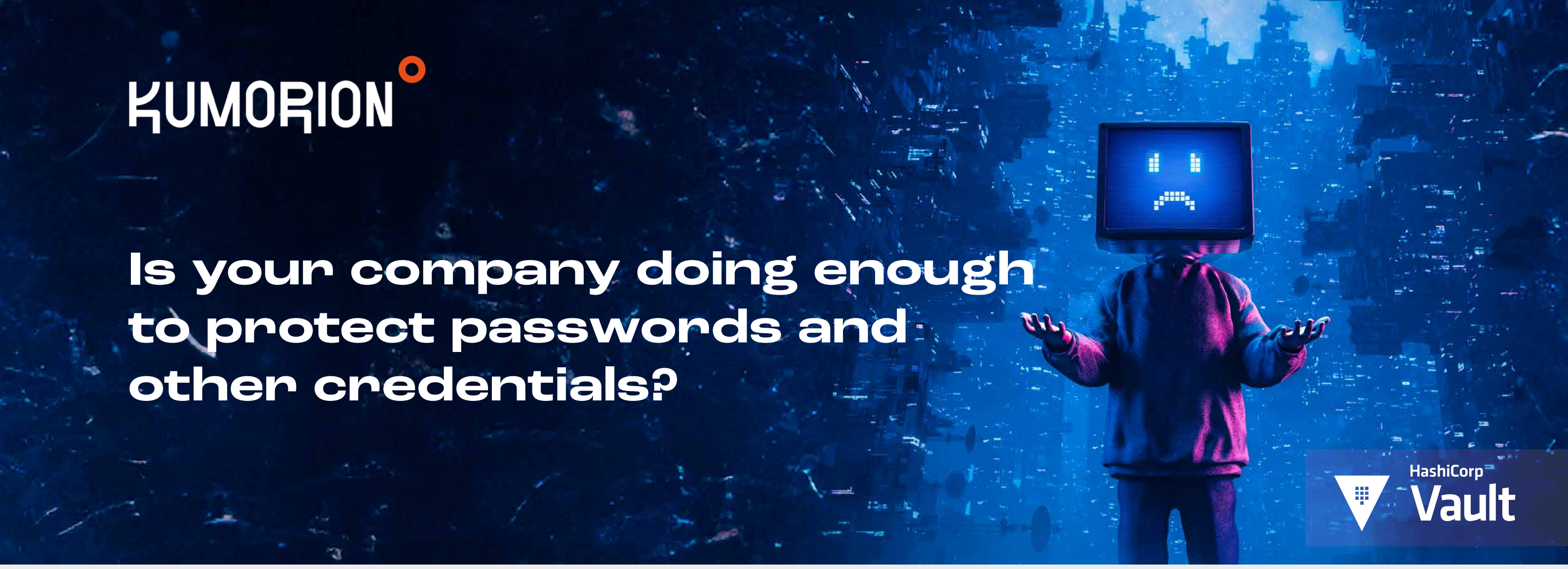

Is your company doing enough to protect passwords and other credentials?

Every login credential is a potential risk to your company’s security. We explain why HashiCorp Vault is the right way to keep your secrets safe.

Passwords and other credentials are the keys to our digital kingdoms. Behind the doors they unlock lie infinite treasures of data on the things that people and companies hold valuable.

Yet these ‘secrets’ – as we call them in the IT world – are often scattered and poorly guarded. From an admin password scribbled on a sticky note to an API key left exposed in some code, lack of control over secrets has led to some staggering breaches.

According to **Verizon’s 2024 Data Breach Investigation Report**, some 77% of web application attacks stem from hacking with the use of stolen credentials. When a single overlooked secret falls into the wrong hands, you may be giving away the keys to your entire kingdom.

“As a company grows, you have a lot more applications and associated secrets. The connections between apps create many access points in the environment, which in turn create more attack vectors that can be exploited. The more complex your infrastructure is, the more important it is to keep your secrets under virtual lock and key,” says Kumorion Founder and Chief Technology Officer, Timo Ahokas.

