OPCITO TECHNOLOGIES

Improving Cloud Security And Intrusion Detection With AWS

About The Customer

The customer is a FinTech organization that provides various financial services worldwide. With an increasing need for digital services, the company decided to transition a significant portion of its operations to the cloud, requiring an advanced cloud security solution.

Business Challenge

The client manages large volumes of sensitive and proprietary data, necessitating a robust and secure cloud environment. The organization sought a solution that could provide extensive visibility into its AWS environment, ensure compliance with stringent regulations like GDPR and PCI-DSS, and detect and respond to security threats in real time. Simultaneously, the company wanted to minimize human errors in managing configurations and access controls.

How Opcito Helped

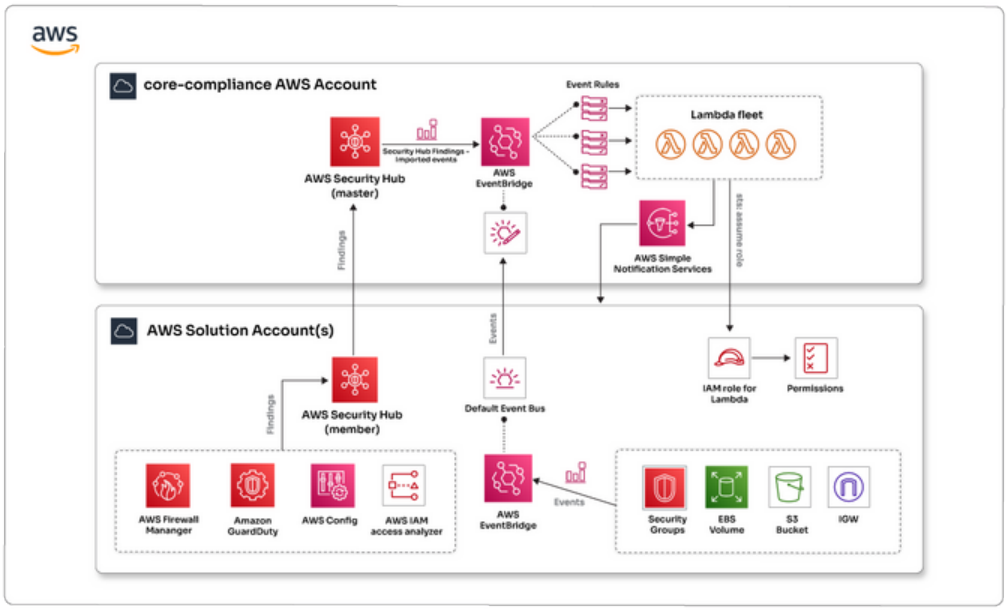
Opcito proposed a comprehensive solution that involved implementing robust CSPM and IDS on AWS, powered by Terraform, for infrastructure automation to meet these requirements. Terraform was selected for its ability to automate infrastructure management, thus reducing human error.

The solution employed a suite of AWS services, each addressing different aspects of the cloud security need.

- **AWS Config:** AWS Config was employed to track and manage configurations of AWS resources. Config rules were tailored to match the GDPR and PCI-DSS compliance regulations, ensuring automatic checks were in place. By providing insights into resource configuration changes, AWS Config aided in maintaining a secure and compliant environment.
- **AWS CloudTrail:** AWS CloudTrail was used to log and monitor all AWS API calls. This continuous surveillance included tracking who made the call, the call's source IP, and whether it was successful or not, providing an internal audit mechanism.

India office +91 (20) 6712 4100 US office +1 (650) 772 4442

- **Amazon GuardDuty:** GuardDuty served as the IDS, offering intelligent threat detection. It analyzed AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs to identify unusual activity patterns or unauthorized behavior.
- **Amazon CloudWatch:** Amazon CloudWatch was deployed for monitoring AWS resources and applications, including the collection and tracking of metrics. CloudWatch alarms were configured to trigger responses based on predefined rules. This allowed the security team to detect potential issues rapidly and respond promptly.
- **AWS Security Hub:** An AWS Security Hub served as the central console, providing a comprehensive view of the security alerts and compliance status aggregated from various AWS services, including AWS Config, GuardDuty, and CloudWatch.
- **Amazon EventBridge:** Used to deliver a stream of real-time data from AWS services to the AWS Security Hub. It triggered automated responses when specific changes or security events were detected, improving the agility and effectiveness of the incident response.
- **AWS IAM Access Analyzer:** Deployed to analyze resource policies and provide detailed reports on resources accessible outside the AWS account, helping prevent unintended access or data leaks.
- **Terraform:** Terraform scripts were written to automate the deployment and management of the AWS resources, ensuring consistency and reducing the possibility of human errors.



Technologies, Tools, and Platforms used

- AWS CONFIG
- AWS CLOUDTRAIL
- AMAZON GUARDDUTY
- AMAZON CLOUDWATCH
- AWS SECURITY HUB
- AMAZON EVENTBRIDGE
- AWS IAM ACCESS ANALYZER
- TERRAFORM

India office +91 (20) 6712 4100

US office +1 (650) 772 4442

Benefits

BOLSTERED SECURITY	Implementing the AWS suite and Terraform, led to a substantial improvement in the cloud security posture.
VISIBILITY	The robust CSPM and IDS system provides holistic visibility into the AWS environment.
COMPLIANCE	Ensures continuous compliance checks against GDPR and PCI-DSS.
THREAT DETECTION	Proactively detects and responds to security threats.
EXPANSION	Successfully implementing this project has opened doors for expansion of the customer's cloud environment.

About Opcito

At Opcito, we believe in designing transformational solutions for our customers, start-ups, and enterprises, with our ability to unify quality, reliability, and cost-effectiveness at any scale. Our core work culture focuses on adding material value to your products by leveraging best practices in DevOps, like continuous integration, continuous delivery, and automation, coupled with disruptive technologies like containers, serverless computing, and microservice-based architectures. We also believe in high standards for quality with a zero-bug policy and zero downtime deployment approach.

India office +91 (20) 6712 4100 US office +1 (650) 772 4442