PRESIDIO®

CASE STUDY

CONTINUOUS COMPLIANCE

STARTINGPOINT

aws partner network

Advanced Consulting Partner

THE CUSTOMER

StartingPoint is a SaaS customer operations and experience platform for service-based companies, firms, and teams to simplify customer on-boarding, project management, helpdesk and service management, team management, and communication. StartingPoint is designed to help companies provide an amazing customer experience after they gain a customer by providing companies and teams an efficient, lean customer operations platform that can be deployed, customized, and leveraged quickly. These core values help companies and their teams decrease customer churn, drive customer service excellence, and increase team productivity.

THE CHALLENGE

As a provider of hosted software, maintaining customer trust is very important. Security misconfiguration and insufficient logging & monitoring are two of the top 10 web application security risks highlighted by the industry recognized OWASP Top 10 list for 2019. Setting configuration and compliance standards and remediating misconfigured cloud resources improves security in the cloud and thereby guards customer trust in the service that StartingPoint delivers.

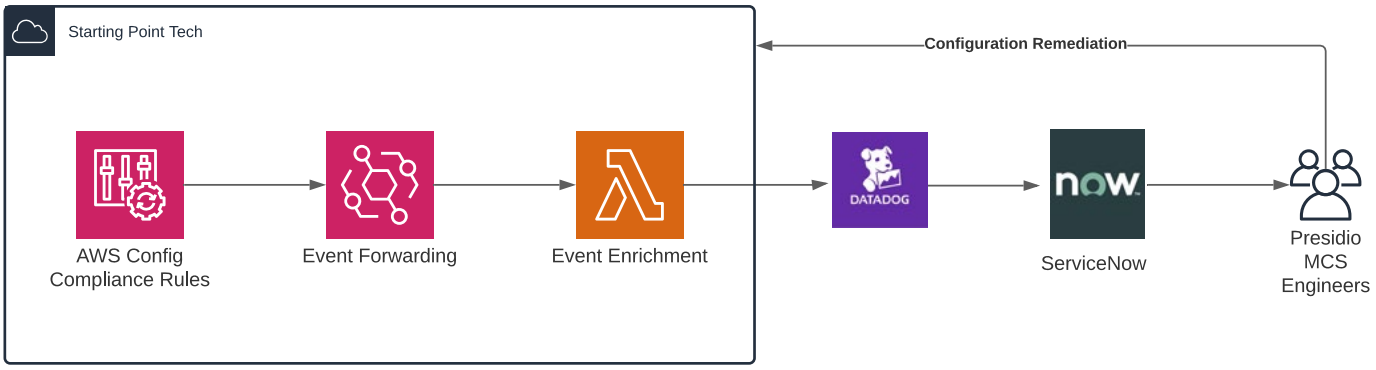
StartingPoint worked with Presidio to ensure their infrastructure stays compliant with the policies they have in place to protect their customer's data. As part of onboarding StartingPoint 's AWS account to Presidio Managed Cloud Services (MCS), key compliance requirements were identified including:

- Encryption of all data at rest
- Encryption of all data in transit between the customer and the StartingPoint Tech application entry point
- Locking down and monitoring AWS root credentials
- AWS access keys and passwords for IAM users are rotated every 90 days
- CloudTrail is enabled and configured properly
- Security Groups limit broad access to sensitive ports
- AWS Config recorders are enabled in all regions
- Load Balancer access logs and VPC flow logs are configured
- RDS backups are enabled and snapshots are private
- Backup Plans are enabled
- S3 buckets deny public access

HOW PRESIDIO HELPED STARTINGPOINT SOLVE THE PROBLEM

Presidio deployed AWS Config Rules and AWS EventBridge Rules for these compliance requirements through CloudFormation. Compliance violations events from AWS Config and key management events from AWS CloudTrail are matched in EventBridge rules and forwarded through SNS to Datadog. Within Datadog event monitors have been configured to alert on those AWS Config and AWS CloudTrail events. Through Datadog integration with ServiceNow, Datadog alerts for non-compliant resources generate an Incident, which is fielded by Presidio MCS engineers. Presidio MCS engineers work with StartingPoint to quickly remediate the non-compliant resource.

Presidio MCS' robust SLAs for Incident response and remediation drive quick action by its engineers to assess and remediate Incidents for non-compliant resources rapidly and thoroughly.



SOLUTION OUTCOMES

Prior to implementing these AWS Config rules, non-compliant resources had been running in the customer's account for some time. The time it took to Identify non-compliant resources dropped from days, and in some cases weeks, to seconds.

Once a non-compliant resource is identified, Presidio MCS engineers are able to respond within minutes to remove the resource, remediate the configuration, or contact the customer to provide detailed documentation on customer-required actions (e.g., rotating the IAM user access key). With the new monitoring, integration and response from Presidio Managed Cloud Services, time to remediate non-compliant resources, for most events, dropped from weeks to less than 20 minutes.

In one case of rapid compliance remediation, a new VPC was created which did not adhere to the standard of enabling VPC Flow Logs. An Incident was quickly generated through AWS Config, Datadog and ServiceNow and Presidio MCS engineers responded quickly, notifying the customer and putting the VPC Flow Log configuration into place.

StartingPoint has a significantly improved security posture through their partnership with Presidio Managed Cloud Services. Through this work, StartingPoint is an excellent position to begin moving forward with any compliance standard or regulatory certification they may wish to pursue.

In summary, by working with Presidio Managed Cloud Services, StartingPoint has:

- Significantly improved their security posture in the cloud
- Decreased detection of insecure configurations from weeks to seconds
- Decreased time-to-remediation of resources not complying with policy from days to hours
- Built a strong foundation for future compliance or regulatory certifications like SOC2, PCI, etc.

SECURITY

Each tier of the application has the least privilege from IAM and networking perspectives.

Governance and security services provide additional insight into the security of the overall environment. Data is protected at rest (KMS- S3, EBS, EFS, RDS) and in transit (ACM- ALB).

OPERATIONAL EXCELLENCE

Upgrades to underlying EC2 instances, Wordpress application containers (performed through CodePipeline and CodeDeploy) and database versions are automated and require zero downtime for completion.

Logging and monitoring are provided by Datadog with a central view into workload and account health.

LEARN MORE

For more information contact us at inquiries@presidio.com.