clearscale

aws partner network

Premier Consulting Partner

TrendShift's Cloud-Based HealthCare SaaS Solution with HIPAA

trendshift

Executive Summary

It was just a few years ago that companies began moving their applications from self-hosted, on-site solutions to cloud-based SaaS platforms. The flexibility, security, reliability, and reduced operating costs were hard to pass up — and they're the reason why many companies are still migrating to cloud-based data storage today.

Now, some companies who made the initial transition to the cloud need new solutions. Perhaps their initial service provider wasn't thoroughly vetted, or the service ended up costing more than they expected. Whatever the reason, ClearScale has been performing more cloud-to-cloud migrations than ever before. Here's one of our most successful examples:

The Challenge

Our challenge was multi-faceted: One of our clients in the healthcare industry, TrendShift, needed to improve and expand their web-based application. They were already using a data center for cloud-based applications, but the performance, reliability, and scalability of the platform simply weren't good enough. They also needed a solution that would integrate easily with open-source platforms while still offering enough security to protect sensitive information.

There was a second significant challenge, too: HIPAA compliance. HIPAA, or the Health Insurance Portability and Accountability Act, has been U.S. law since 1996. The most important section of this act is Title II, which sets the standards for digital healthcare data access and transfers while remaining in compliance with privacy regulations set by the U.S. Department of Health and Human Services. Not just any data center can hold, process, and transfer healthcare specific data — only fully compliant cloud services can be used for this kind of migration.

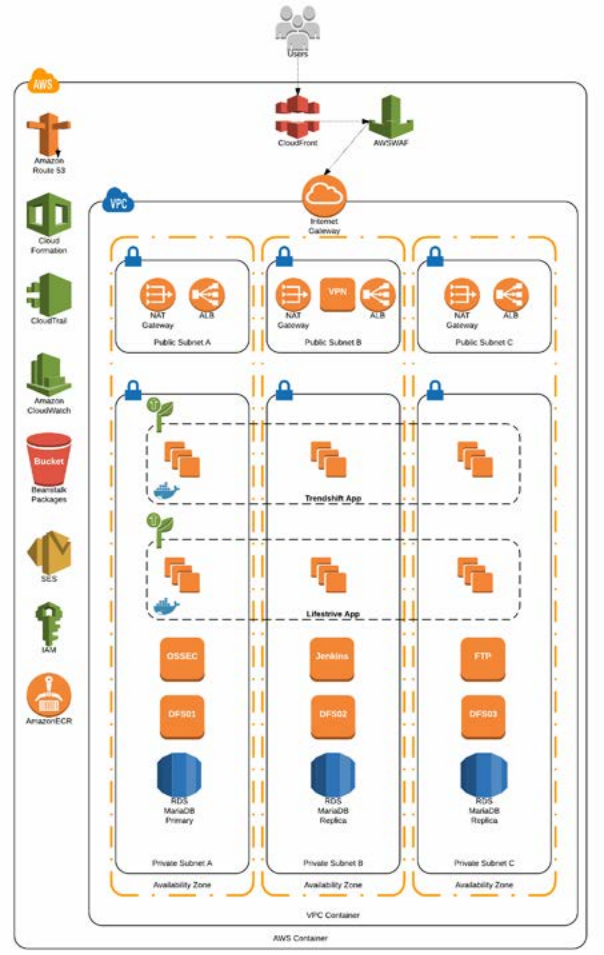
The third significant challenge was cost reduction. TrendShift needed additional reliability and scalability while addressing the legal regulations of the healthcare industry. To keep the cost of this project affordable, the right web platform and services would have to be selected and implemented correctly.

The ClearScale Solution

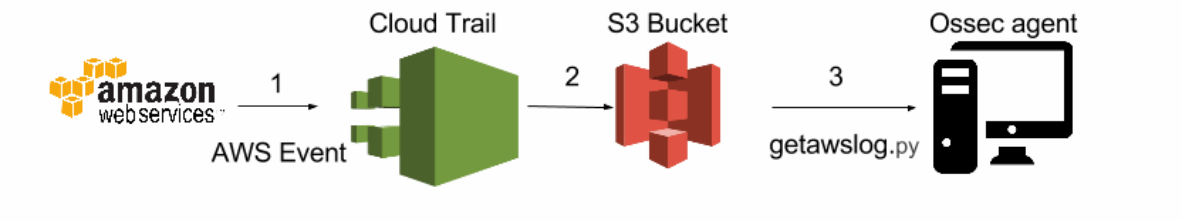
To ensure we met all stated objectives, ClearScale organized a ten-tier plan that we implemented over the course of 13 weeks. We started with building out the application security and storage tiers. From there, our team focused on connectivity and security with the DNS and monitoring tiers. To conclude the development and deployment and ensure future success, we added the final three tiers focused on automation, storage, and analytics. This solution ensured that TrendShift felt the immediate business impact of this migration as well as experiencing a longer-term payoff — all while remaining HIPAA compliant.

Elastic Beanstalk and HIPAA Compliance

The first and most important step was migrating to a reliable, scalable, cost-effective, and HIPAA compliant application platform that allowed the client to develop code without having to deal with dev ops overhead. Amazon Elastic Beanstalk combined with its use of Amazon EC2 Container Service (Amazon ECS) was our immediate choice for this scenario. This deployment solution, which is used by pharmaceutical company Novartis, who trusts that their cloud transfers — which contain highly sensitive data — will be HIPAA compliant. It's also trusted by entertainment giant Netflix as well as NASA's Jet Propulsion Laboratory, which used it for the Mars Curiosity Mission. Why? Because Amazon's ECS isn't just secure; it also boasts impressive reliability (99.95% for each ECS Region) and formidable auto-scaling capabilities, in addition to the low cost of operation that TrendShift needed. Amazon Elastic Beanstalk with Amazon ECS was the perfect place to start.

