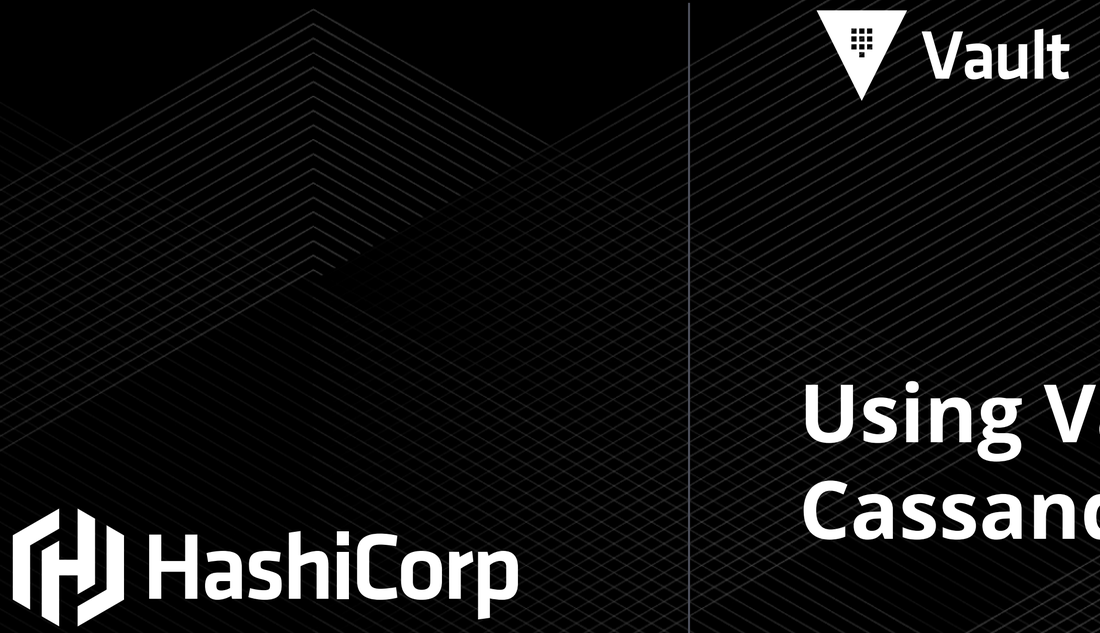


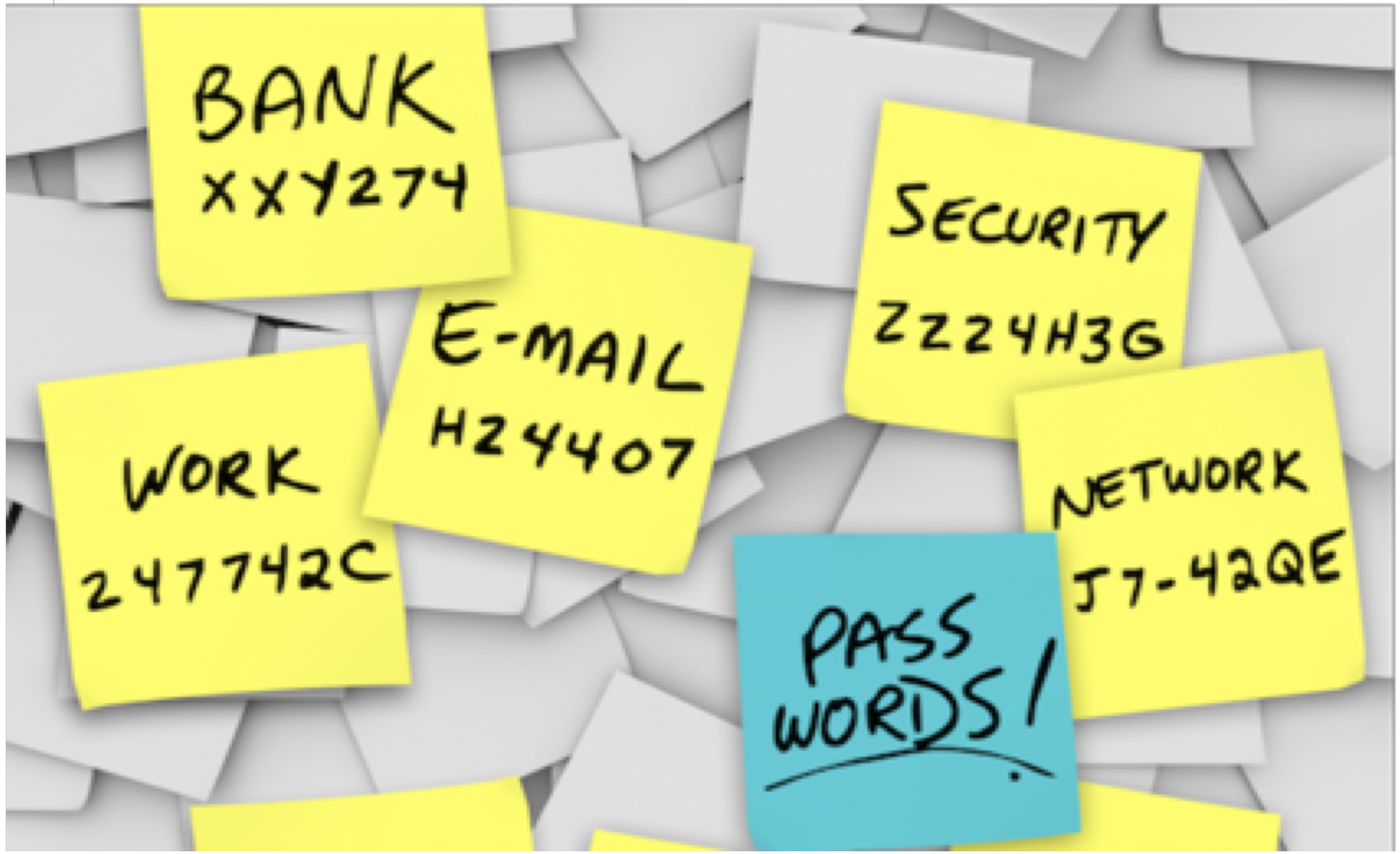
Using Vault Dynamic Secrets with Cassandra

