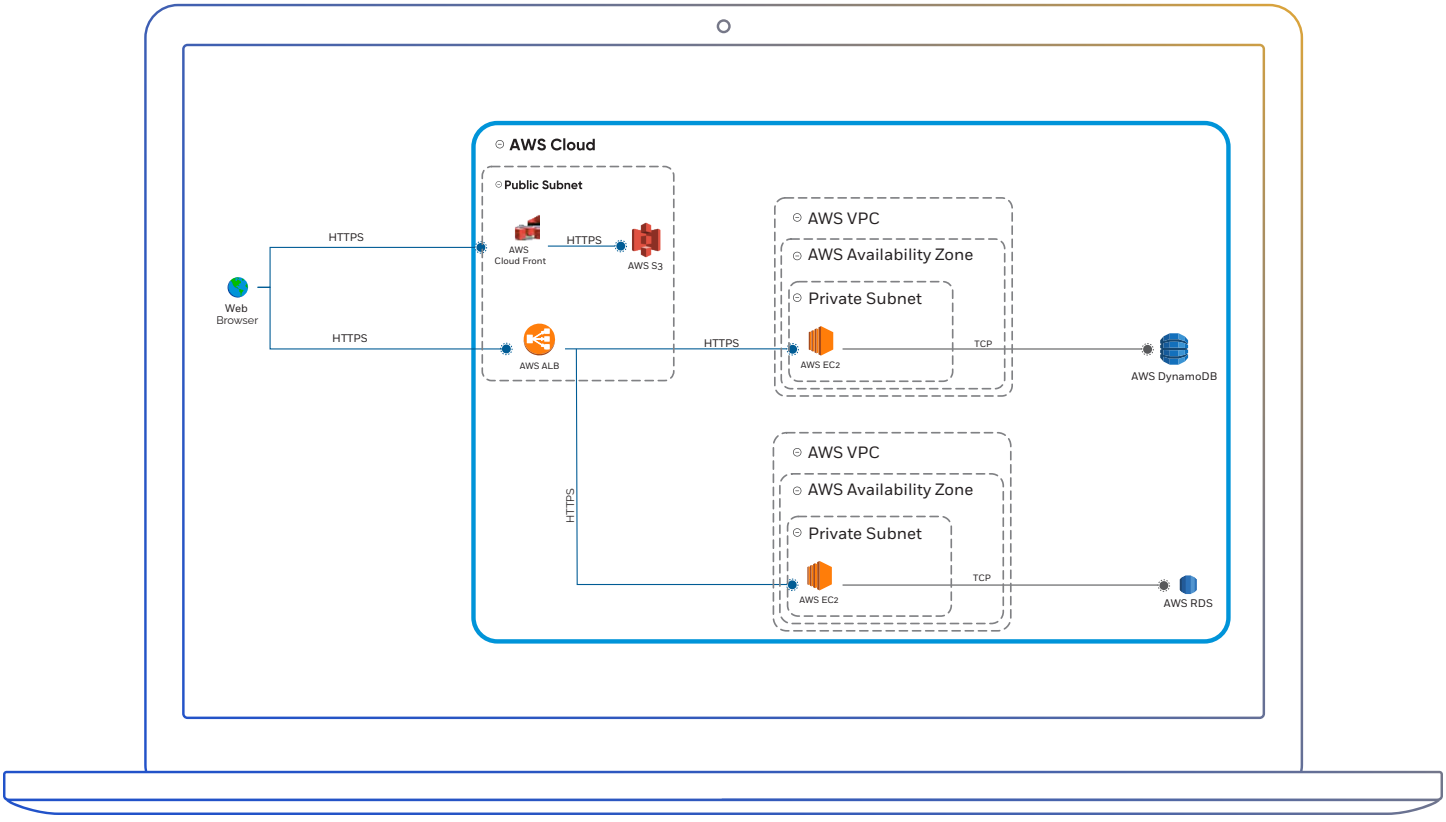
Building a Scalable Threat Modeling Program for the Cloud

A threat model for cloud infrastructure workload requires a library with reusable components unique to Cloud platforms (AWS, Azure & Google Cloud). Threat modeling allows users to design the architecture diagram for their cloud workload. To ensure that potential threats are identified, the threat modeling process must be methodical. Using a task list will help security experts achieve a consistent level of test exposure and proper completeness of a threat model.

