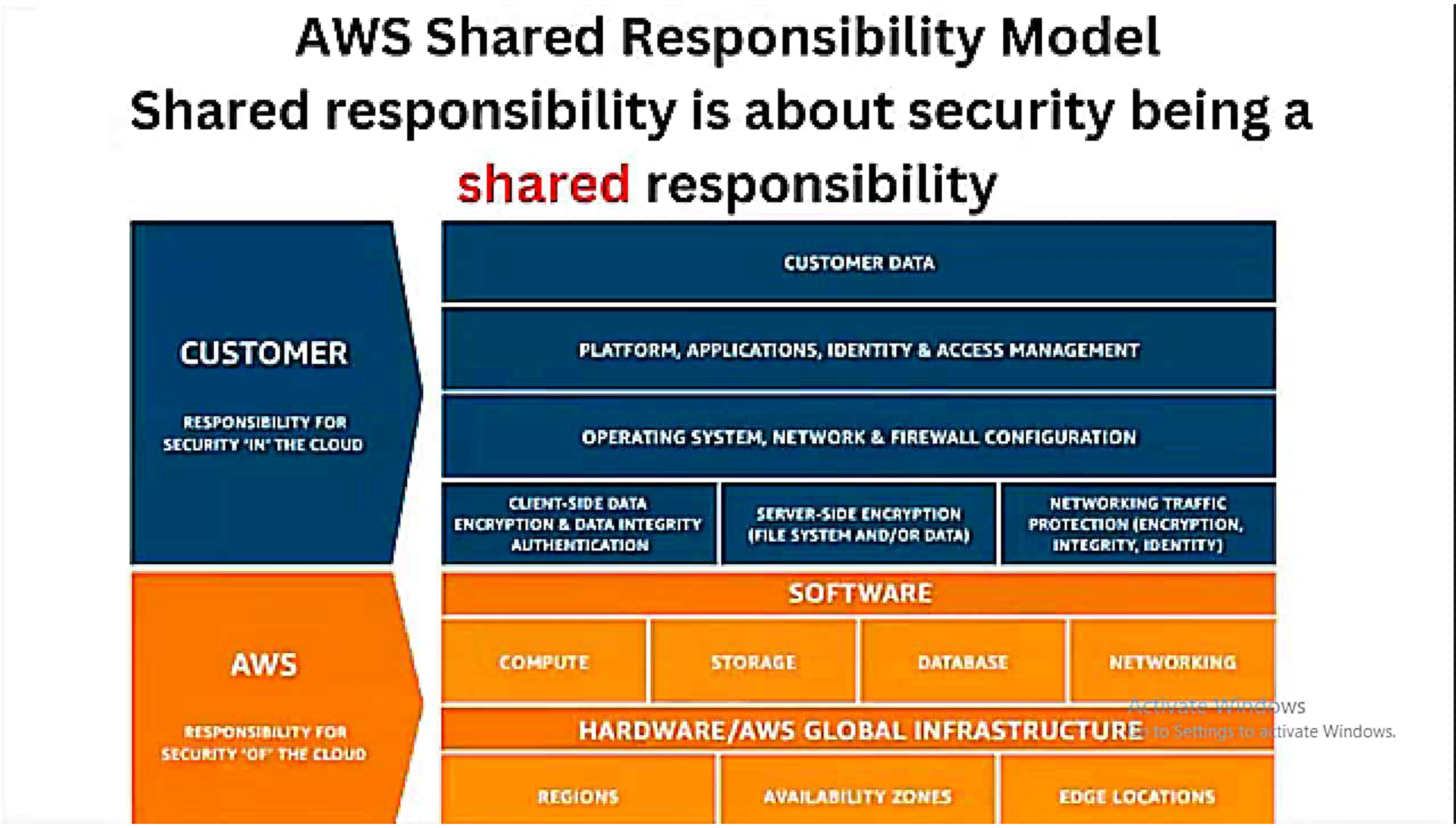
SESSION 12

AWS SECURITY AND COMPLAINCES



AWS Shared Responsibility Model

Shared responsibility is about security being a shared responsibility

CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

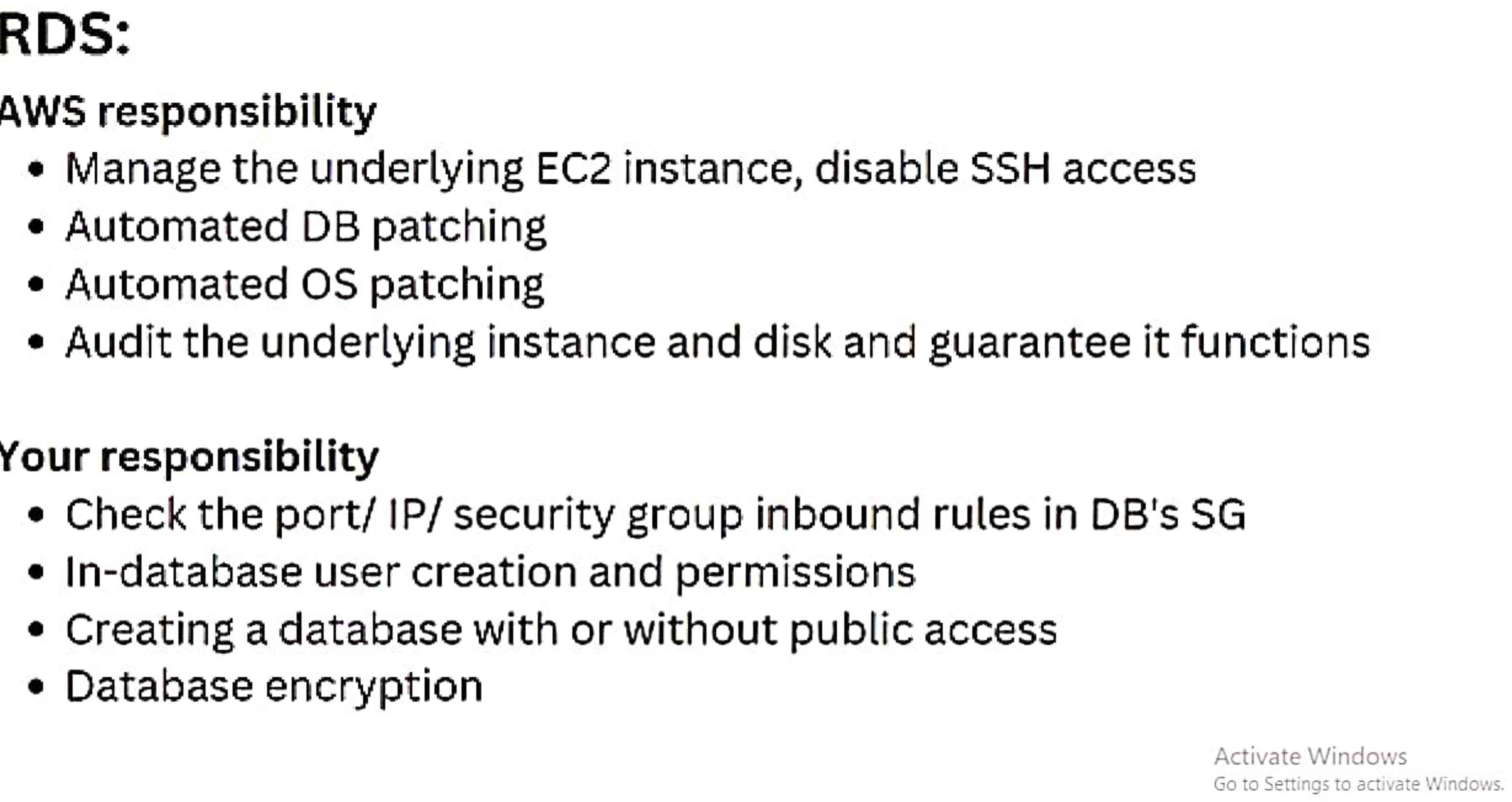
AVAILABILITY ZONES

EDGE LOCATIONS

AWS Responsibility: Security of the Cloud
Protecting Infrastructure

Customer responsibility: Security in the cloud
For EC2, firewall, IAM,

Shared Controls: Patch Management, Configuration Management, Awareness and Training



RDS:

AWS responsibility

- Manage the underlying EC2 instance, disable SSH access
- Automated DB patching
- Automated OS patching
- Audit the underlying instance and disk and guarantee it functions

Your responsibility

- Check the port/ IP/ security group inbound rules in DB's SG
- In-database user creation and permissions
- Creating a database with or without public access
- Database encryption