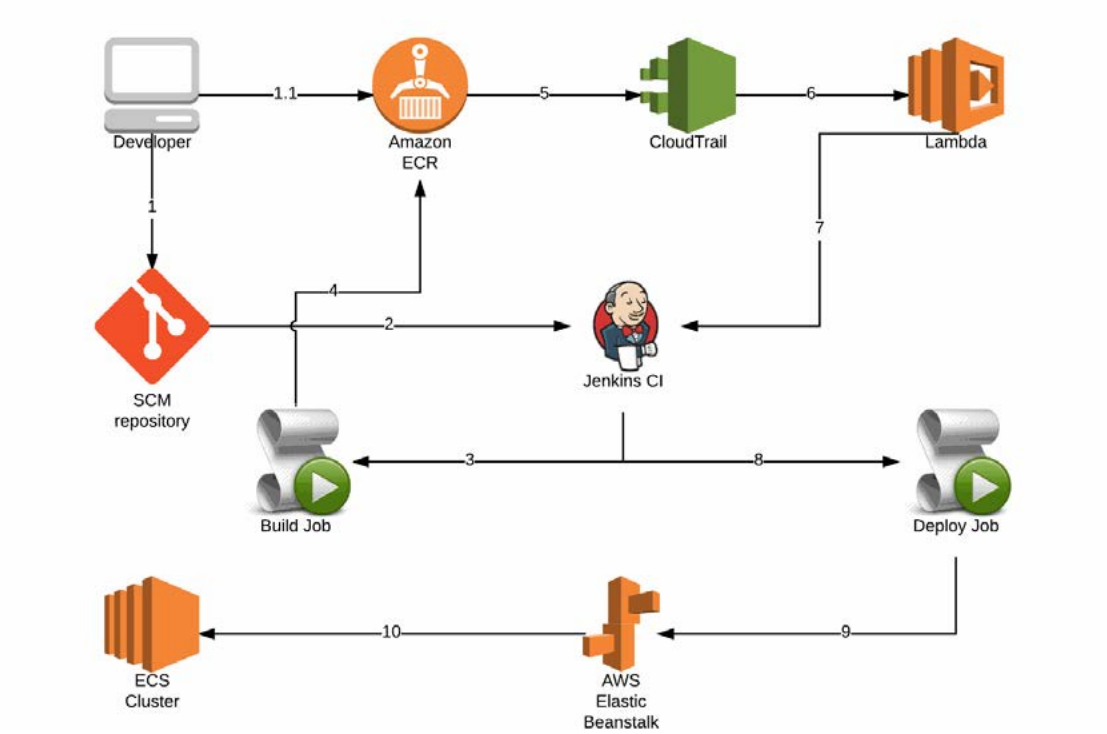


Also, in order to meet the HIPAA compliance standards we needed to make sure all data was encrypted in transit and at rest along with a preferred Intrusion Detection System (IDS). Amazon EBS (Elastic Block Storage) with encryption enabled was the perfect fit to meet the encryption at rest. Forcing SSL encryption for all internal and external communications between the applications and database would satisfy the encryption in-transit requirement. Last, OSSEC being a leader as an - source Intrusion Detection System (IDS), would satisfy this final requirement.



CI/CD with Docker, Jenkins, and Blue/Green Deployments

To properly run and deploy this client's web-based application, we set up Jenkins in conjunction with Docker. Jenkins provides continuous testing for scripts and services, building Docker images and ensuring no faulty code ever reaches the client's application. Once code is deemed ready for deployment, Jenkins creates a new Docker image that is pushed to AWS, and the build is deployed. This allows Beanstalk, another AWS application, to update the application's build with the Docker image; the changes are then pushed to the customer. Remarkably, all of this happens in a matter of hours, if not minutes!



Because Elastic Beanstalk performs an in-place update when you update your application versions, your application may become unavailable to users for a short period of time. It is possible to avoid this downtime by performing a Blue/Green deployment, where you deploy the new version to a separate environment, and then swap CNAMEs of the two environments to redirect traffic to the new version instantly.

With Jenkins CI it's possible to deploy new code revision to the Elastic Beanstalk application environment named as "blue," then after a successful deploy to the "blue" environment swap CNAMEs of the two environments named "blue" and "green."

AWS WAF, CloudWatch, and CloudTrail

To monitor uptime and security requirements and prevent attacks and intrusions, we configured a combination of Amazon WAF, CloudWatch, and CloudTrail. CloudWatch ensures that all functions of an application run quickly and smoothly. WAF security rules were put in place to provide control over which web application traffic to allow. If there's ever a need to scale up, CloudWatch logs events and sends alerts so that additional resources can be dedicated to the application. CloudTrail, on the other hand, monitors the back end of the application, ensuring governance, compliance, and operational and risk auditing services are all being performed. While CloudWatch looks at application demands, CloudTrail notes AWS account activity, including changes to the Management Console, SDKs, and command line tools. Together, these services ensure this client always has automated eyes on their application security and performance.

AWS Migration

Once all of the environments were deployed and tested, we proceeded with synchronizing their database over an IPSEC VPN tunnel to prevent downtime and data loss. Once the data was transferred we performed a mock test of the client traffic to insure the stability of the environment and integrity of data.

After the successful mock migration, we performed a simple DNS switch to the new CloudFront distribution to route all users to the new AWS environment.

Final Result and Benefits

With ClearScale's help, TrendShift was able to get the business improvements they needed. Since launch, they've seen all the cost savings they expected as well as the future-proofing they hoped for. Thanks to our dedicated DevOps team and the flexibility of AWS Platform, ClearScale was able to build a safe, HIPAA compliant and highly reliable solution that performs better than the client's prior deployment.