Design the Cloud Architecture

Scaling a threat modeling process for AWS requires building a personalized architecture diagram. This diagram will indicate the workflow of the various parts of system components, making it easier to identify threats due to its visual structure. Architecture diagrams can be built by using pre-built templates, an integrated wizard for AWS or you can also build a template from scratch. The wizard allows security and non-security experts to build a threat model template specifically for AWS in 2 or 3 minutes.

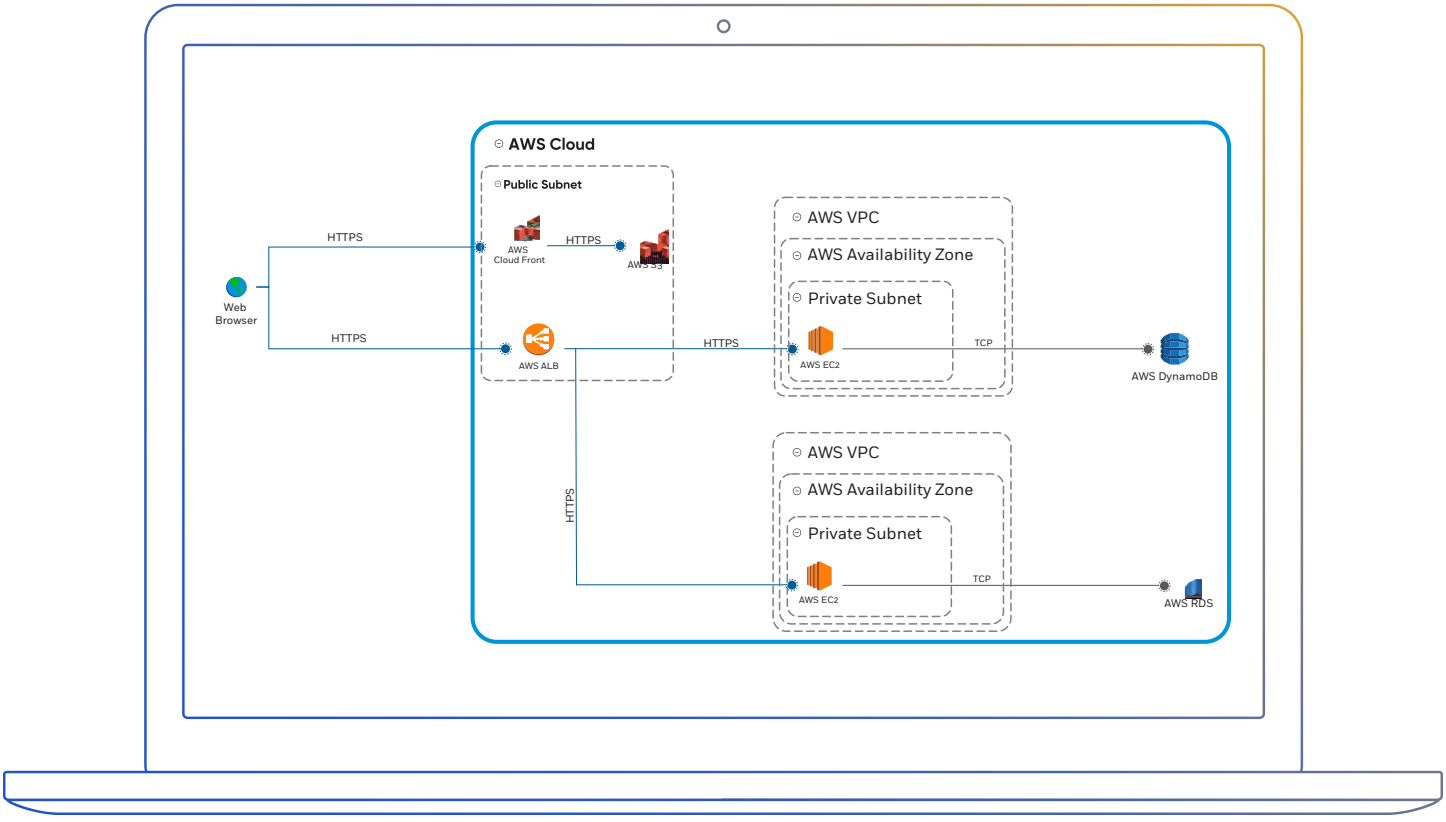
Threat models can also be built automatically from the existing workload in the AWS cloud ecosystem. ThreatModeler integrates with any type of AWS configuration, allowing users to build threat models for their cloud workload. This feature gives users access to continuously monitor threat models in real time.