John Dohoney, Jr

Sr. Solution Engineer
Americas – West (Los Angeles)

Hashicorp Vault is a secure store, with tight control access to tokens, passwords, certificates, encryption keys for protecting sensitive data, and other secrets in dynamic infrastructure.

Passwords are a problem...

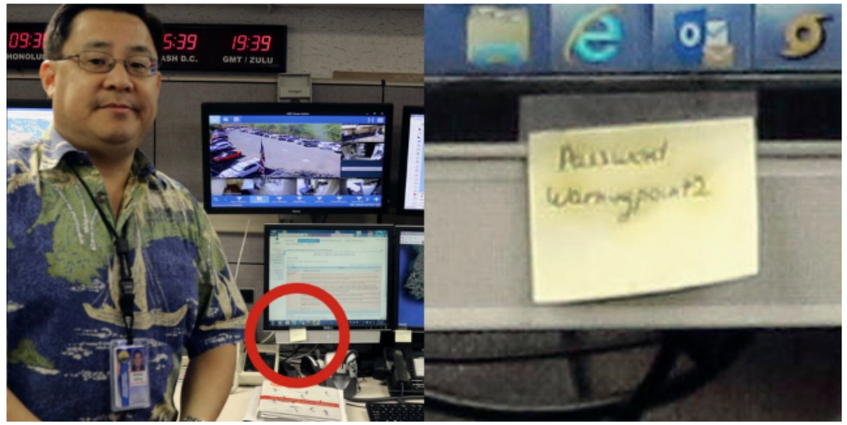


Then we add password policies, and increase the number of systems we need to access causes ...

It gets worse...