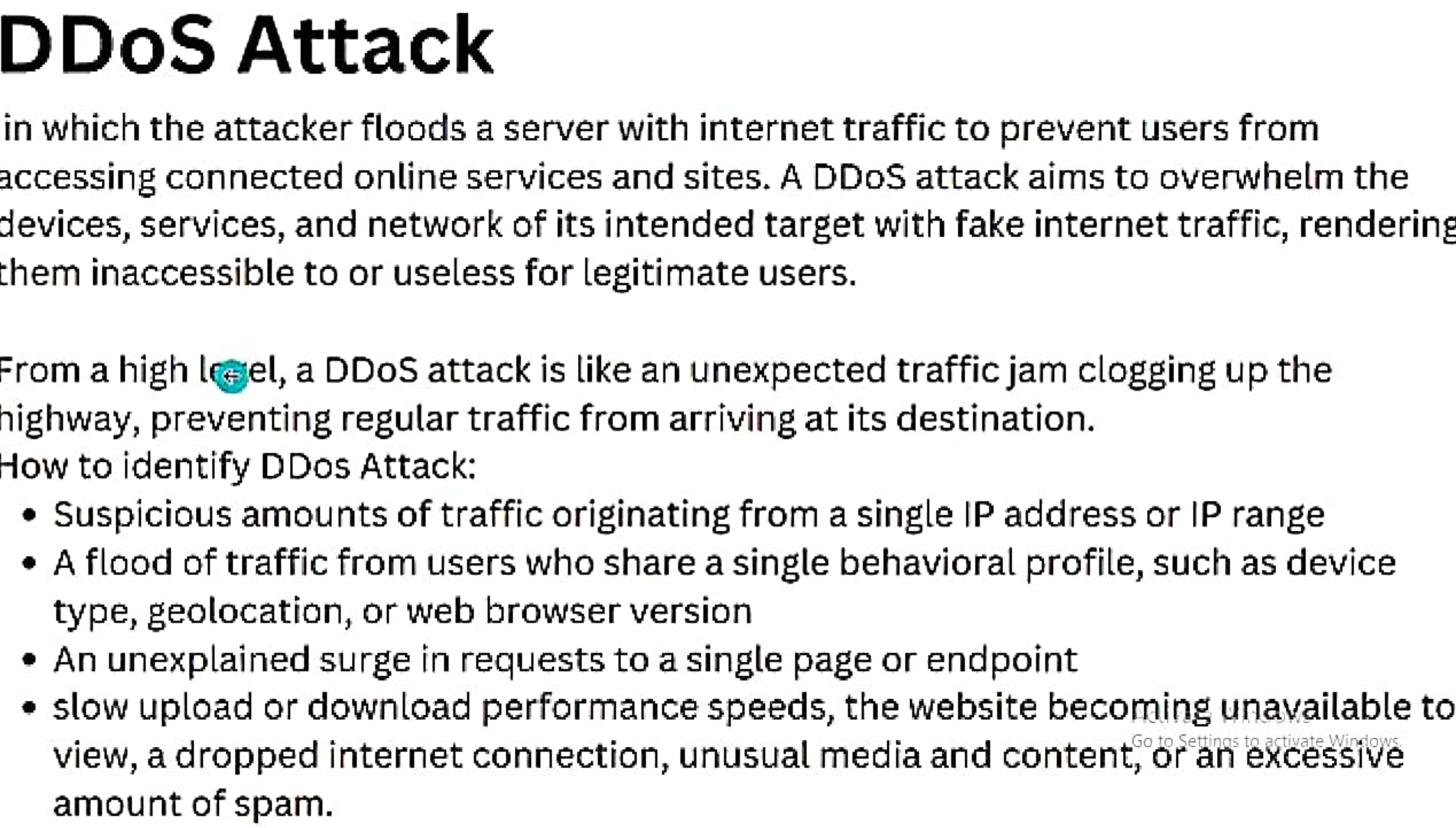
AWS S3:

AWS responsibility:

- Guarantee you get unlimited storage
- Guarantee you get encryption
- Ensure separation of the data with different customers
- Ensure AWS employees can't access your data

Your responsibility:

- Bucket configuration
- Bucket policy/ public setting
- IAM user and roles
- Enable Encryption

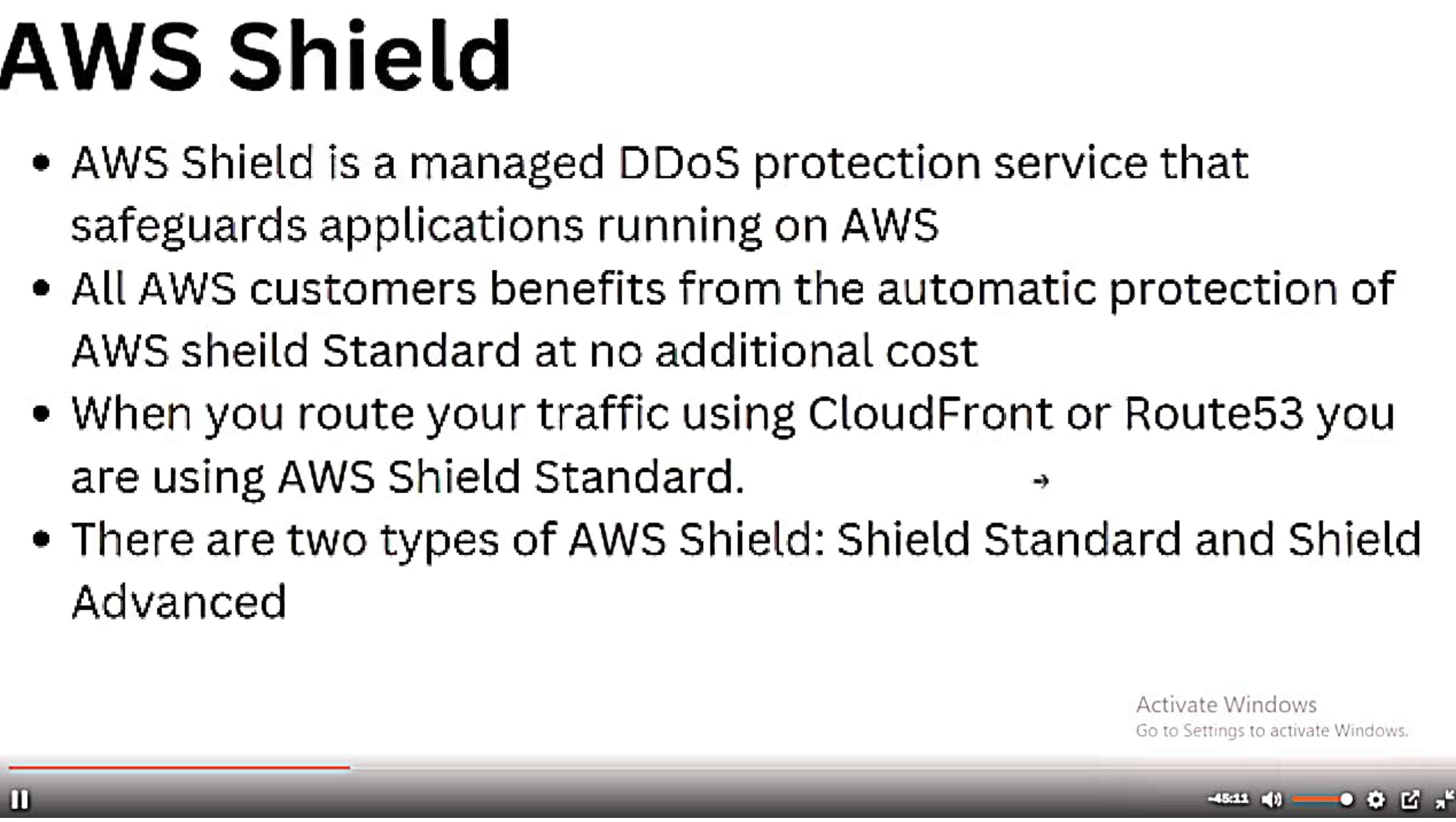


DDoS Attack

in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites. A DDoS attack aims to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.