Identify the Threat

Identifying threats for a cloud environment is very similar to the traditional environment with some more add-ons related to IaaS or PaaS. Organizations need to understand the controls used by AWS to protect their data and identify risks and threats. Threat modeling provides a threat library compatible with cloud environments, that includes all potential threats applicable to AWS.

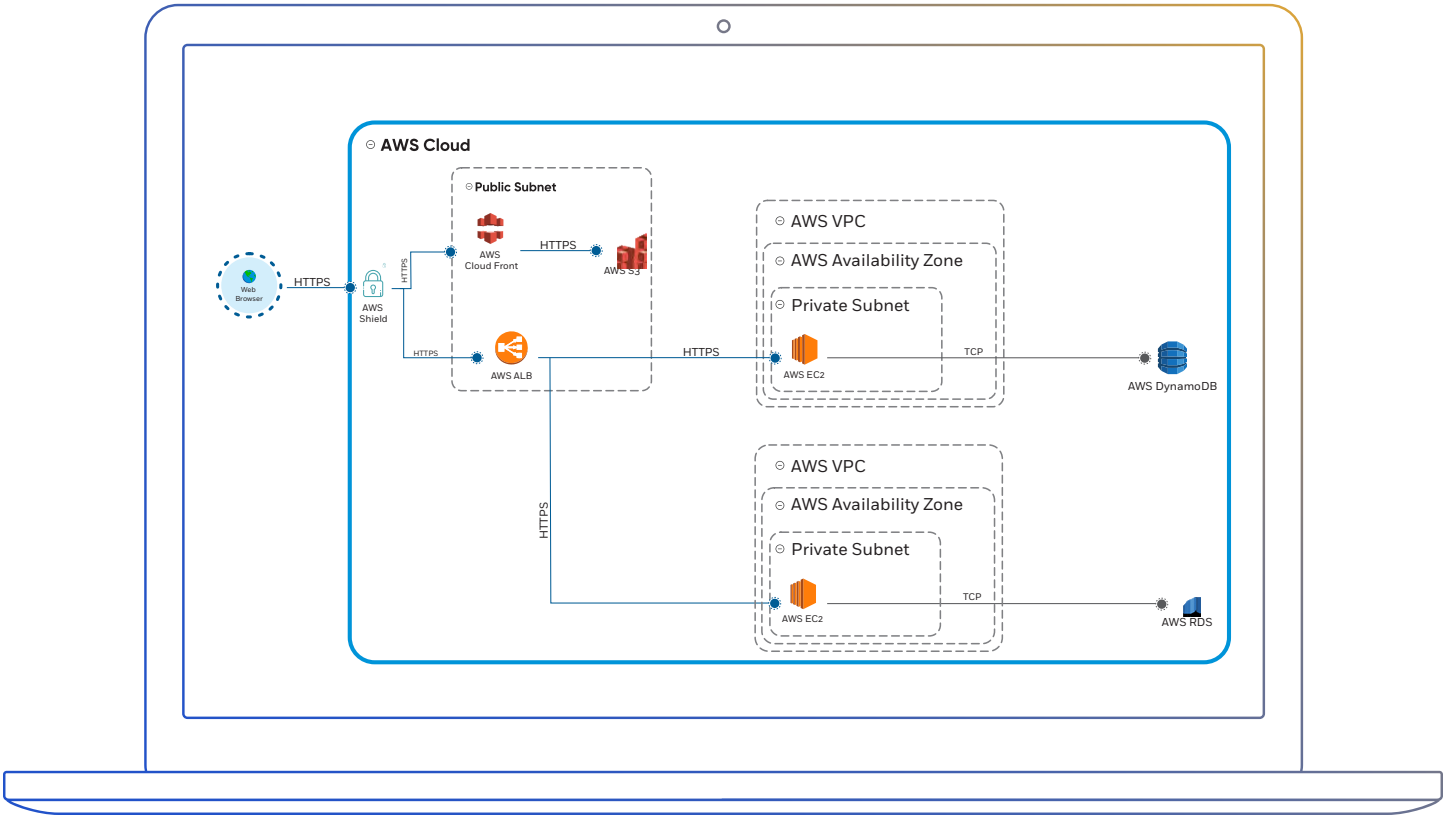
ThreatModeler offers a comprehensive library specific to AWS environments. This library includes the cloud top 12 & CAPEC threats. ThreatModeler's cloud security framework is specially designed to deliver security requirements relevant to AWS workloads. Users are able to import custom security policies into the library.



