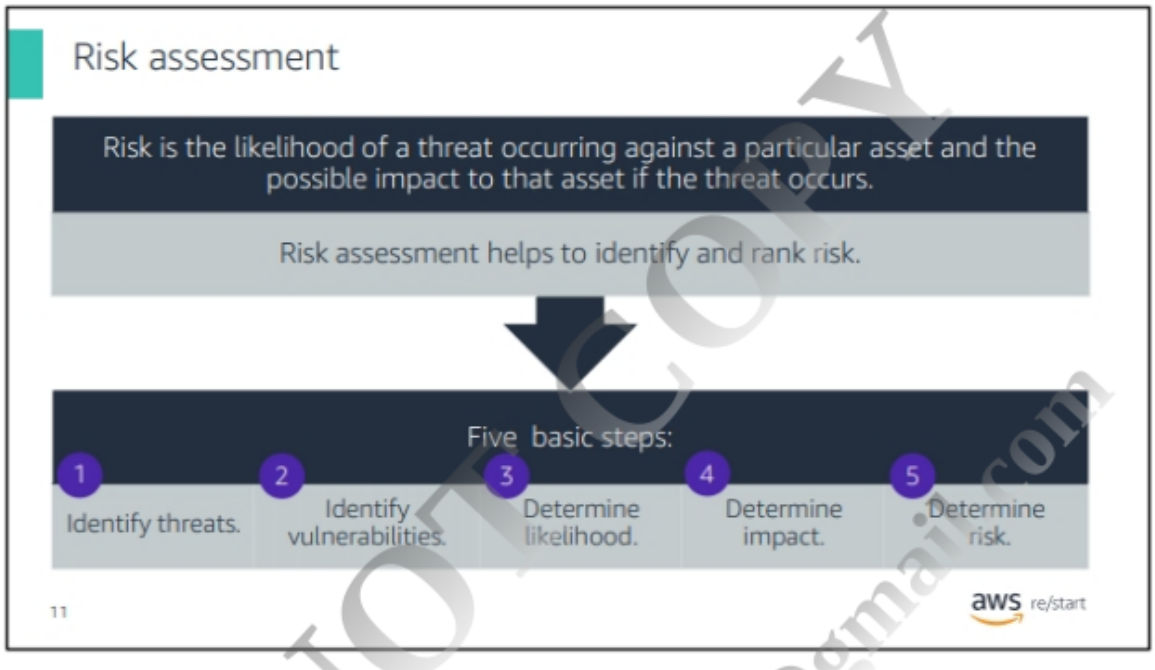
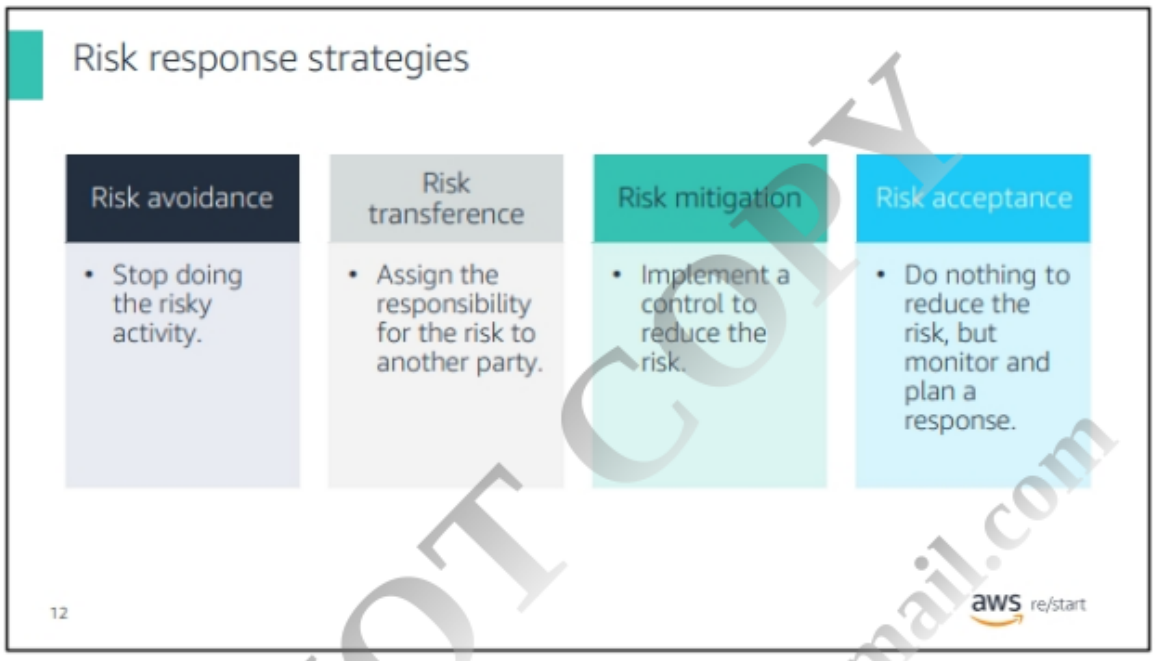
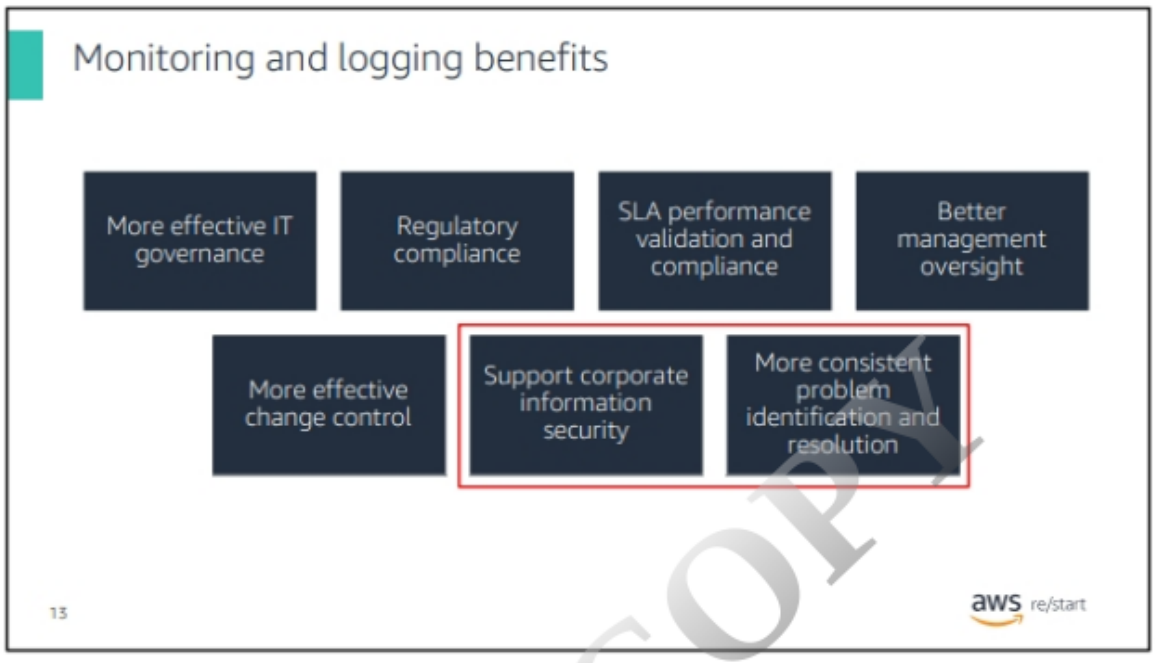