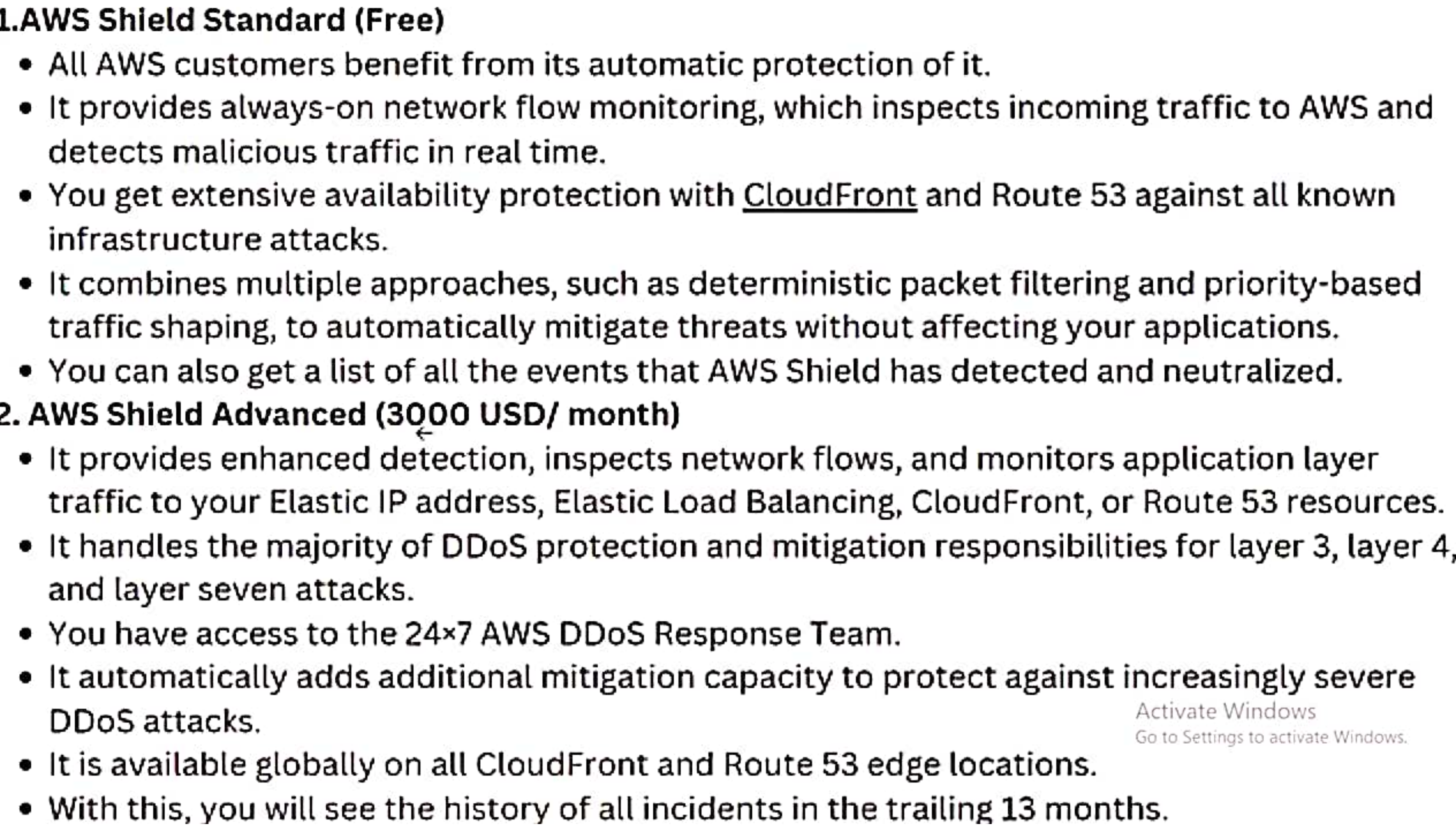
From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.
How to identify DDos Attack:

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version
- An unexplained surge in requests to a single page or endpoint
- slow upload or download performance speeds, the website becoming unavailable to view, a dropped internet connection, unusual media and content, or an excessive amount of spam.



AWS Shield

- AWS Shield is a managed DDoS protection service that safeguards applications running on AWS
- All AWS customers benefits from the automatic protection of AWS sheild Standard at no additional cost
- When you route your traffic using CloudFront or Route53 you are using AWS Shield Standard.
- There are two types of AWS Shield: Shield Standard and Shield Advanced

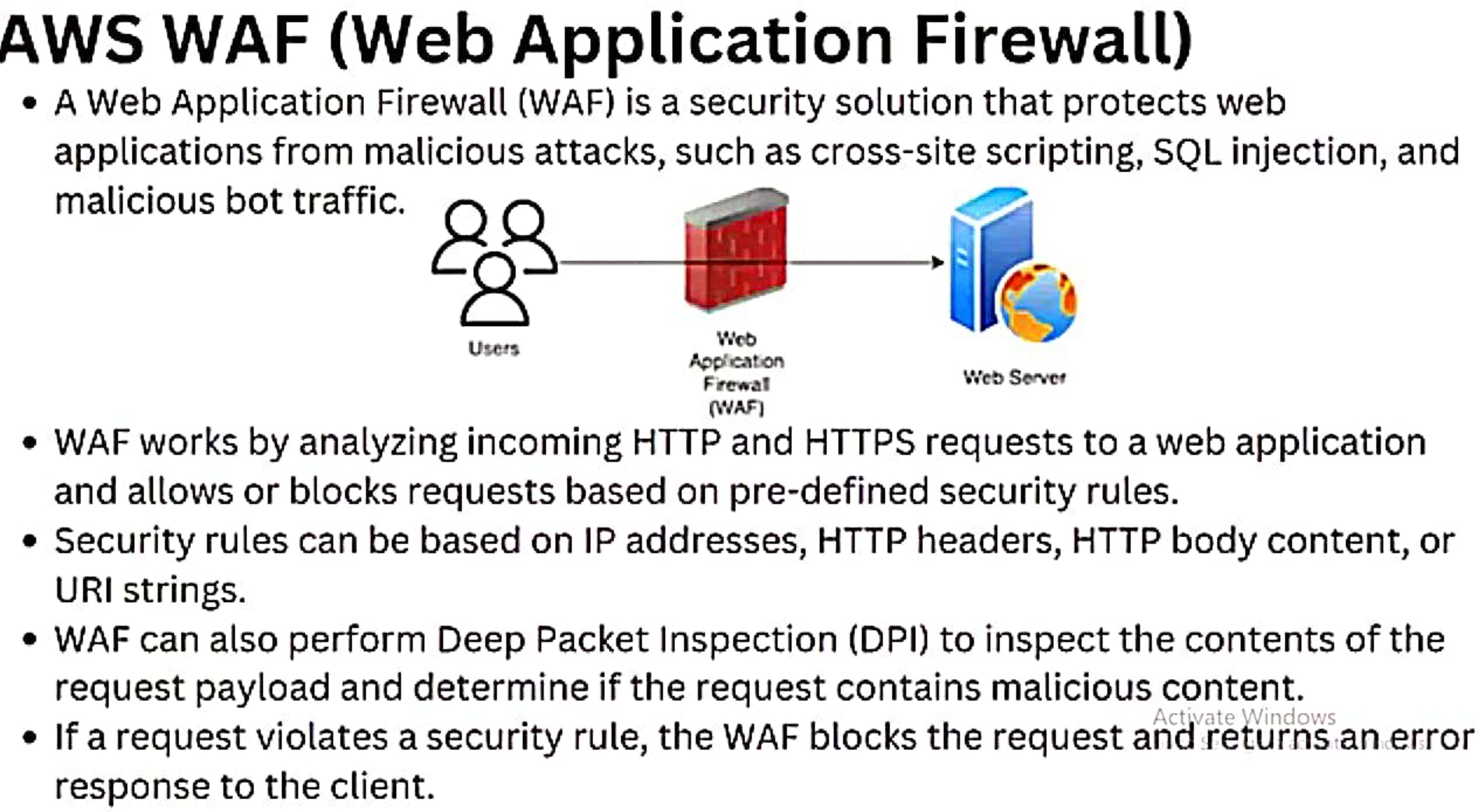


1.AWS Shield Standard (Free)

- All AWS customers benefit from its automatic protection of it.
- It provides always-on network flow monitoring, which inspects incoming traffic to AWS and detects malicious traffic in real time.
- You get extensive availability protection with CloudFront and Route 53 against all known infrastructure attacks.
- It combines multiple approaches, such as deterministic packet filtering and priority-based traffic shaping, to automatically mitigate threats without affecting your applications.
- You can also get a list of all the events that AWS Shield has detected and neutralized.