A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note

Kif Leswing Jan. 16, 2018, 3:07 PM



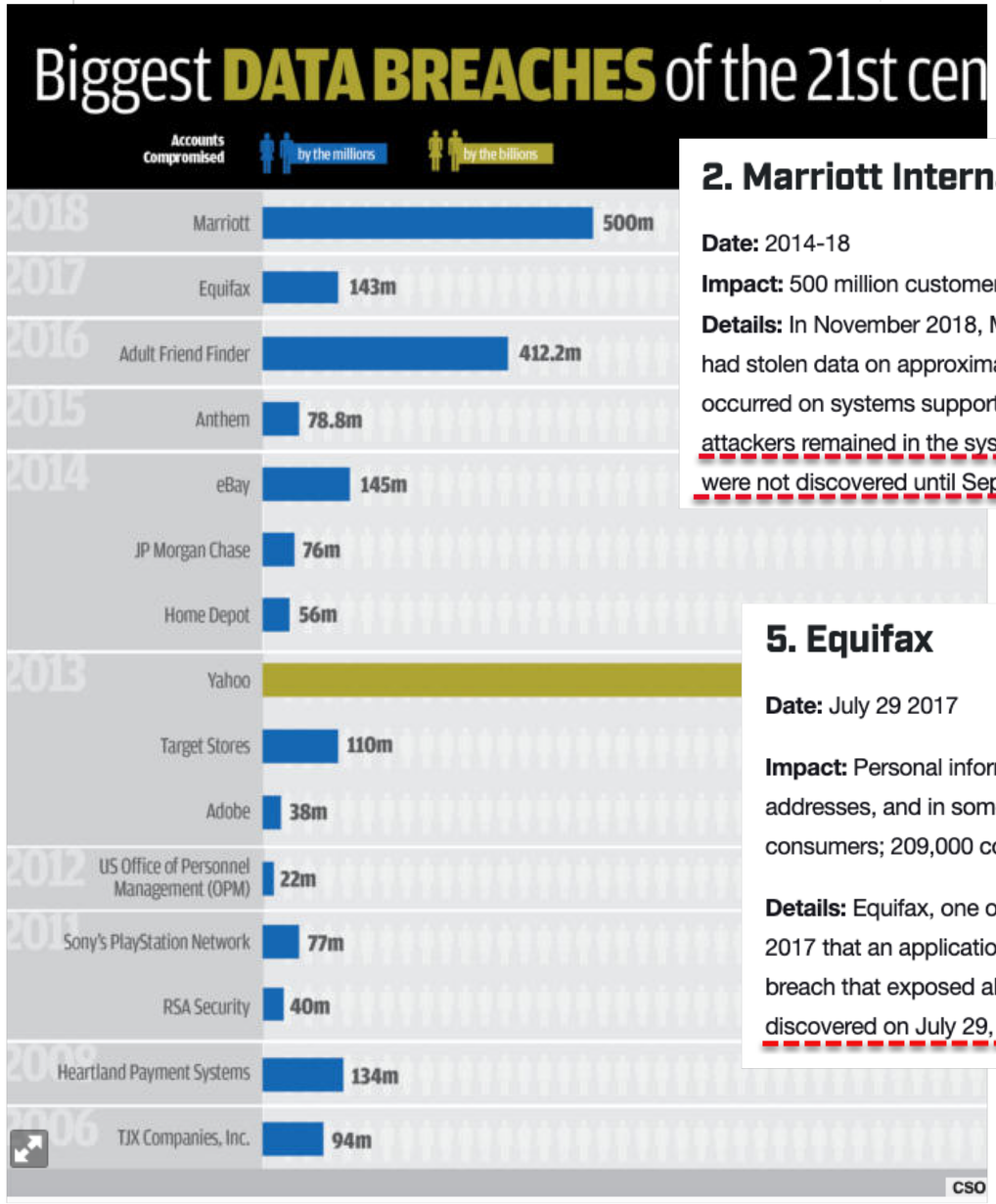
AP/Composite/Rob Price

- **A false alert warning of an inbound missile was broadcast in Hawaii on Saturday.**

Reference: https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1

Illegal Systems access happens …

Even the best companies are vulnerable



2. Marriott International

Date: 2014-18

Impact: 500 million customers

Details: In November 2018, Marriott International announced that cyber thieves had stolen data on approximately 500 million customers. The breach actually occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

5. Equifax

Date: July 29 2017

Impact: Personal information (including Social Security Numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed.

Details: Equifax, one of the largest credit bureaus in the U.S., said on Sept. 7, 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 147.9 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May.

Reference: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Feature: **Dynamic Secrets**

CHALLENGE SOLUTION RESULTS

Secrets everywhere – The Challenges

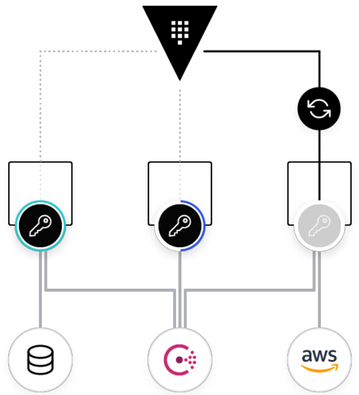
1.We don't actually know which access credentials are where in the enterprise?

2. Many systems are not designed for secrets management.

3. What do we do when there's a breach? Is it practiced?

4. Access authorization needs to be re-factored to meet the challenges of cyber-criminals.

The Problem: "Secrets Sprawl”



Secret Sprawl is defined as plaintext access to access credentials located in multiple places within your enterprise

The Solution

Vault centrally manages and enforces access to secrets and systems based on trusted sources of application and user identity.

AFTER

- **Increase productivity** & reduce time to deploy security workflows with centralized management
- **Control costs** with automated compliance and policy management, controls to support teams to self-manage their own environments
- **Reduce risk** with dynamic secrets, control groups, and other tools to allow Vault to conduct security operations while protecting sensitive information in flight and at rest.