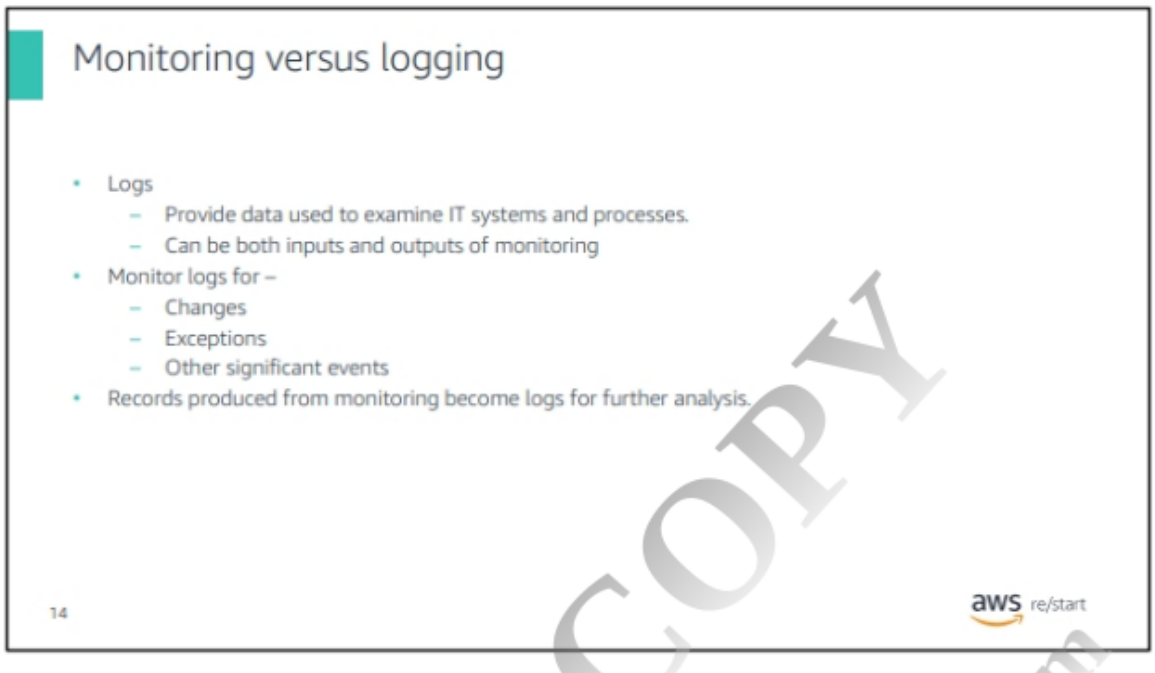
What are the most critical assets or critical business processes that need the most protection?