2. AWS Shield Advanced (3000 USD/ month)

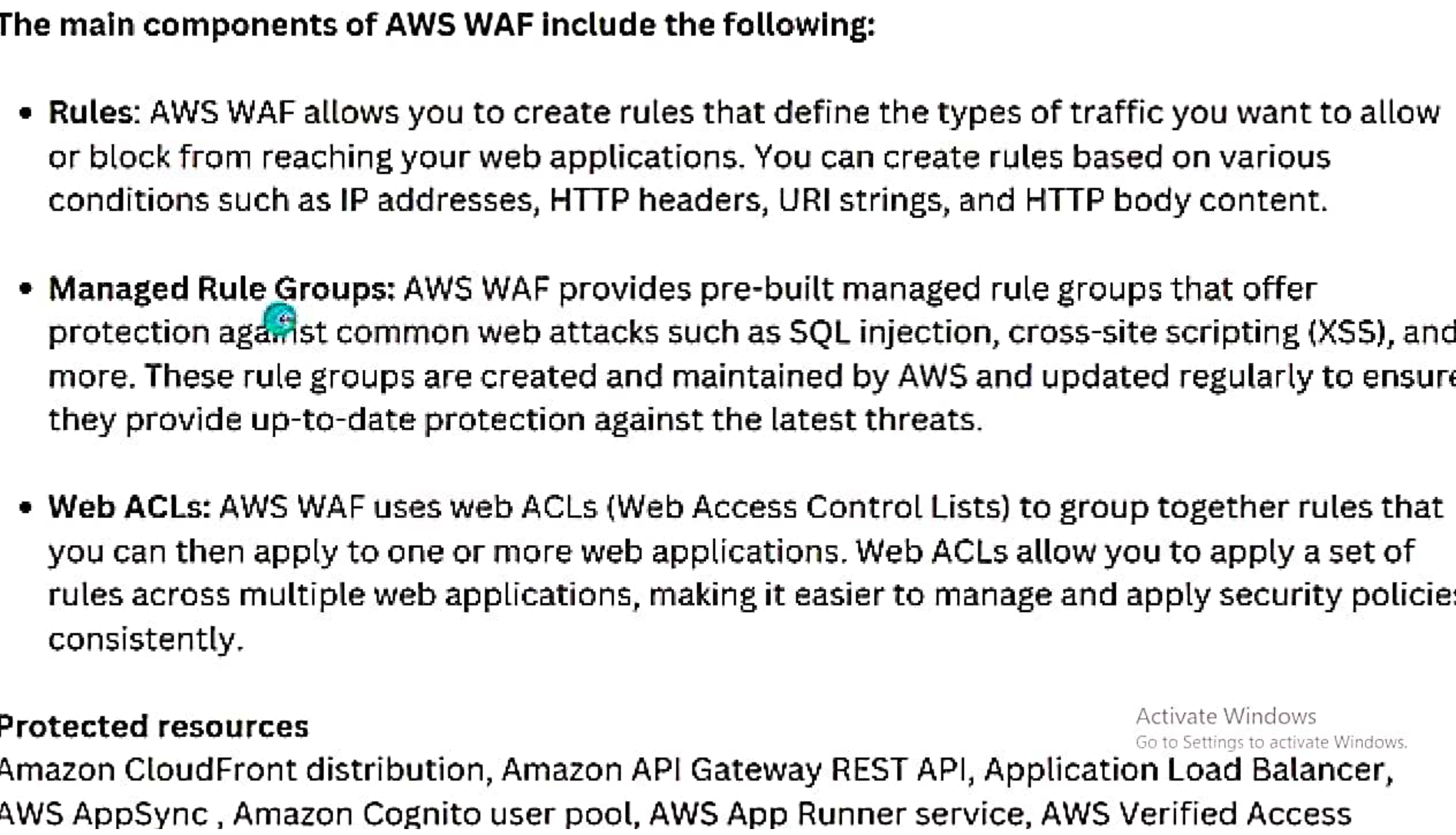
- It provides enhanced detection, inspects network flows, and monitors application layer traffic to your Elastic IP address, Elastic Load Balancing, CloudFront, or Route 53 resources.
- It handles the majority of DDoS protection and mitigation responsibilities for layer 3, layer 4, and layer seven attacks.
- You have access to the 24×7 AWS DDoS Response Team.
- It automatically adds additional mitigation capacity to protect against increasingly severe DDoS attacks.
- It is available globally on all CloudFront and Route 53 edge locations.
- With this, you will see the history of all incidents in the trailing 13 months.



AWS WAF (Web Application Firewall)

- A Web Application Firewall (WAF) is a security solution that protects web applications from malicious attacks, such as cross-site scripting, SQL injection, and malicious bot traffic.

- WAF works by analyzing incoming HTTP and HTTPS requests to a web application and allows or blocks requests based on pre-defined security rules.
- Security rules can be based on IP addresses, HTTP headers, HTTP body content, or URI strings.
- WAF can also perform Deep Packet Inspection (DPI) to inspect the contents of the request payload and determine if the request contains malicious content.
- If a request violates a security rule, the WAF blocks the request and returns an error response to the client.

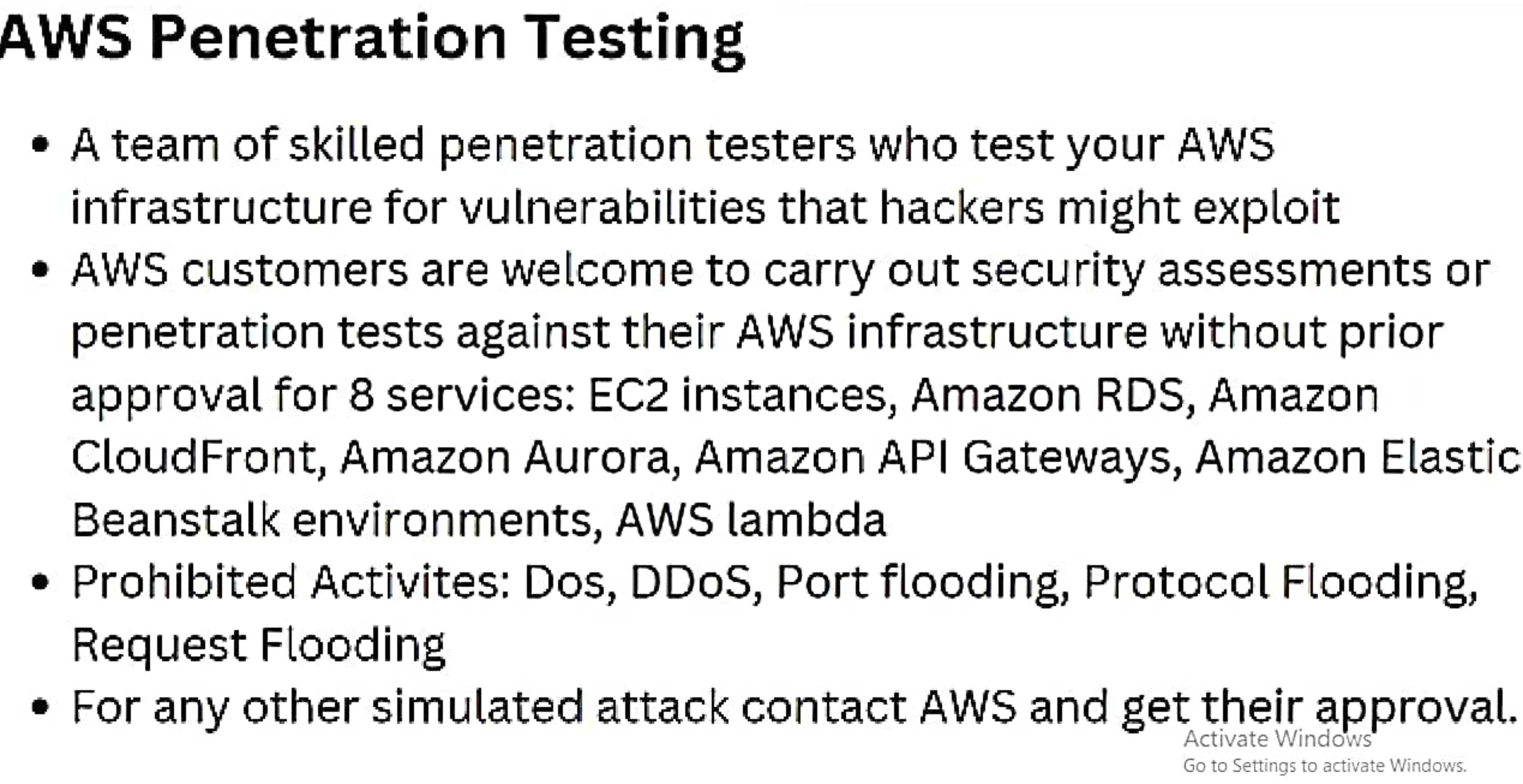


The main components of AWS WAF include the following:

- **Rules**: AWS WAF allows you to create rules that define the types of traffic you want to allow or block from reaching your web applications. You can create rules based on various conditions such as IP addresses, HTTP headers, URI strings, and HTTP body content.
- **Managed Rule Groups:** AWS WAF provides pre-built managed rule groups that offer protection against common web attacks such as SQL injection, cross-site scripting (XSS), and more. These rule groups are created and maintained by AWS and updated regularly to ensure they provide up-to-date protection against the latest threats.
- **Web ACLs:** AWS WAF uses web ACLs (Web Access Control Lists) to group together rules that you can then apply to one or more web applications. Web ACLs allow you to apply a set of rules across multiple web applications, making it easier to manage and apply security policies consistently.