Implement the Security Controls

Security controls cover management, operational and technical functions designed to mitigate threats to information systems. ThreatModeler provides a comprehensive list of security controls utilized to design the cloud architecture. Security controls allow users to protect high value resources from various threats.

In the figure below, you can use AWS security groups, AWS Shield or IAM roles to protect various resources. It is also possible to define threats mitigated by identifying security control in your threat modeling tool. The architecture below uses an AWS shield security control to protect the resources from DOS attack.



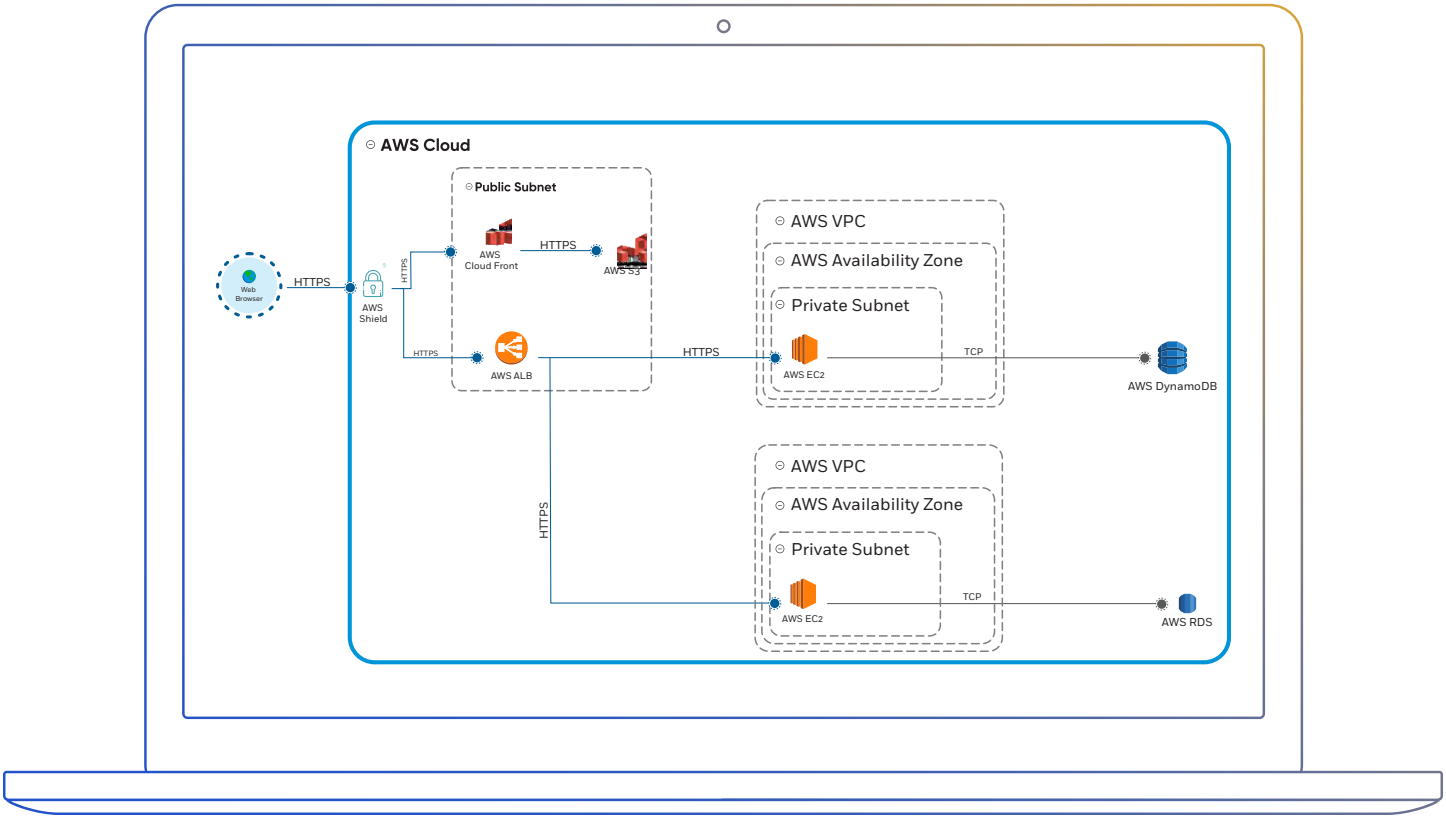
Example of AWS Security Controls

NAME	DESCRIPTION
AWS Inspector	Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices.
AWS VPC Endpoint	Enables private connectivity to services hosted in AWS from within your VPC without an Internet connection. With this feature, there is no requirement for an Internet Gateway, VPN, Network Address Translation (NAT) devices, firewall proxies or attaching an EIP.