Based on the results of the risk assessment, decide which security response strategy to use for a particular asset or activity.

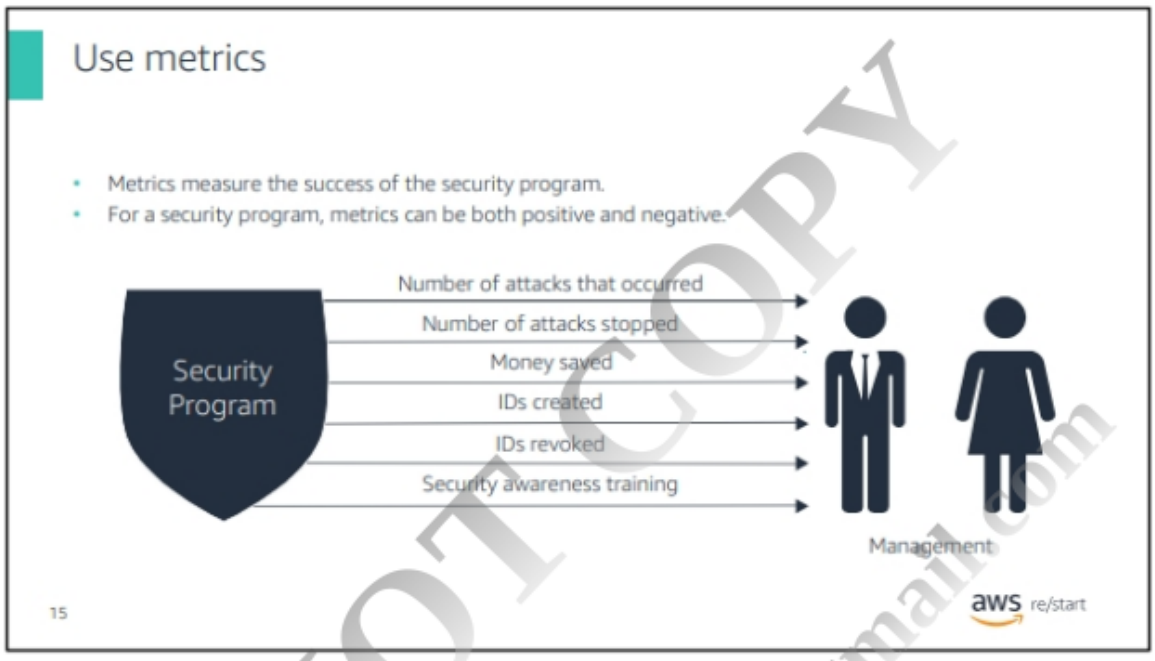


Monitoring and logging also are tools that help in security analysis because they provide the data that is used to identify and resolve security problems.