Feature: **Dynamic Secrets**

CHALLENGE **SOLUTION** RESULTS

Benefits

- Bounded Credentials or Privilege Bracketing reduces Attack Surface, even if they should leak. The exposure is minimized to the “Lease Duration”
- Credentials are unique to a user/application, and easier to isolate due to unique credentials
- Easier revocation

```
$ vault read database/creds/readonly
Key                Value
---                -----
lease_id           database/creds/readonly/999c43f0-f79e-ba90-24a8-4de5af33a2e9
lease_duration     1h
lease_renewable    true
password           A1a-u7wxtrpx09xp40yq
username           v-root-readonly-x6q809467q98yp4yx4z4-1525378026e
```

Feature: **Dynamic Secrets**

CHALLENGE **SOLUTION** RESULTS

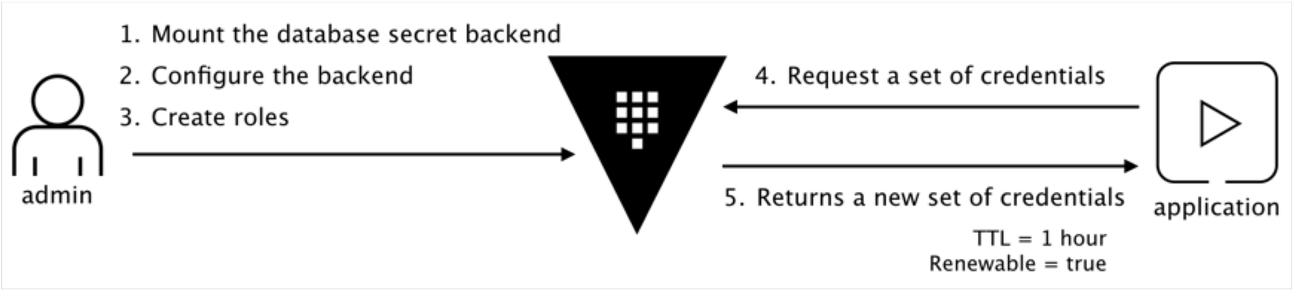
Dynamic Secrets

Vault grants tokens for access, not credentials, to ensure least privilege with security and ensure break glass functionality

- Set expiry to ensure that access is automatically revoked on time
- Revoke outstanding access at will
- Break glass functionality to halt all access in critical situations

ENTERPRISE

- Further control access to secrets with Sentinel policies



VAULT ADOPTION

Demonstration
Dynamic Secrets

Feature: **Dynamic Secrets - Big Ideas**

CHALLENGE

SOLUTION

RESULTS

How do Dynamic Secrets Help

Privilege Separation - Separation of privilege refers to the compartmentalization of privileges across various application or system sub-components, tasks, and processes.

Vault Implementation -- Create a specific policy based on role that in this case, compartmentalizes database access

Privilege Bracketing - Elevate privileges on an as-needed basis for specific applications and tasks only for the moment of time they are needed, without requiring administrative credentials or exposing passwords.

Vault Implementation -- Dynamic Secrets that utilize a Time-based "Lease" for access

Non-repudiation - You are who you say you are and it can be audited

Vault Implementation -- Vault provides meta-data and audit logging for traceability

Feature: **Dynamic Secrets**

CHALLENGE SOLUTION RESULTS

Cassandra Customizations

1. In the **<Cassandra root>/conf**, two parameters require changing (if not already)

```
# - AllowAllAuthenticator performs no checks - set it to disable authentication.
# - PasswordAuthenticator relies on username/password pairs to authenticate
#   users. It keeps usernames and hashed passwords in system_auth.credentials table.
#   Please increase system_auth keyspace replication factor if you use this authenticator.
#   If using PasswordAuthenticator, CassandraRoleManager must also be used (see below)
## authenticator: AllowAllAuthenticator
authenticator: PasswordAuthenticator
# - AllowAllAuthorizer allows any action to any user - set it to disable authorization.
# - CassandraAuthorizer stores permissions in system_auth.permissions table. Please
#   increase system_auth keyspace replication factor if you use this authorizer.
## authorizer: AllowAllAuthorizer
authorizer: org.apache.cassandra.auth.CassandraAuthorizer
```

2. Java 8 is the preferred version, I was able to make this work with Java 10, and 11
3. Cassandra complained there was no log directory, so one was created at **<Cassandra root>/logs**

Feature: **Dynamic Secrets**

CHALLENGE

SOLUTION

RESULTS

Vault Database Secret Engines and Plugin System

1. Vault database secrets Engines documents - https://www.vaultproject.io/docs/secrets/databases/index.html
2. Vault Database Plugins - https://www.vaultproject.io/docs/internals/plugins.html
3. Vault Database Plugin Github Repo - https://github.com/hashicorp/vault/tree/master/plugins/database

Thank you

hello@hashicorp.com

www.hashicorp.com