AWS WAF	AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.
AWS Shield	AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS from common, most frequently occurring, network and transport layer DDoS attacks.
AWS KMS	AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data and uses FIPS 140-2 validated hardware security modules to protect the security of your keys.
AWS Security Groups	AWS security groups (SGs) are associated with Ec2 instances and provide security at the protocol and port access level. Each security group – working much the same way as a firewall – contains a set of rules that filter traffic coming into and out of an EC2 instance.
AWS IAM	Describes the AWS CLI commands that you can use to administer IAM. Provides syntax, options, and usage examples for each command.

Validate the Correct Implementation of Security Controls

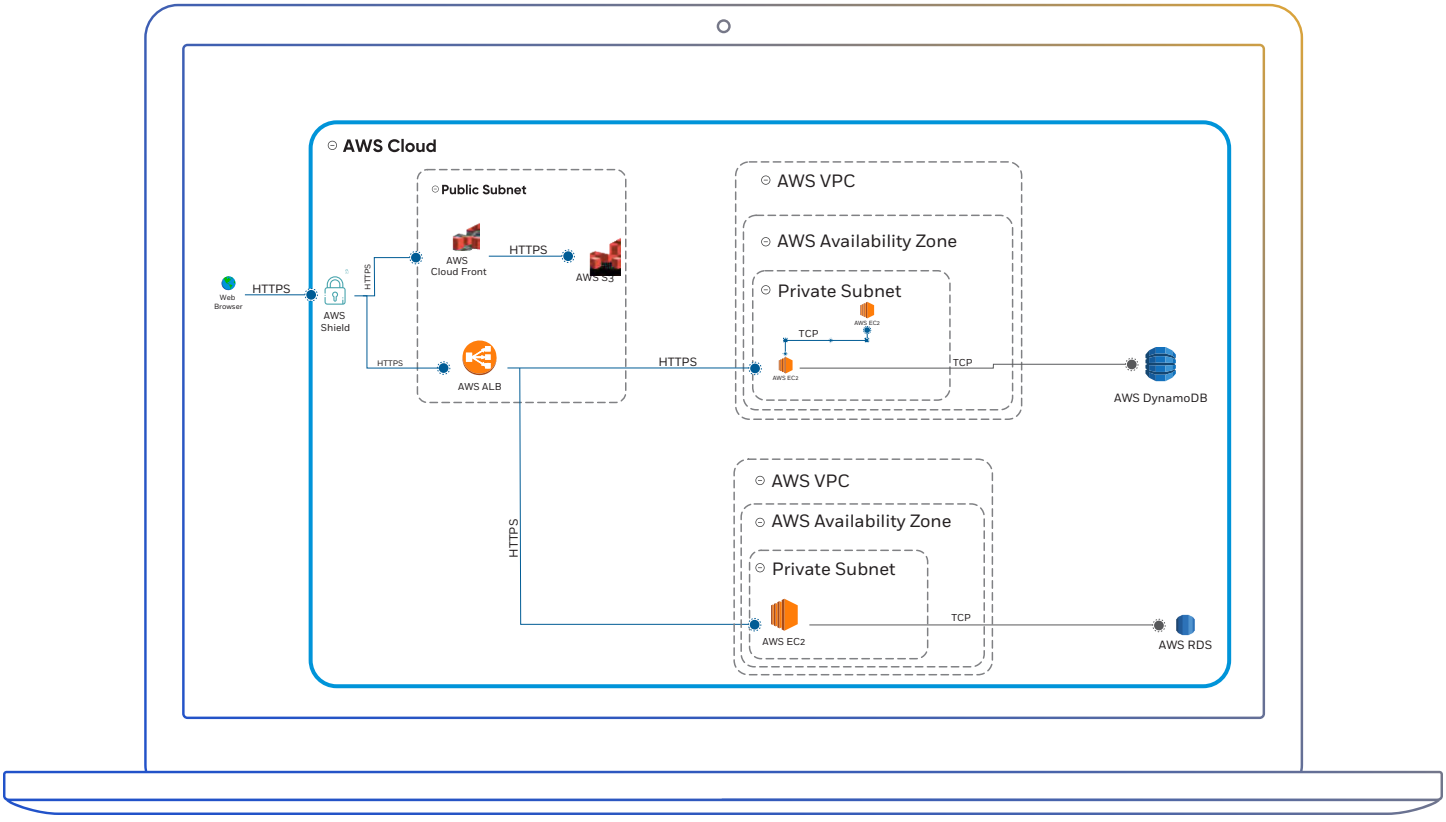
Validating the proper implementation of security controls is one of the most important steps.