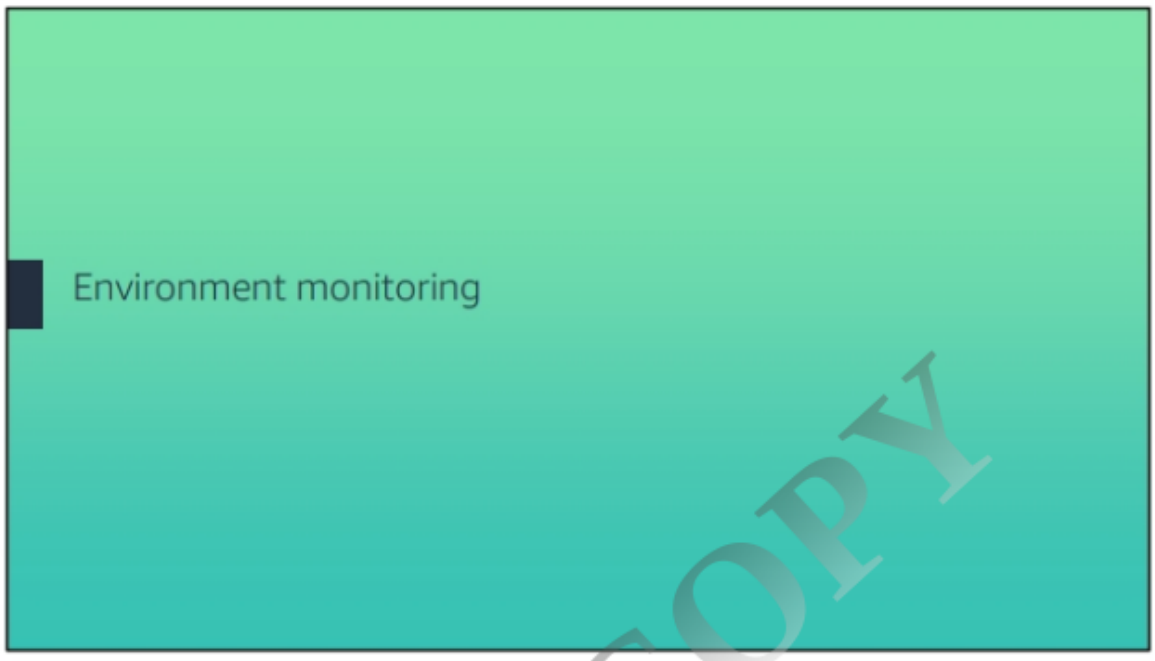


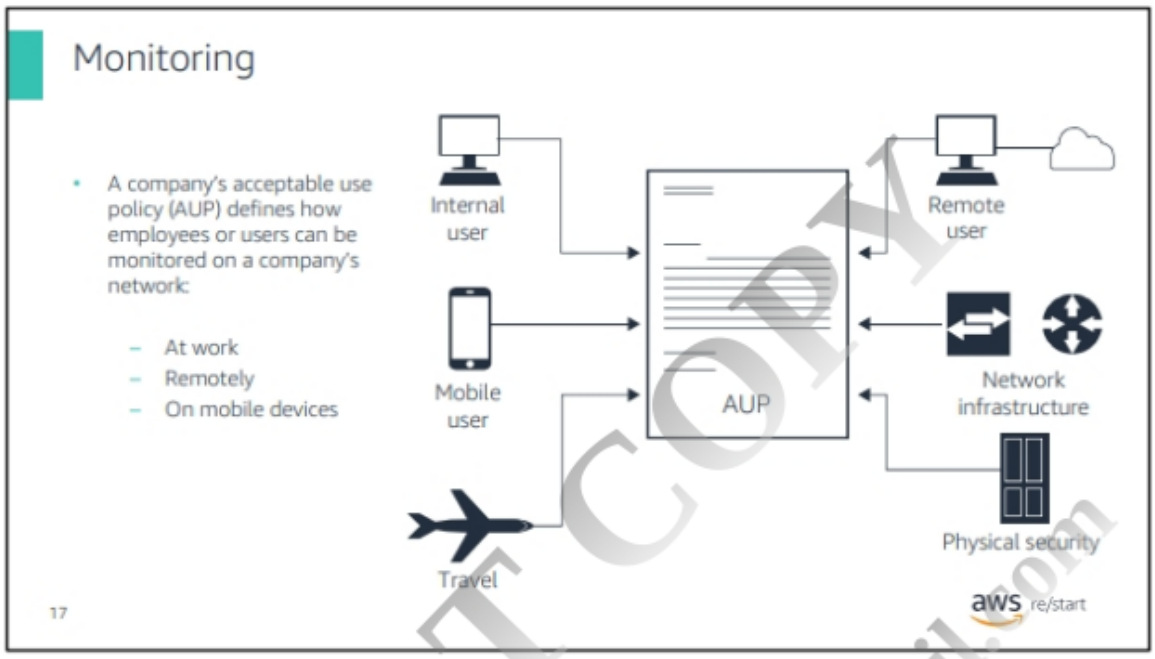
Monitoring and logging complement each other: Log significant events that are monitored in the environment.

