

# Flux7 Improves Security in AWS with Effective Secret Management

## Electronic Health Record provider meets HIPAA requirements in the cloud with HashiCorp Vault

### Profile

This large provider of electronic record management for healthcare organizations emphasizes the benefits of its cloud offering as a clear selling point in the market. Its healthcare platform seeks to connect doctors, patients and data to drive better health and save lives. In connecting all the people involved in a patient's health care, this organization coordinates care to ensure better health outcomes, whether a patient is in the lab, pharmacy, doctor's office or imaging center. By serving the entire healthcare ecosystem, this company is able to offer its award-winning EHR at no cost to practices.

### Challenge

Managing patient healthcare records means that this organization is subject to HIPAA requirements. As client data is the lifeblood of this organization, it also has strict internal guidelines to protect the security of this data. As a result, the organization sought best-in-class security for its cloud-based solution. Part of its challenge in doing so was managing its various credentials such as passwords. While the organization had developed a homegrown solution for credential management, it was not easy to manage and did not meet all of the company's security and availability requirements.

Additionally, to maintain customer use and satisfaction it is imperative that the organization maintain standards for the highest levels of availability, with a goal of maintaining an RPO of 5 minutes and RTO of 15 minutes. As a result, the proposed security solution needed to maintain the highest levels possible for availability, reliability and repeatability.

### Solution

The firm felt that they needed a commercial grade secret management system and believed HashiCorp Vault was the answer. They called in the AWS experts at Flux7 who based on their deep AWS security and compliance experience affirmed the organization's belief that Vault would indeed best address their requirements.

#### *The Vault solution addressed the healthcare provider's key goals through:*

- **Management of Dynamic and Static Secrets:**

Vault provides an interface to static secrets in encrypted form as well as dynamic secrets with tight security controls. As this firm had a need to manage both, Vault was an ideal choice. For this firm's passwords and keys, Vault dynamically creates secrets, generating them automatically and on demand. Ensuring credential management meets security and compliance needs, Vault can set up dynamic secrets to expire within a given time period, greatly decreasing their value if leaked. Further, with this approach, passwords cannot be re-used; even within the lease period, they are a one-time use only.

- **Vault SSH Secret Backend:** The Vault SSH backend dynamically generates SSH credentials for remote hosts, thus increasing security by removing the need to share private keys with all users needing access to infrastructure.

- **Auditing:** Vault has an easy integration with Splunk, this company's log management system. By sending important log data to Splunk, Information Security has access to data such as which secrets were used by which operator, at what time and on which system(s).

### Business Needs

- Ensure HIPAA Compliance
- Effective secret management
- Maintain the highest levels of availability and reliability

### Benefits

- Met and exceeded RTO and RPO goals
- Secured previously insecure assets and processes
- Effective balance between security and agility

### Technical Details

- Services Used: HashiCorp Vault, HashiCorp Consul, AWS S3

- **Repeatability:** In order to meet this organization's RPO of five minutes or less, Flux7 recommended running its system with ECS and Docker containers, which can be quickly and easily recreated. For example, if a node were to crash, a replacement could be recreated within milliseconds.
- **Secure Introduction:** Using Docker also means that the Vault system is secure from the outset; there is no concern about introducing a vulnerability from a corrupted source. Moreover, Docker containers are immutable. Together, these concepts in action mean that secret management is created and housed in a secure fashion and can easily be recreated in the same way, if needed.

In addition to these benefits, Flux7 worked with the EHR provider's team to further strengthen its system and assure it meets its RPO goals by deploying and replicating its system cross-region and across AWS availability zones. In near real time, the system is copied cross-region and to both Virginia and Oregon AWS availability zones. As the system is copied in near real time, if a failure were to occur, the data lost would be much less than the five minute ceiling.

Flux7 also recommended establishing a backup system that exports the organization's encrypted data to Amazon's Simple Storage system, S3. The S3 backup solution provides secure, durable, highly-scalable cloud storage that serves as yet another data fail safe for this firm whose client data is the lifeblood of its organization.

## Benefits

The organization realized three key benefits from its new secret management system. First, it achieved an effective balance between security and agility, with individual teams now able to access the right credentials at the right time. And, the centralized Information Security team is able to maintain governance over credentials, receive important forensics data such as who accessed what credentials, and enforce their policies through automation. This balance resulted in less day-to-day management for both security and development, allowing them to dedicate more time to strategic initiatives.

In addition, the Vault system helped the firm increase its security with a better place to store their credentials. As the corporate secret store moving forward, the firm knows their passwords are safe. Last, this project helped this EHR provider secure systems and processes they were unable to previously secure. Because Vault allows dynamic backend for SSH, the firm was able to secure this process and related systems with dynamic key generation. Traditionally, SSH keys are challenging with users either having access to these keys, or having weak, insecure passwords. In either case, they were a vulnerability waiting to happen. Now, however, this organization has the benefit of disposable, one time passwords that all but eliminate this risk, ensuring the security of a previously insecure area of the business.

---

### LEARN MORE ABOUT OUR CLOUD INFRASTRUCTURE ASSESSMENT SERVICES

[www.flux7.com/cloud-infrastructure-assessment/](http://www.flux7.com/cloud-infrastructure-assessment/)

Austin-based Flux7 is a team of IT experts helping businesses realize and optimize the benefits of technology by using DevOps processes and full-stack expertise. Flux7's team delivers specialist development skills, architecture, and operations knowledge, accelerating an IT team's progress toward achieving business agility using best practices in continuous delivery and integration. Through a unique blend of services and products, Flux7 provides high-quality solutions that directly address the challenges faced by CIOs and IT teams to achieve short-term results with long-term benefits. With decades of combined industry experience, best-practices and industry benchmarks, our team is committed to creating sustainable, reliable solutions. For more information about Flux7, visit [flux7.com](http://flux7.com) or email [info@flux7.com](mailto:info@flux7.com).

Contact us today for a needs assessment: <http://bit.ly/1GHDZvf>

[www.flux7.com](http://www.flux7.com) | 844.358.9700 |   