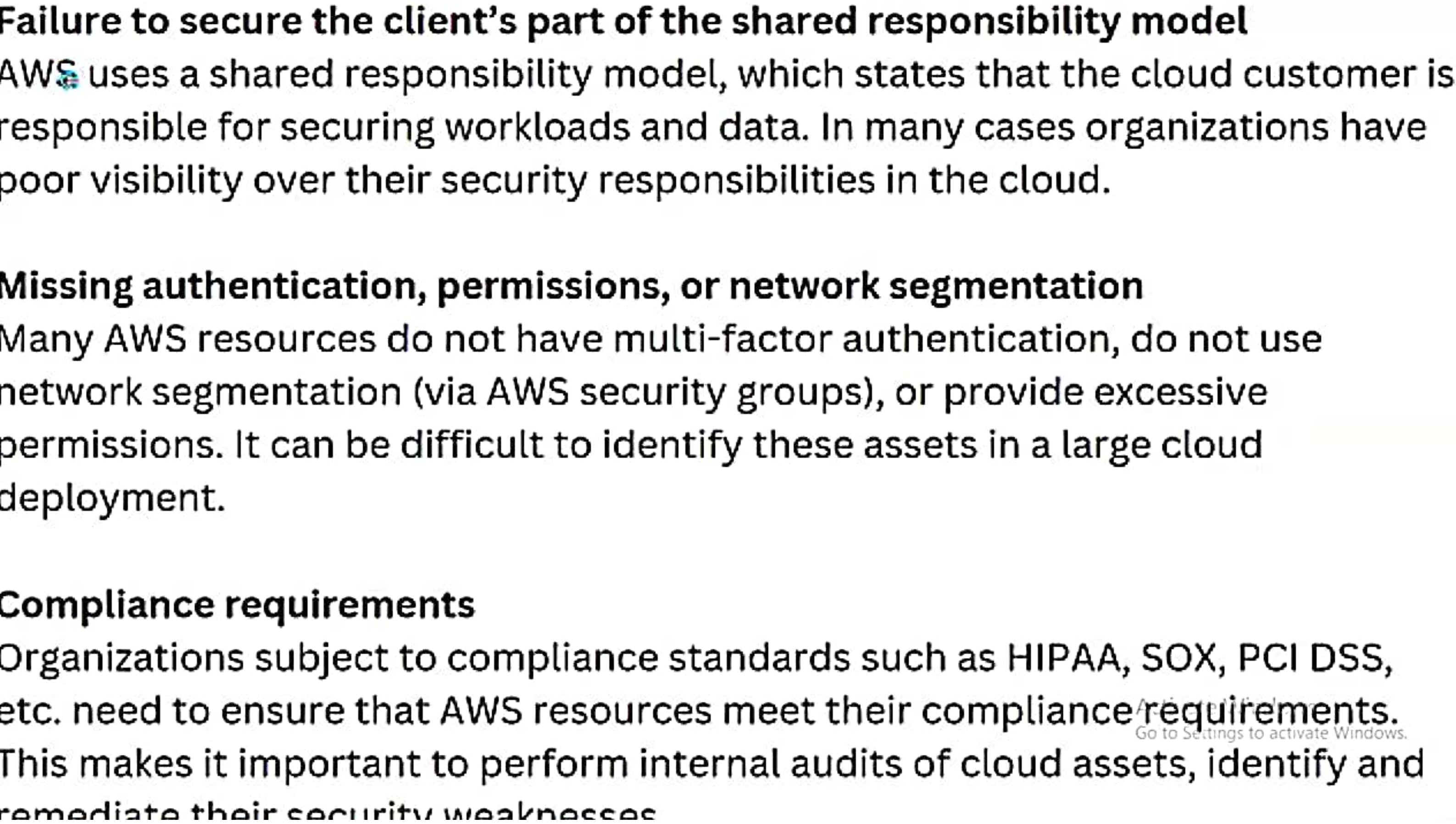
Protected resources

Amazon CloudFront distribution, Amazon API Gateway REST API, Application Load Balancer, AWS AppSync , Amazon Cognito user pool, AWS App Runner service, AWS Verified Access



AWS Penetration Testing

- A team of skilled penetration testers who test your AWS infrastructure for vulnerabilities that hackers might exploit
- AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services: EC2 instances, Amazon RDS, Amazon CloudFront, Amazon Aurora, Amazon API Gateways, Amazon Elastic Beanstalk environments, AWS lambda
- Prohibited Activites: Dos, DDoS, Port flooding, Protocol Flooding, Request Flooding
- For any other simulated attack contact AWS and get their approval.



Failure to secure the client’s part of the shared responsibility model

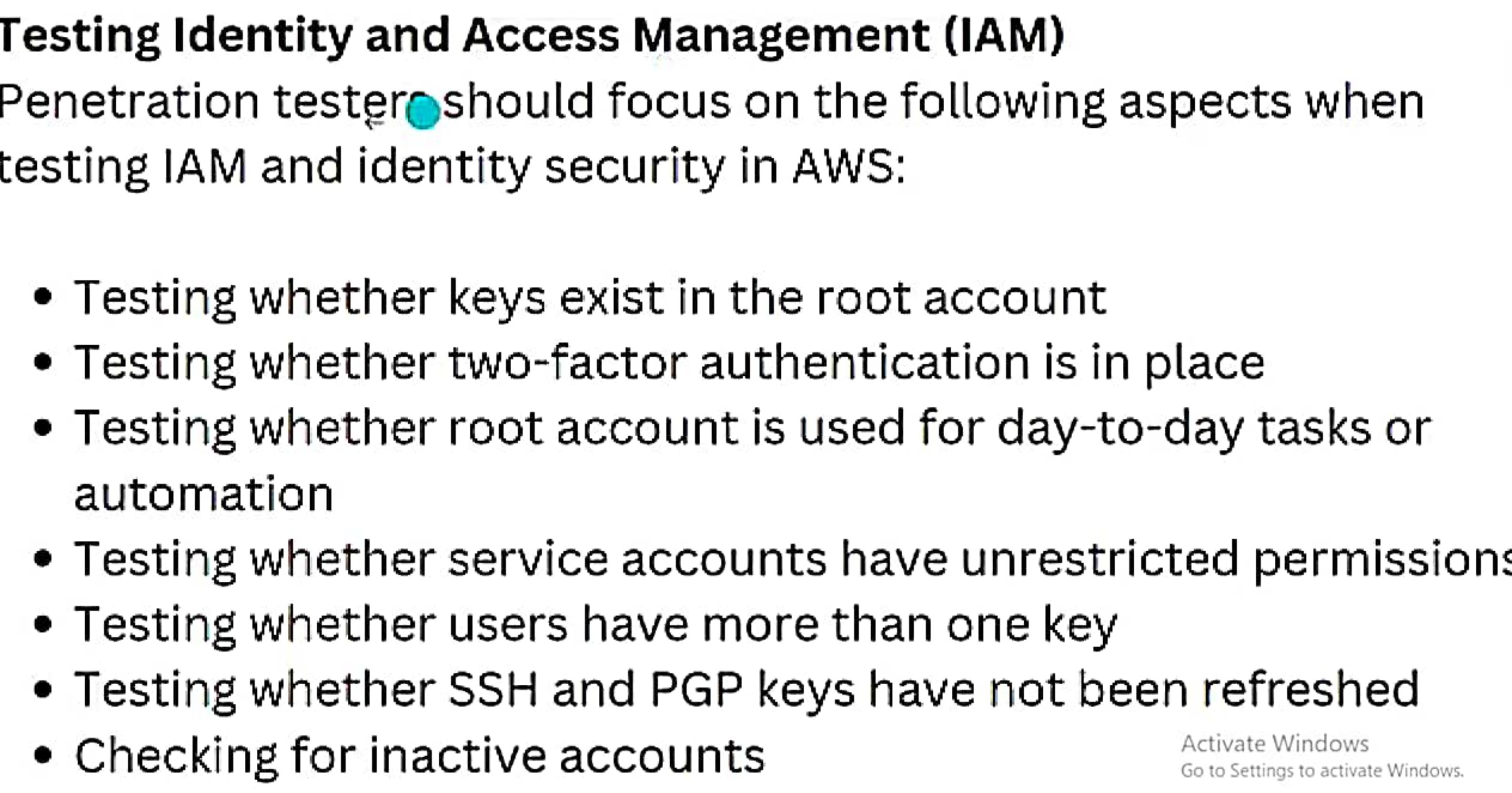
AWS uses a shared responsibility model, which states that the cloud customer is responsible for securing workloads and data. In many cases organizations have poor visibility over their security responsibilities in the cloud.