The next topics discuss monitoring and logging in more detail.

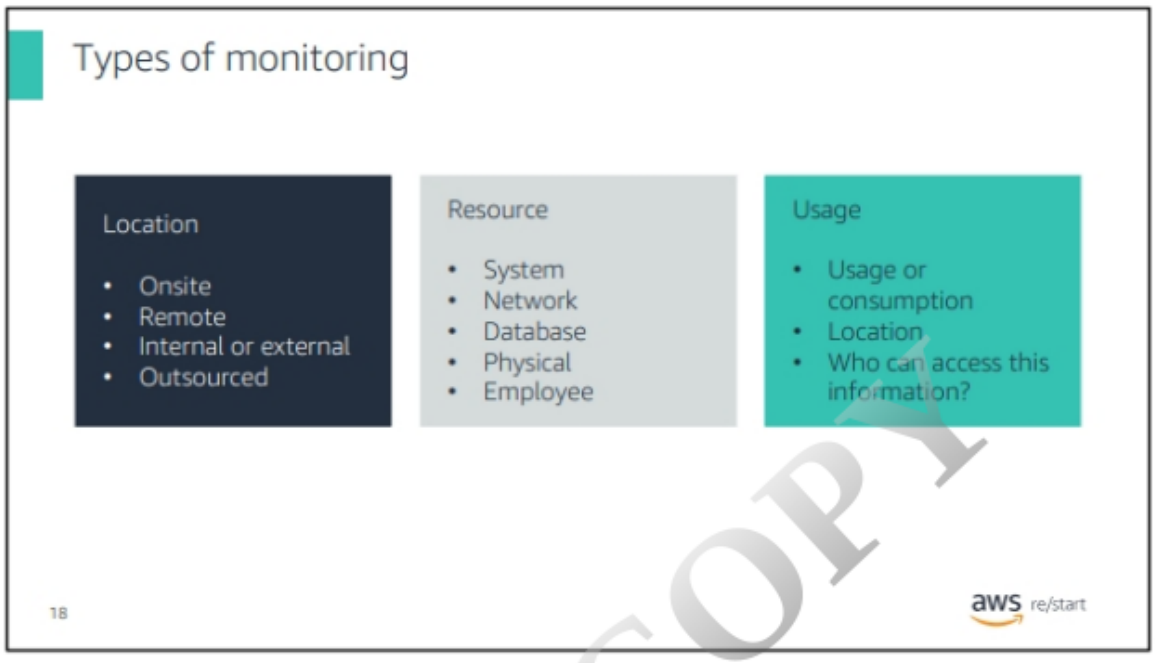


Use metrics to assess and demonstrate the success of your security solution.