Kumorion is an advocate for implementing the **Vault secret-management solution** from US cloud-infrastructure leader HashiCorp. The solution is designed for storing passwords, certificates, encryption keys and more, with special tools that give you complete control over these critical secrets.

While Vault is suitable for any environment, it’s widely used when security is paramount. This includes DevOps workflows, cloud-infrastructure projects and industries that handle sensitive information.

Tools to rotate, revoke and audit secrets

A common way in which secrets are compromised is through failure to rotate credentials (i.e. the periodic changing of passwords, keys or other authentication information). One of the reasons that passwords and keys may not be rotated is because it’s often challenging to track down all the places they’re used. This challenge can be overcome by making HashiCorp Vault a single source of truth for maintaining and managing secrets.

P2

“Changing some but not all credentials can risk breaking critical systems, which is why passwords are sometimes left unchanged. HashiCorp Vault solves this issue with tools to rotate credentials and automatically synchronize them across all systems,” explains Kumorion Cloud Architect, **Shankar Lal**.

Failure to revoke credentials is another way in which companies are exposed to breaches. For example, an employee may leave a company yet still be able to access a specific domain. Or an external developer may have a temporary username and password to work on some code, while the person who granted the credentials may not keep track of having done so.

None of this necessarily implies malice from any party involved. But the more secrets that are in circulation, the greater the risk of exposure. We are all vulnerable to phishing attacks.

“Once you create a secret for accessing a system, it often lingers longer than is necessary. This leads to security risks if it’s not revoked. HashiCorp has addressed this with a feature for creating dynamic secrets. These are credentials that exist for only a short, predefined period – even just 10 minutes,” says Lal.

“This dynamic secrets feature is not only useful for granting access to externals, but also for controlling role-based internal access. For example, an analyst may need read-only access to see a database just long enough to pull certain numbers for a report,” he explains.

HashiCorp Vault also provides robust auditing features, allowing administrators to track who has accessed a system and with which credentials. Audit logs show unauthorized attempts to retrieve sensitive information and can be used to trigger alerts when unexpected logins take place.

Kumorion manages HashiCorp Vault for your company

While it’s possible for companies to take HashiCorp Vault into use on their own, effective management of the solution requires deep technical knowledge and careful configuration. This is where Kumorion brings significant expertise, simplifying the implementation through a managed services approach that covers all aspects of deploying and maintaining Vault.

“Kumorion has more than five years of experience running Vault for the Nokia corporate private cloud, which is one of the largest in the world. We have delivered Vault-as-a-Service to hundreds of teams and users, and also used Vault internally in multiple large scale services we have built. Now we’re bringing this knowledge and experience to other customers too,” explains Ahokas.

Kumorion hosts Vault in the customer's cloud or on-premise servers. Managed services include automated backups, high availability configurations, and clustering to prevent any single point of failure. In case of issues with the Vault application, Kumorion's managed service is able to perform automated health checks and trigger the recovery process.

For companies wanting to take the next step in this domain, Kumorion recommends evaluating the status of your secret protection framework through the following best-practice model:

- Level 1 – Unmanaged Secrets: Secrets exist but are not stored in a secure vault. There is a high risk of exposure
- Level 2 – Vaulted Secrets: Static secrets are stored in a vault. Without regular updates, these secrets remain vulnerable to exposure – even many years later
- Level 3 – Rotated Secrets: Automatic rotation changes secrets at monthly, weekly or even hourly intervals
- Level 4 – Dynamic Access: Secrets are created dynamically when needed, even for a very short duration. Integration with Kubernetes, databases and public clouds – including AWS and Azure –allows for seamless management of these short-lived credentials

"HashiCorp Vault enables levels 2, 3 and 4 – depending on the approach you choose. This flexibility means it fulfills the needs of many businesses. You can start small and build up to level 4. Kumorion can evaluate your security setup and suggest the right approach," says Ahokas.

"Every company is of course the master of its own secrets, but we recommend being at least on level 2 in this day and age."

CONTACT US TODAY TO LEARN MORE ABOUT HOW WE CAN HELP YOUR BUSINESS.

INFO@KUMORION.COM +358 400 428 515

KUMORION