Missing authentication, permissions, or network segmentation

Many AWS resources do not have multi-factor authentication, do not use network segmentation (via AWS security groups), or provide excessive permissions. It can be difficult to identify these assets in a large cloud deployment.

Compliance requirements

Organizations subject to compliance standards such as HIPAA, SOX, PCI DSS, etc. need to ensure that AWS resources meet their compliance requirements. This makes it important to perform internal audits of cloud assets, identify and remediate their security weaknesses



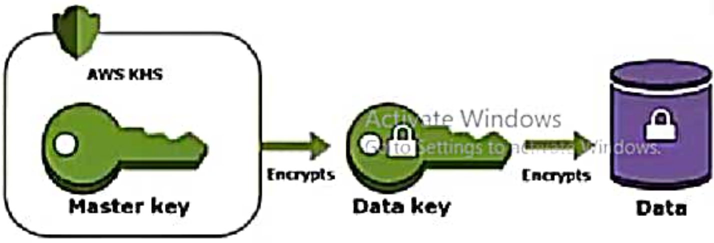
Testing Identity and Access Management (IAM)

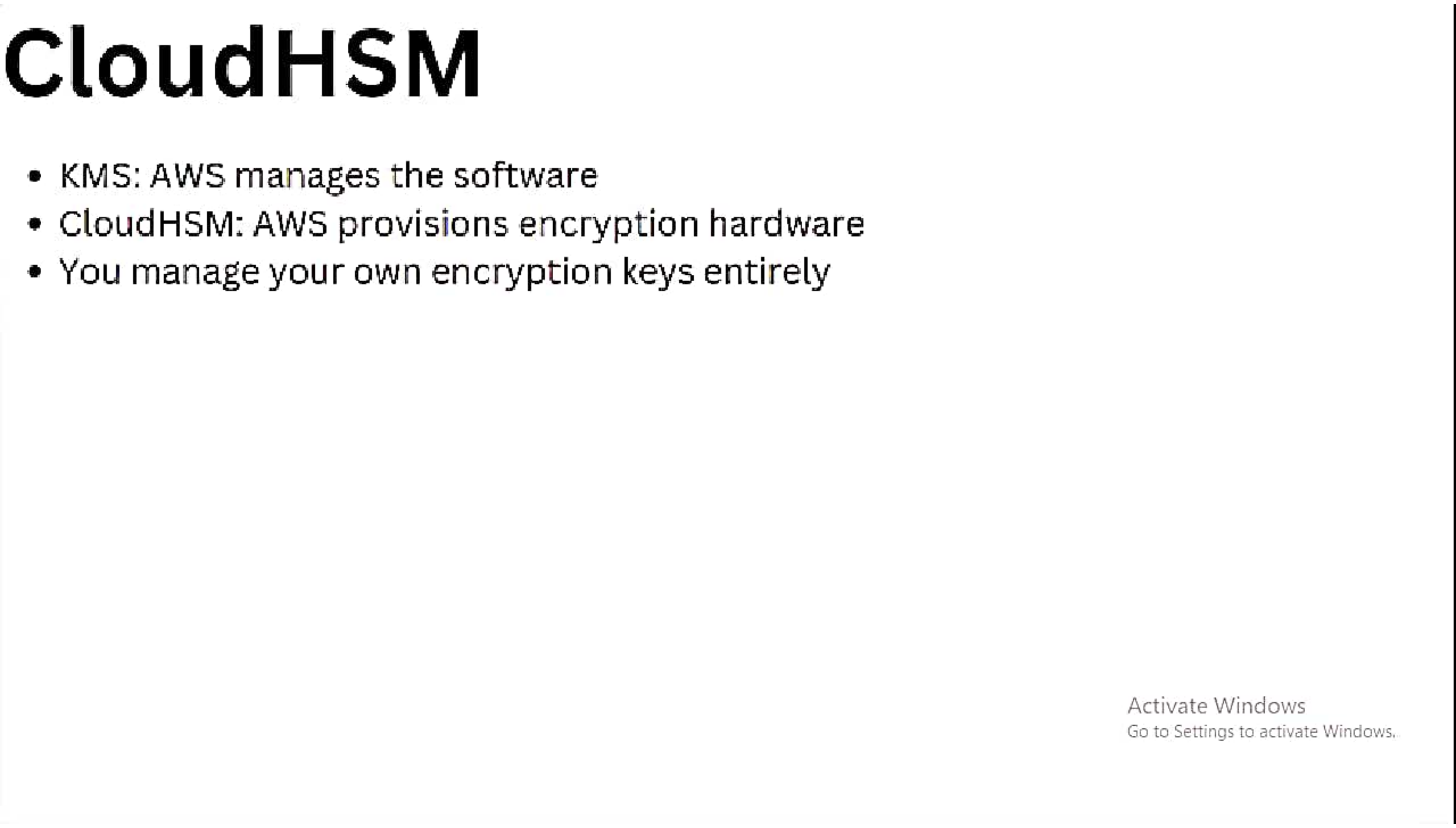
Penetration testers should focus on the following aspects when testing IAM and identity security in AWS:

- Testing whether keys exist in the root account
- Testing whether two-factor authentication is in place
- Testing whether root account is used for day-to-day tasks or automation
- Testing whether service accounts have unrestricted permissions
- Testing whether users have more than one key
- Testing whether SSH and PGP keys have not been refreshed
- Checking for inactive accounts

Key Management System= AWS manages the encryption keys for us

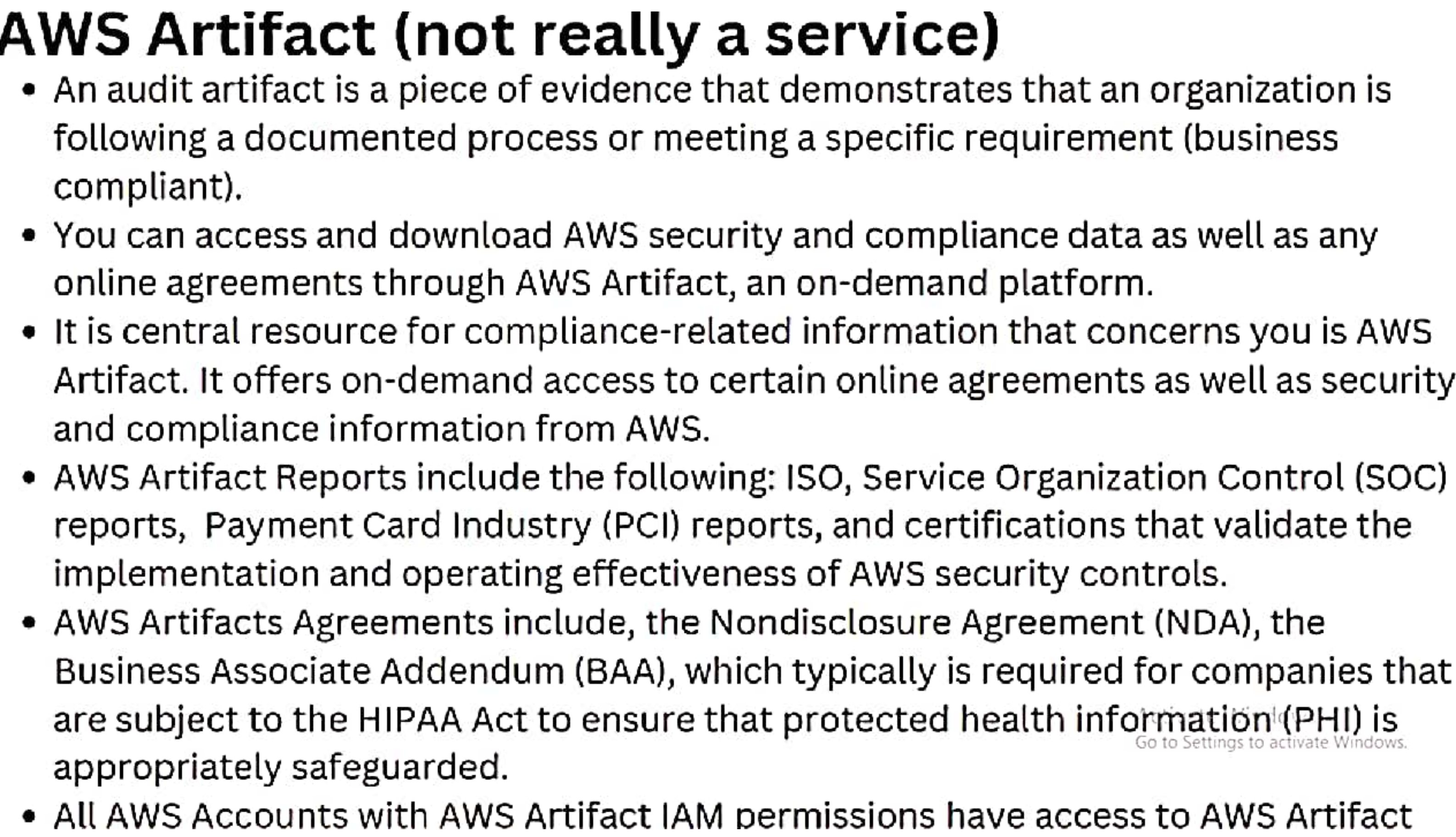
- **Data at Rest:** data stored/archived on a device, S3 deep Archive
- **Data in transit:** data being moved from one location to another, Transfer from on-premise to AWS , EC2
- We want to protect in both states, for this we use encryption keys
- Data encryption is vital if you have sensitive data that must not be accessed by unauthorized users.
- KMS makes it easy for you to create and manage encryption keys
- Many AWS services are integrated to use KMS to encrypt your data with a simple checkbox
- Encryption Opt-in: EBS volumes(encrypt volumes), S3 buckets(encryption of objects), Redshift database, RDS database, EFS drives
- Encryption automatically enabled: CloudTrail logs, S3 Glacier, Storage Gateway





