AWS SECURITY RECOMMENDATIONS FOR:

SKINQUE

By Sarah Sullivan.

Skinque

34b Capel Street,
Dublin 2,
Ireland.
(01) 456 - 7890

Security Recommendations

February 22nd 2021

Overview

Your company Skinque, has contacted me to offer security recommendations in preparation for your business move to Amazon Web Services (AWS). It is my understanding that Skinque runs an online retail site that specializes in selling handmade cruelty free skin care products. It is fantastic to hear that you ship your products globally from your Skinque headquarters in France. I've learned that your on premises infrastructure is limited and you want to begin expanding into new markets.

I have reviewed your web application and the different offerings of the mobile application on both the Android PlayStore and Apple store, but I have been briefed that you would now like to add more features in the coming months, as well as have more capabilities to analyze your website visitors activities, to better inform your business growth plan.

Goals

1. **Be clear on what security recommendations suit you:** It is my job to make this transition as easy as possible for you, which is why I will do all the research on the correct security measures to offer you and your company, so rest assured everything will be up to the highest standard.
2. **Your online retail site will be kept completely safe:** These recommendations are designed to keep SKinque's retail site safe, both from an operational standpoint and to potential outside attacks.

What Customers Who Use AWS Security Solutions Say:

“The AWS WAF Security Automations solution is like a dream come true because it has made security so much easier, better, and more scalable. We talk about it all the time—how did we ever survive before moving over to AWS WAF?"

Thomas Wick - eVitamins.

"We love it when we are able to simply provide extra security without any inconvenience."

- Roger Zou on Amazon GuardDuty. SnapInc.

“It’s almost as if no limitations exist on the AWS Cloud. We’re able to scale up machines to do whatever we want without any real concern, be it cost or security." - Matt O'Halloran.

IT Director, Ascender HCM

Security, Identity & Compliance on AWS

Please read the below to familiarise yourself with what AWS can offer in terms of security to Skinque:

Data Protection

AWS provides services that will help you protect your data, accounts and workloads from unauthorized access. AWS data protection services provide encryption, key management and threat detection that continuously monitors and protects your accounts and workloads.

Infrastructure Protection

AWS protects your web applications by filtering traffic based on rules that you create. For example, you can filter web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allows you to block common attack patterns, such as SQL injections or cross-site scripting.

Identity & Access Management

AWS Identity Services enable you to securely manage identities, resources and permissions at scale. With AWS, you have identity services for your workforce and customer-facing applications to get started quickly and manage access to your workloads and applications.

Threat Detection & Continuous Monitoring

AWS identifies threats by continuously monitoring the network activity and account behavior within your cloud environment.

Compliance & Data Privacy

AWS gives you a comprehensive view of your compliance status and continuously monitors your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows.

Why Choose AWS for Security?

Using AWS for security, Skinque will gain the control and confidence needed to securely run the most **flexible** and **secure** cloud computing environment available today. As an AWS customer, you will benefit from AWS data centers and a network architected to **protect your information**, identities, applications, and devices. With AWS, you can improve your ability to meet core security and compliance requirements, such as data locality, protection, and confidentiality with our comprehensive services and features. AWS allows you to **automate** manual security tasks so you can shift your focus to scaling and innovating your business. Plus, you pay only for the services that you use. All customers benefit from AWS being the only commercial cloud that has had its service offerings and associated supply chain vetted and accepted as secure enough for top-secret workloads.

Benefits

Scale Securely with Superior Visibility and Control

With AWS, YOU control where your data is stored, who can access it, and what resources your organization is consuming at any given moment. Identity and access controls combined with continuous monitoring for near real-time security information makes sure that the right resources have the right access at all times, wherever your data is stored.

Automate and Reduce Risk with Deeply Integrated Services

Automating security tasks on AWS allows a more secure solution, by reducing human configuration errors and giving your team more time to focus on other work critical to your business. Automating makes it easier for your security team to work closely with developer and operations teams to create and deploy code faster and more securely.

Build with the Highest Standards for Privacy and Data Security

AWS is careful about your privacy. With AWS, you can build on the most secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and manage retention. All data flowing across the AWS global network that interconnects our data centers and regions is automatically encrypted at the physical layer before it leaves our secured facilities.

Largest Ecosystem of Security Partners and Solutions

Extend the benefits of AWS by using security technology and consulting services from familiar solution providers you already know and trust. We have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing day to day management.