Users can validate security controls by logging into their AWS cloud system and make surreal controls are implemented. ThreatModeler Cloud Edition includes a new feature that continuously monitors threat models, allowing users to certify the controls are implemented and they can be aware of any changes and updates. Users can review those changes and incorporate them to a new version of their current threat model.



Monitor the Changes to the Cloud Architecture

Once the implementation of security controls has been validated, new versions of the cloud architecture can be generated. With ThreatModeler's new feature, users can save and lock different threat model diagrams to monitor the changes made to each version of the cloud architecture. The diagram below depicts two different versions of a threat model. Users can review old versions and see the difference between them with just one click.



ThreatModeler Cloud Edition for AWS

As organizations recognize the importance of cloud computing, the need for a threat modeling tool for the cloud becomes a requirement. Most of the threat modeling practices today are using manual cloud environments. Unfortunately, manual processes are outdated, involving higher costs and lack of accuracy.

ThreatModeler – an official AWS Technology partner – provides an automated, structured approach to build secure cloud environments. This cloud platform threat modeling solution allows organizations to build threat models from pre-defined templates of various AWS architectures or even create a threat model using a wizard plugin in just a couple of minutes.

Organizations can scale their threat modeling process across their entire DevOps portfolio, regardless of whether the initiatives are in-house or deployed within their AWS environment. The outputs generated by ThreatModeler are consistent, concrete, and actionable – allowing organizations to generate a comprehensive attack surface analysis of their entire IT footprint – whether in-house or on the AWS and Azure platform – along with the relevant mitigating controls.

ThreatModeler Cloud Edition for AWS includes the following exclusive features and benefits:

1. **Create threat models automatically for AWS**
Users are able to gather information from their AWS platform and import this data to the ThreatModeler library to automatically build a threat model.

2. **Cloud-Native Security Framework**
ThreatModeler™ provides a comprehensive toolbox with specific security controls that apply to the AWS environment. This feature saves time and effort to organizations when creating their own security controls.

3. **Continuous Monitoring**
ThreatModeler continuously monitors threat models, intelligently notifying users of updates and changes.

4. **Reusable Templates**
ThreatModeler allows organizations to build threat models related to their AWS environment in minutes and immediately receive the actionable output needed for secure, rapid-deployment decisions. Users are able to use pre-built templates to customize threat models for AWS infrastructures.

5. **Integration with CICD pipeline**
ThreatModeler's bi-directional API gives users the ability to leverage their existing investments in technologies such as JIRA & Jenkins – if it's part of their DevOps and CI/CD toolchain, they would want it to be part of their threat modeling process.

Get a demo.