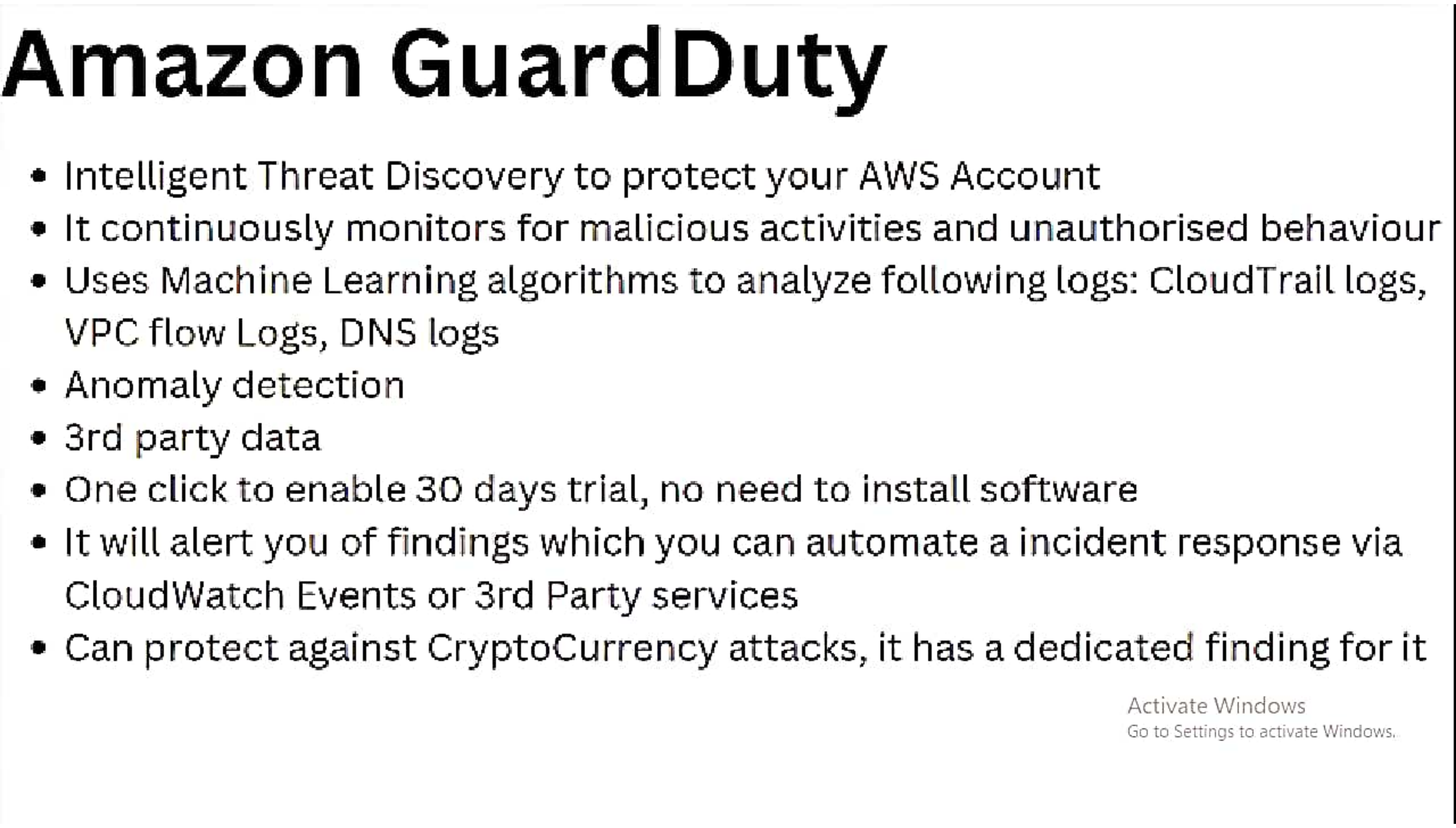
CloudHSM

- KMS: AWS manages the software
- CloudHSM: AWS provisions encryption hardware
- You manage your own encryption keys entirely



AWS Artifact (not really a service)

- An audit artifact is a piece of evidence that demonstrates that an organization is following a documented process or meeting a specific requirement (business compliant).
- You can access and download AWS security and compliance data as well as any online agreements through AWS Artifact, an on-demand platform.
- It is central resource for compliance-related information that concerns you is AWS Artifact. It offers on-demand access to certain online agreements as well as security and compliance information from AWS.
- AWS Artifact Reports include the following: ISO, Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications that validate the implementation and operating effectiveness of AWS security controls.
- AWS Artifacts Agreements include, the Nondisclosure Agreement (NDA), the Business Associate Addendum (BAA), which typically is required for companies that are subject to the HIPAA Act to ensure that protected health information (PHI) is appropriately safeguarded.
- All AWS Accounts with AWS Artifact IAM permissions have access to AWS Artifact

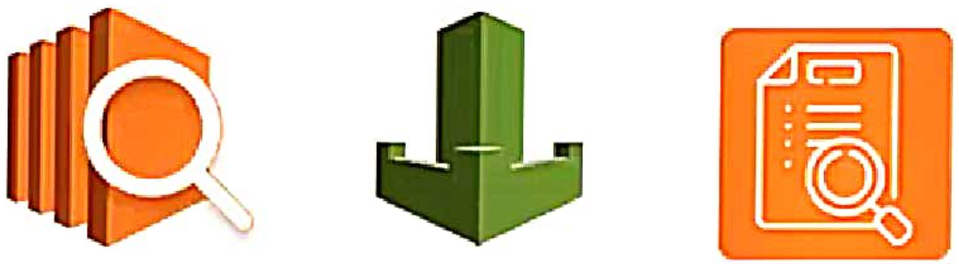


Amazon GuardDuty

- Intelligent Threat Discovery to protect your AWS Account
- It continuously monitors for malicious activities and unauthorised behaviour
- Uses Machine Learning algorithms to analyze following logs: CloudTrail logs, VPC flow Logs, DNS logs
- Anomaly detection
- 3rd party data
- One click to enable 30 days trial, no need to install software
- It will alert you of findings which you can automate a incident response via CloudWatch Events or 3rd Party services
- Can protect against CryptoCurrency attacks, it has a dedicated finding for it