Inherit the Most Comprehensive Security and Compliance Controls

To help in Skinque's compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet security and compliance standards for your company.

Strategic Security

AWS is designed to help you build secure, high-performing, resilient, and efficient infrastructure. Our security services and solutions are focused on delivering the following key strategic benefits crucial to helping you implement your organization's optimal security posture:

Prevent

Define user permissions and identities, infrastructure protection and data protection measures for a smooth and planned AWS adoption strategy

Detect

Gain visibility into your organization's security posture with logging and monitoring services. Ingest this information into a scalable platform for event management, testing, and auditing

Respond

Automated incident response and recovery to help shift the primary focus of security teams from response to analyzing root cause

Remediate

Leverage event driven automation to quickly remediate and secure your AWS environment in near real-time

Ok, let’s examine my AWS Security recommendations to Skinque:

Identity & Access Management

RECOMMENDATION 1

Firstly, I am suggesting that you securely manage access to your services and resources by using **AWS IAM** (Identity and Access Management). AWS IAM enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

With AWS IAM you can create users, assign them individual security credentials or request temporary security credentials to provide users access to AWS services and resources. You can manage permissions in order to control which operations a user can perform. You can create roles in IAM and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. You can enable identity federation to allow existing identities (users, groups, and roles) in your enterprise to access the AWS Management Console, call AWS APIs and access resources, without the need to create an IAM user for each identity.

Price: IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.

Why do I recommend Skinque use IAM? AWS IAM is at the heart of AWS security because it empowers you to control access by creating users and groups, assigning specific permissions and policies to specific users, setting up multi-factor authentication (MFA) for additional security, and so much more. And to top it all off, IAM is free to use! So why not!

RECOMMENDATION 2

I would also suggest Skinque take advantage of **AWS Organizations.** AWS Organizations helps to centrally manage and govern your environment as you grow and scale your AWS resources. And since Skinque is planning to expand into new markets, this is the right service to take advantage of. By using AWS Organizations, you can programmatically create new AWS accounts and allocate resources, group accounts to organize workflows, apply policies to accounts or groups for governance and simplify billing by using a single payment method for all of your accounts. AWS Organizations is also integrated with other AWS services, so you can define central configurations, security mechanisms, audit requirements and resource sharing across accounts in your organization.

Price: AWS Organizations is available to all AWS customers at no additional charge.

Why do I recommend Skinque use AWS Organizations? Skinque can use AWS Organizations to create a security group within their team and provide users with read-only access to all of the company resources to identify and mitigate security concerns.

Detection

Let’s now take a look at detectioning a potential security issue. Here are my recommendations.

RECOMMENDATION 3

Firstly, let’s take a look at **AWS CloudWatch.** Amazon CloudWatch is a monitoring and observability service. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS and on-premises servers. You can use CloudWatch to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly. To take action quickly, you can set up automated actions to notify you if an alarm is triggered and automatically start auto scaling, for example, to help reduce mean-time-to-resolution.

Price: With Amazon CloudWatch, there is no up-front commitment or minimum fee; you simply pay for what you use. You will be charged at the end of the month for your usage. However, as Skinque is only starting out using AWS, I would suggest we stick with the Free Tier on AWS for most of our security recommendations. Most AWS Services (EC2, S3, Kinesis, etc.) send metrics automatically for free to CloudWatch. Many applications should be able to operate within these free tier limits. You can learn more about AWS Free Tier here.

Why do I recommend Skinque use AWS CloudWatch? Using CloudWatch alarms to detect any configuration changes involving AWS security groups will help you prevent unexpected inbound and/or outbound rule modifications that may lead to unrestricted or unauthorized access to Skinque’s resources or web apps/page etc.

RECOMMENDATION 4

The next suggestion I have is for Skinque to use **AWS CloudTrail.** It is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

Price: You can view, filter, and download the most recent 90 days of your account activity for all management events in supported AWS services free of charge. You can set up a trail that delivers a single copy of management events in each region free of charge. Once a CloudTrail trail is set up, Amazon S3 charges apply based on your usage. You will be charged for any data events or additional copies of management events recorded in that region.

Why do I recommend Skinque use AWS CloudTrail? I think it would be a good idea to make use of CloudTrail as Skinque is implementing security features across the online retail store. It could be useful to have an insight into user activity - who is doing what online that may or may not affect the overall security of the company. AWS CloudTrail provides a number of security features to consider as you develop and implement your own security policies. Please be aware that CloudTrail doesn't represent a complete security solution, so treat CloudTrail as a helpful consideration rather than prescription.

