

#### Security

## Simplify Security Incident Response and Digital Forensics on AWS

# Detecting and responding to security issues in your AWS environment

Enterprise-scale IT environments produce vast quantities of log data, and investigating security incidents in these environments usually entails sorting through that data. As outlined in the AWS Shared Responsibility Model, AWS manages security of the cloud, while security in the cloud is the responsibility of the customer. As the customer, you retain control of what security you choose to implement to protect your own content, platform, applications, systems and networks, no differently than you would for applications in an on-site datacenter. This includes, but is not limited to: encrypting sensitive data, implementing the proper identity and access management policies, and managing operating system, network, and firewall configurations. In the event that a security incident occurs in your AWS environment, you are responsible for determining when the attack happened, how systems were breached, and which resources were compromised.

#### The AWS Solution

1

AWS provides a variety of tools to help customers with their forensics practices in complex, enterprise-scale AWS environments. Logging, monitoring, and resource management services can help you respond more effectively if a security breach occurs by offering the data that enables forensic investigation of the malicious activity. This allows you to quickly determine the root cause and prevent future attacks from successfully exploiting the same vulnerability.

By following a few best practices, you can help ensure that you capture relevant data to perform forensics if a security incident occurs:

#### Turn on AWS CloudTrail in every AWS Region:

Do not limit your CloudTrail logging to AWS Regions that you actively use. Turning CloudTrail on in every AWS Region will allow you to identify unusual behavior more easily, such as AWS services being provisioned from an AWS Region that your organization does not use.

#### Protect log information:

Verify that audit trails are enabled and active for system components, and regularly back them up. Consider storing them in a location that requires different credentials, so attackers cannot delete log files that may provide evidence of their malicious activity.

#### 3 Never ignore AWS abuse communication:

AWS will automatically send an email to your registered email address when an abuse case is filed. Respond immediately, and consider setting up a dedicated email response address. The more promptly you respond to a security incident, the better you can limit its impact on your business.

#### 4) Isolate affected resources immediately:

One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.





## Recover from security incidents more quickly

As AWS adoption grows and architectures become more complex, monitoring and responding to activity across the entire environment by looking at log data becomes an increasingly arduous task. In addition to AWS CloudTrail, AWS Config, AWS CloudWatch, Elastic Load Balancing, VPC Flow Logs, and other AWS services, third-party and custom applications in your AWS account produce log data. These data sources can be an invaluable resource for forensic investigation, but they also contribute to the sheer scale of log data that must be managed. Third-party logging and monitoring solutions available from software vendors in AWS Marketplace can help you deal with this scale by making it easier to determine what data is relevant and what isn't. These tools can be integrated with both AWS-native and thirdparty/custom applications across your on-premises and cloud environments, and dramatically simplify log analysis by correlating activities that may otherwise seem unrelated (Figure 1). Once you have discovered that the security of your environment has been compromised, this correlation helps you rapidly pinpoint the root cause — when the attack commenced, which vulnerability it exploited, which systems were compromised, and when the attack ceased, without error-prone and time-consuming manual processes. From there, you can rebuild the compromised systems so you can get them back into production quickly and mitigate the vulnerabilities that were exploited. By leveraging third-party logging and monitoring tools from AWS Marketplace, you can more effectively perform digital forensics on the AWS Cloud.

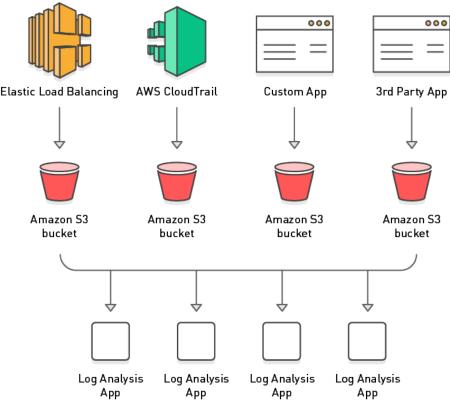


Figure 1. Logging and monitoring solutions in AWS Marketplace simplify forensics by aggregating your log data and enabling more effective correlation

### Get Started with Security Software in AWS Marketplace



Find and deploy the solution you need in minutes



Save money with pay-as-you-go pricing



Scale globally across all AWS Regions