Amazon Inspector

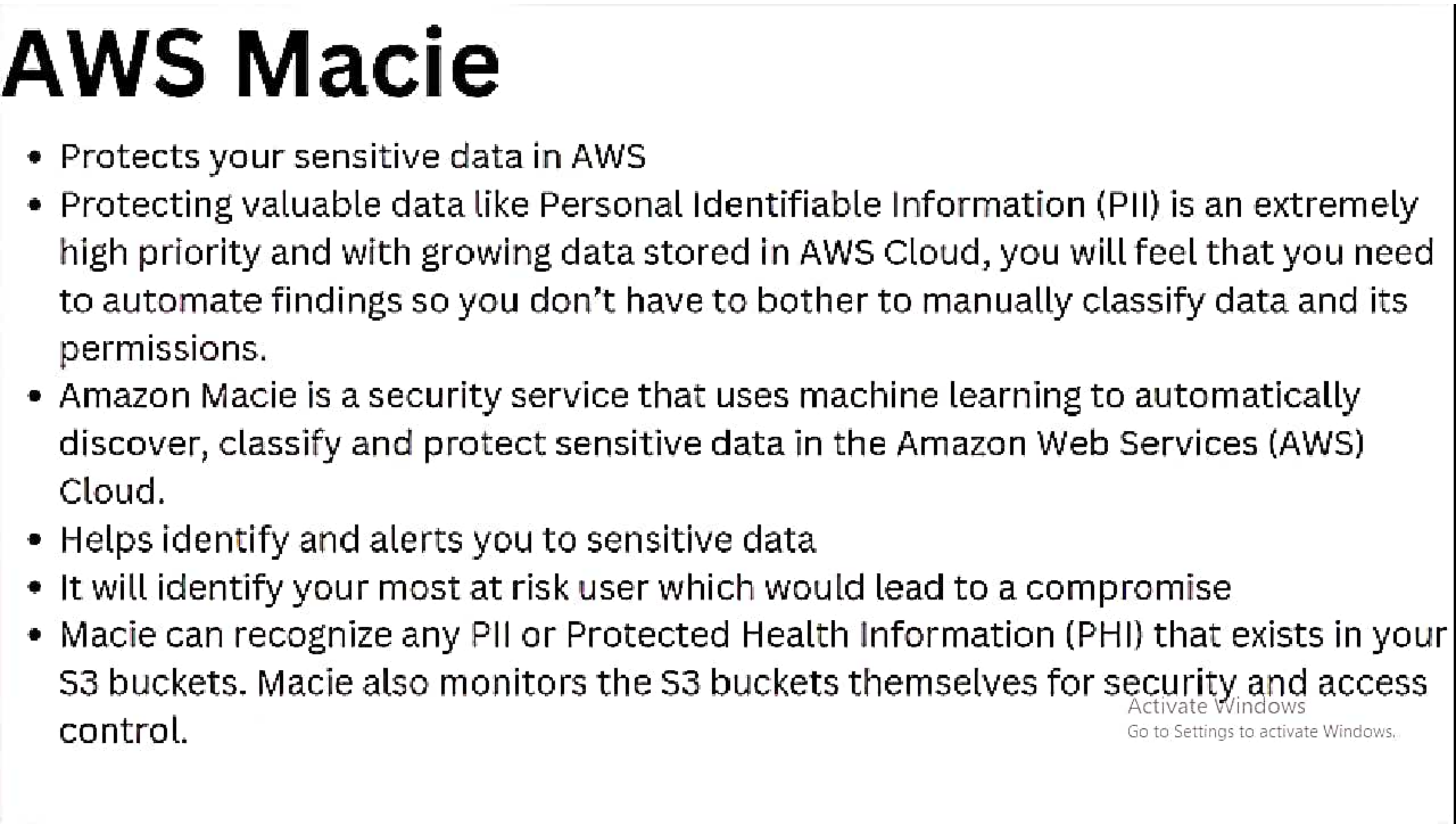
- Automated Security Assessment
- It aids in the detection of vulnerabilities in your EC2 instances and apps. Furthermore, it enables you to make security testing a more frequent event as part of the development and IT operations.
- Amazon Inspector displays a clear list of security and compliance issues that have been prioritized by severity level.



Install the AWS agent on EC2 Instances

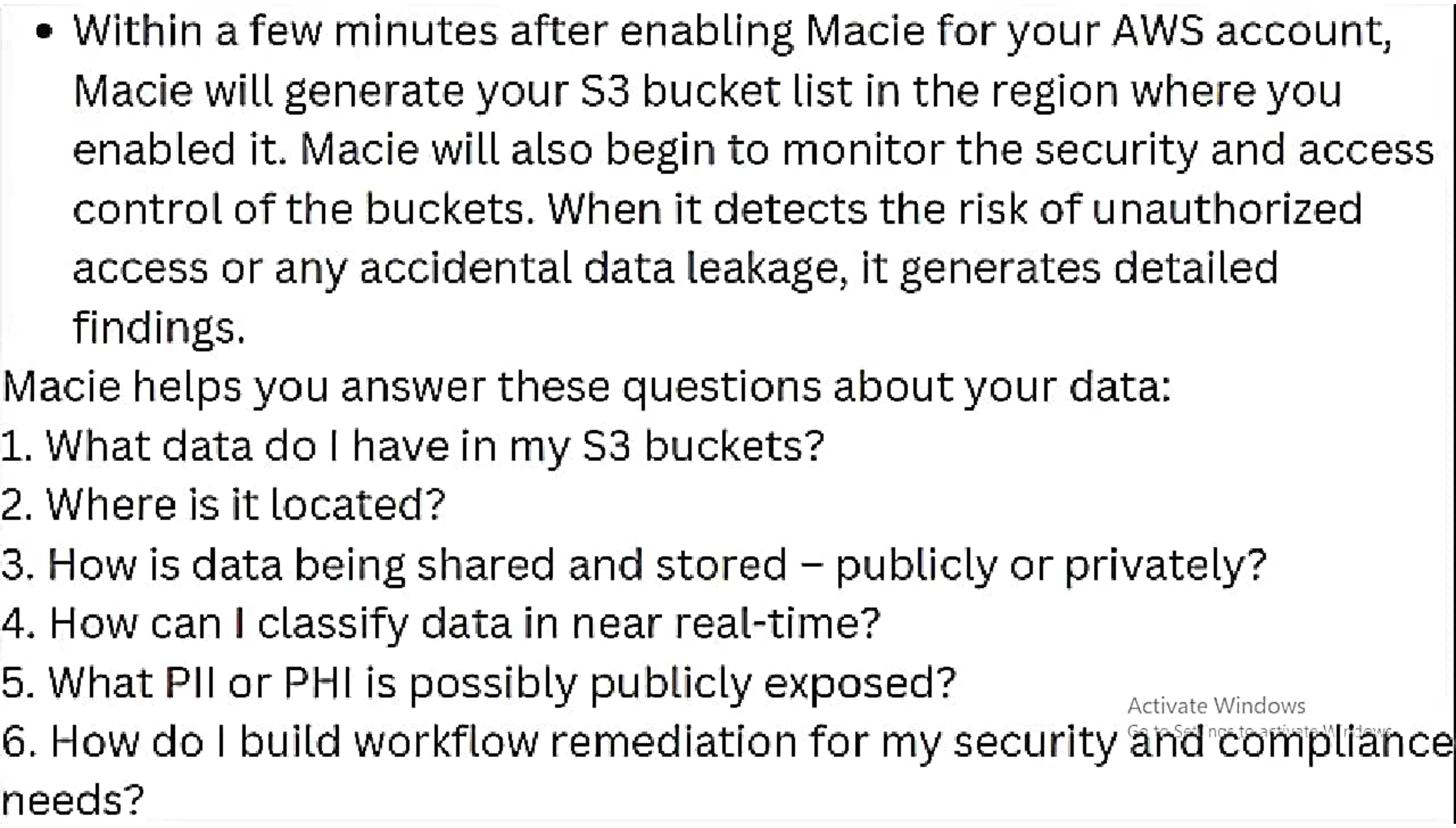
Run an assessment for assessment target according to assessment template

Review findings and remediate issues



AWS Macie

- Protects your sensitive data in AWS
- Protecting valuable data like Personal Identifiable Information (PII) is an extremely high priority and with growing data stored in AWS Cloud, you will feel that you need to automate findings so you don’t have to bother to manually classify data and its permissions.
- Amazon Macie is a security service that uses machine learning to automatically discover, classify and protect sensitive data in the Amazon Web Services (AWS) Cloud.
- Helps identify and alerts you to sensitive data
- It will identify your most at risk user which would lead to a compromise
- Macie can recognize any PII or Protected Health Information (PHI) that exists in your S3 buckets. Macie also monitors the S3 buckets themselves for security and access control.



- Within a few minutes after enabling Macie for your AWS account, Macie will generate your S3 bucket list in the region where you enabled it. Macie will also begin to monitor the security and access control of the buckets. When it detects the risk of unauthorized access or any accidental data leakage, it generates detailed findings.

Macie helps you answer these questions about your data:

1. What data do I have in my S3 buckets?
2. Where is it located?
3. How is data being shared and stored – publicly or privately?
4. How can I classify data in near real-time?
5. What PII or PHI is possibly publicly exposed?
6. How do I build workflow remediation for my security and compliance needs?