RECOMMENDATION 5

My 5th recommendation for Skinque is to utilize **Amazon GuardDuty**. It is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With GuardDuty, you have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

Price: Any new account to Amazon GuardDuty can try the service for 30-days at no cost in each supported region. You will have access to the full feature set and detections during the free trial. This makes it easy for you to experience Amazon GuardDuty at no cost and take the guesswork out of the cost of the service beyond the free trial.

Why do I recommend Skinque use AWS GuardDuty? Skinque could benefit greatly from using AWS GuardDuty. GuardDuty security findings are informative and actionable for security operations, findings include the affected resource's details and attacker information, such as IP address and geo-location. GuardDuty makes enablement and management across multiple accounts easy.

RECOMMENDATION 6

The next suggestion I have for Skinque is to make use of **AWS Config.** It is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Price: You pay $0.003 per configuration item recorded in your AWS account per AWS Region. A configuration item is recorded whenever a resource undergoes a configuration change or a relationship change. The resource could be an AWS, third party or custom resource. You can stop recording configuration items at any time and still continue to access the previously recorded configuration items. Charges per configuration item are rolled up into your monthly bill.

Why do I recommend Skinque use AWS Config? I suggest AWS Config for Skinque because Config monitors the resources in your AWS account and can trigger alerts and events. With config, you could automatically run security compliance code on resources. This could be beneficial as you could concentrate wholly on getting your business up and running online, without worrying about manually running code.

Infrastructure Protection

RECOMMENDATION 7

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

Price: All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks. I would advise to stick with the Free Tier version for now, as Skinque is still a small company, we don’t need to waste money on Shield Advanced for the first few months at least, but we can revisit in the near future as Skinque grows and expands.

Why do I recommend Skinque use AWS Shield? DDOS attacks are quite common and can be detrimental to online business. Sometimes a DDOS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. While attackers just simply do it for “fun”, it will not be fun for Skinque when they may begin to lose money due to a DDoS attack taking place. So I suggest utilising AWS Shield for protection.

RECOMMENDATION 8

My next suggestion is to consider **AWS WAF.** It is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injections or cross-site scripting, and rules that filter out specific traffic patterns you define. AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules.

Price: With AWS WAF, you pay only for what you use. The pricing is based on how many rules you deploy and how many web requests your application receives. There are no upfront commitments.

Why do I recommend Skinque use AWS WAF? I am suggesting AWS WAF as I think it is important to have Skinque as secure and reliable as possible. But configuration is so important with AWS WAF. Here's an example of where things can go wrong. Capital One used AWS WAF to protect their web application, but it was not configured properly, so because of this a hacker was able to get the access to their data in an S3 and download it. If you decide to opt for AWS WAF, please do not hesitate to contact me and I can discuss the correct configuration settings with you.

Data Protection

RECOMMENDATION 9

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Identifying and protecting sensitive data at scale can become increasingly complex, expensive, and time-consuming. Amazon Macie automates the discovery of sensitive data at scale and lowers the cost of protecting your data. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII). Macie's alerts, or findings, can be searched and filtered in the AWS Management Console and sent to Amazon EventBridge, formerly called Amazon CloudWatch Events, for easy integration with existing workflow or event management systems, or to be used in combination with AWS services, such as AWS Step Functions to take automated remediation actions. This can help you meet regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Privacy Regulation (GDPR).

Price: You can get started with Amazon Macie by leveraging the 30-day free trial for bucket evaluation. The trial includes 30-days of Amazon S3 bucket inventory and bucket-level security and access control assessment at no cost. After the 30 day free trial, you are charged based on the number of Amazon S3 buckets evaluated for bucket-level security and access controls and the quantity of data processed for sensitive data discovery. For sensitive data discovery jobs, the first 1 GB processed every month in each account comes at no cost. For each GB processed beyond the first 1 GB, charges will occur. You can quickly get started with Macie leveraging the

30-day free trial. Each new account that is enabled with Macie receives this free trial period, even in multi-account configurations.

Why do I recommend Skinque use AWS Macie? I recommend making use of the free 30 day trial to see if it is something that Skinque could benefit from using. It is important to note that companies are automating increased security and controls. Automating security and controls is probably the biggest reason to make the move to the cloud, it just makes your life easier!