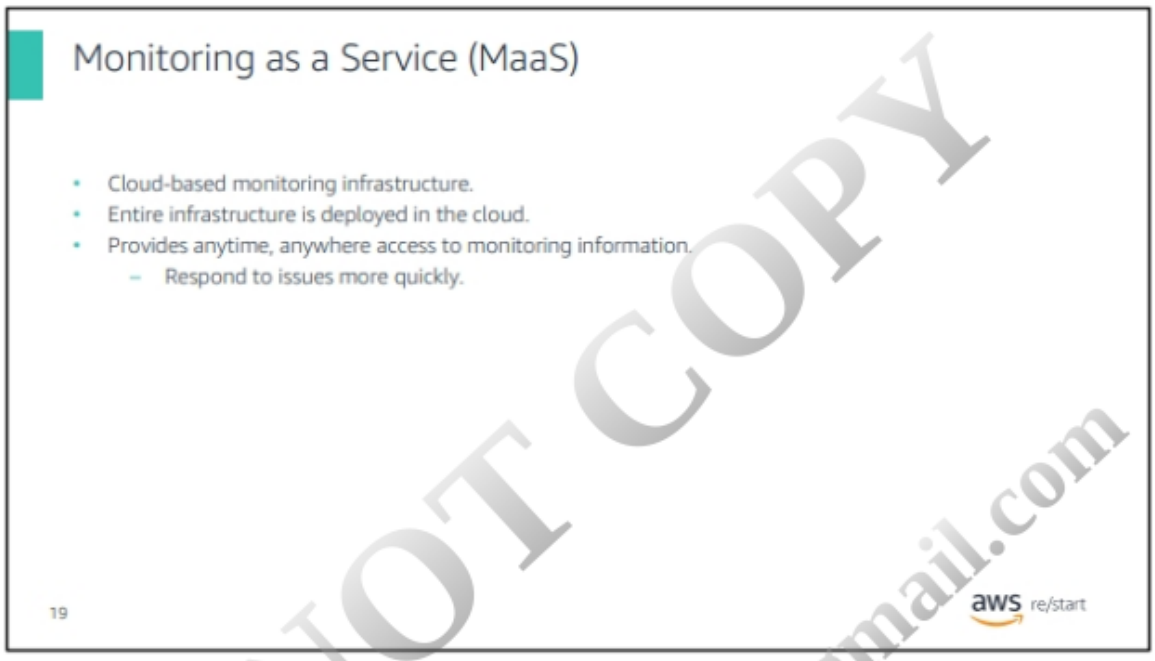




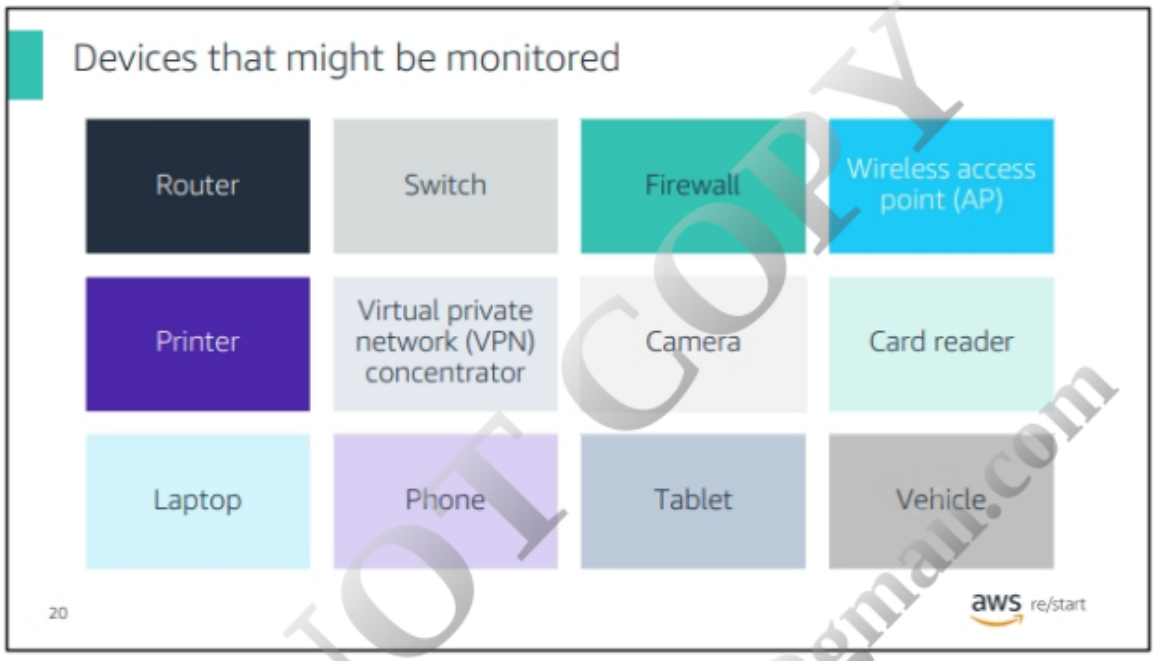
A company can define a set of rules that determine what or who is monitored by creating an acceptable use policy (AUP) document.



The types of monitoring can vary based on where the monitoring occurs and what type of resource or usage is being monitored.



External sources or third parties can provide monitoring. For example, in the AWS Cloud, the Amazon CloudWatch service provides monitoring service for AWS Cloud resources and the applications that you run on AWS.



You can monitor almost any type of device that you can connect to a network.