RECOMMENDATION 10

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

Price: Each customer master key (CMK) that you create in AWS Key Management Service (KMS) costs $1/month until you delete it, regardless of where the underlying key material was generated by the service, a custom key store, or if you imported it. For a CMK with key material generated by the service, if you opt-in to have it automatically rotate the key each year, each new key version raises the cost of the CMK by $1/month. AWS KMS retains and manages each previous version of the CMK to ensure you can decrypt data encrypted under previous versions. You are not charged an ongoing monthly fee for the data key pairs themselves as they are neither stored nor managed by the service. In the month a key is created, the $1 monthly charge for key storage will be a prorated fee to the nearest full hour.

Why do I recommend Skinque use AWS KMS? It is highly recommended to rotate your CMK's to ensure the security of your cloud infrastructure. When automatic key rotation is enabled, KMS generates new cryptographic material every 365 days and retains the older cryptographic material (old key). In this way, both keys can be used to encrypt or decrypt data. There are various benefits of enabling automatic rotation of CMK. Properties of CMK's such as key ID, key ARN, policies, permissions do not change. It is not required by the user to remember any schedule or calendar to update CMK, which could be valuable for a new company to AWS - as it is one less thing to remember and more time to focus on other aspects of the business!

RECOMMENDATION 11

AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates. With AWS Certificate Manager, you can quickly request a certificate, deploy it on ACM-integrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API

Gateway, and let AWS Certificate Manager handle certificate renewals. It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally.

Price: Public and private certificates provisioned through AWS Certificate Manager for use with ACM-integrated services are free. You pay only for the AWS resources you create to run your application. With AWS Certificate Manager Private Certificate Authority, you pay monthly for the operation of the private CA and for the private certificates you issue.

Why do I recommend Skinque use AWS Certificate Manager? TLS certificates are a type of digital certificate, issued by a Certificate Authority (CA). The CA signs the certificate, certifying that they have verified that it belongs to the owners of the domain name which is the subject of the certificate. This is very important so that visitors to Skinque's website can see that your website is secure. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

Incident Response

RECOMMENDATION 12

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations. Amazon Detective simplifies this process by enabling your security teams to easily investigate and quickly get to the root cause of a finding. Amazon Detective can analyze trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty, and automatically creates a unified, interactive view of your resources, users, and the interactions between them over time. You can get started with Amazon Detective in just a few clicks in the AWS Console. There is no software to deploy, or data sources to enable and maintain.

Price: Amazon Detective is priced based on the volume of data ingested from AWS CloudTrail, VPC Flow Logs, and Amazon GuardDuty findings. You are charged Per Gigabyte (GB) ingested per account/region/month. There is no additional charge to enable these log sources for analysis or for data stored in Amazon Detective. Amazon Detective maintains up to a year of aggregated data for its analysis.

Why do I recommend Skinque use AWS Detective? Amazon Detective makes it much easier to conduct faster and more efficient investigations into security issues across AWS workloads. Detective is a region based service, and must be enabled in each region. AWS Detective can be set up in a master-member type account setup the same way GuardDuty can be. Please be aware that AWS Detective will take some time to baseline your environment and regular activity before it can identify all suspect behaviour. AWS Detective is a great addition to any organisation's security toolset.

Compliance

RECOMMENDATION 13

My recommendation to Skinque for Compliance is AWS Artifact - it is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Price: No Cost to AWS customers.

Why do I recommend Skinque use AWS Artifact? I recommend that Skinque take advantage of using AWS Artifact to assess and validate the security and compliance of the AWS infrastructure and services that you use. If you are obligated to demonstrate the compliance of your cloud architectures during system design, development and audit life cycles, which Skinque is, I would wholly take advantage of using Artifact.

Conclusion

In conclusion, I hope that I have been able to recommend the appropriate security solutions for Skinque. I have recommended services which cover different aspects of security in the cloud including data and infrastructure protection, identity and access management, threat detection and continuous monitoring, compliance and data privacy, all of which are key fundamental features that AWS security offer to benefit your company. Choosing AWS security solutions for Skinque will offer you a flexible and secure cloud computing environment. You will also benefit from AWS data centers and a network architected to protect your information, identities, applications, and devices. As mentioned previously, AWS allows you to automate manual security tasks so you can shift your focus to scaling and innovating your business, which I know is a major goal for Skinque.

Thank you for contacting me to offer you security recommendations and solutions to ease your transfer to the AWS cloud. I hope the information in this document proves useful to you and your business.

Feel free to reach out so we could discuss this portfolio in more detail if you should need it.