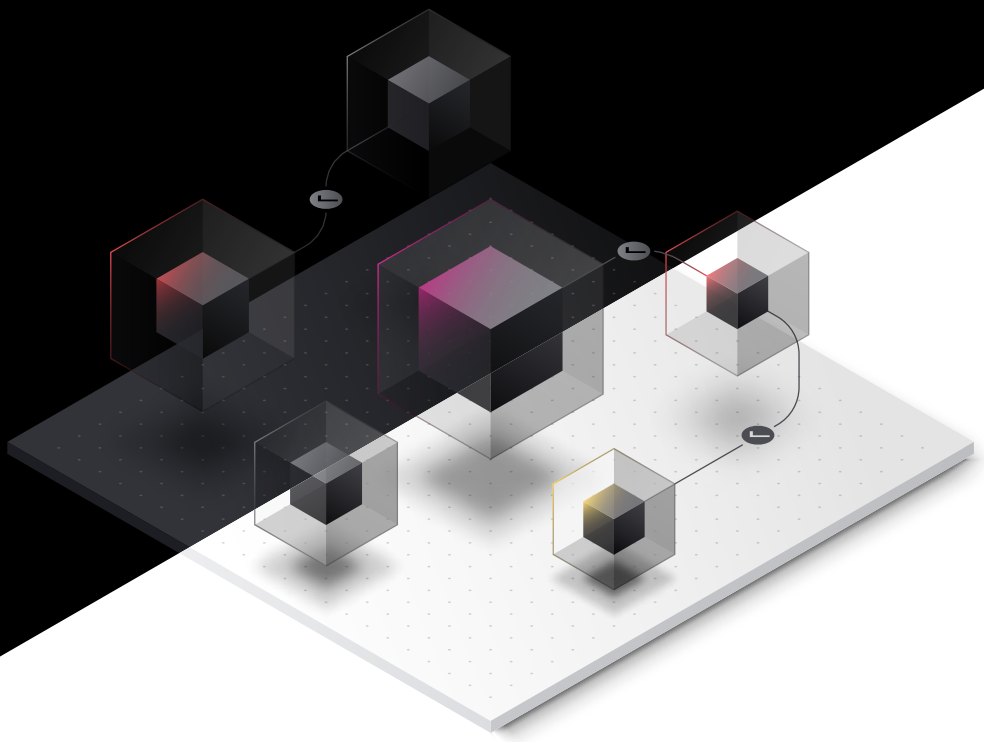
HashiCorp

Ne jamais faire confiance. Toujours tout authentifier et autoriser.



aws PARTNER

Ne jamais faire confiance.

Toujours tout authentifier et autoriser.

La transition depuis des environnements et centres de données sur site traditionnels vers une infrastructure cloud dynamique s'avère complexe et présente de nouveaux défis en matière de sécurité pour les entreprises. Il existe un plus grand nombre de systèmes à gérer, plus de points de terminaison à surveiller, plus de réseaux à connecter, et plus d'utilisateurs ayant besoin d'un accès. Le risque potentiel de violation de données s'accroît considérablement, et ce n'est qu'une question de temps avant qu'une telle violation ne se produise en l'absence d'un positionnement approprié quant à la sécurité.

La sécurisation des centres de données traditionnels nécessitait de gérer et de sécuriser un périmètre IP comprenant des réseaux et des pare-feux, des HSM, des SIEM ainsi que d'autres restrictions de l'accès physique. Cependant ces solutions ne sont plus suffisantes à mesure que les entreprises migrent vers le cloud.

La sécurisation de l'infrastructure dans le cloud exige une approche différente.

Au fur et à mesure que les entreprises migrent vers le cloud, les mesures qu'elles ont prises pour sécuriser leurs centres de données privés commencent à disparaître. Les périmètres et les accès basés sur IP sont remplacés par des adresses IP éphémères, et à cela s'ajoute le besoin pour un personnel en constante évolution d'accéder à des ressources partagées. La gestion des accès et des adresses IP à grande échelle devient aléatoire et complexe. La sécurisation de l'infrastructure, des données et de l'accès devient de plus en plus difficile dans les clouds et les centres de données sur site, ce qui résulte en des frais généraux élevés et requiert un haut niveau d'expertise. Ce changement demande une approche différente de la sécurité : un modèle de confiance différent. Un modèle basé sur le « zéro confiance » et dans lequel tout est toujours authentifié et autorisé.

En raison de l'environnement hautement dynamique, les organisations parlent d'approche « Zero Trust » de la sécurité cloud. Qu'est-ce que la sécurité « Zero Trust » implique réellement et qu'est-ce qui est nécessaire pour la réussite de sa mise en œuvre ?

Défis

en matière de sécurité Zero Trust multi-cloud

Gestion de l'accès par IP

Les solutions traditionnelles de protection des infrastructures, des données et de l'accès reposent sur la nécessité de sécuriser en fonction des adresses IP. Applications communiquant avec des bases de données, utilisateurs accédant aux hôtes et aux services et serveurs communiquant à travers les clouds : tous sont traditionnellement protégés en autorisant ou en restreignant l'accès en fonction des adresses IP. La gestion de l'accès à cette même infrastructure et aux mêmes données à mesure que les entreprises migrent vers le cloud s'avère beaucoup plus difficile et complexe sur le plan opérationnel, car les adresses IP sont plus dynamiques et changent fréquemment.

Sécurisation de la connectivité machine

L'accès machine-machine constitue un élément central d'une organisation axée sur le cloud. Les méthodes ITIL antérieures nécessitant des systèmes de tickets conventionnels sont lentes, lourdes et pas assez flexibles pour répondre aux exigences de sécurité rigoureuses des environnements cloud dynamiques actuels.

Évolutivité en fonction de la demande

La gestion traditionnelle des accès et des identités impliquant des processus manuels est lente, inefficace et insuffisante. Des mesures de sécurité telles que jetons, cartes-clés et mots de passe requièrent une intervention informatique directe qui nécessite autant des ressources importantes que du temps, en particulier lorsque cela est nécessaire pour des centaines ou des milliers d'utilisateurs individuels et de machines.

Permettre

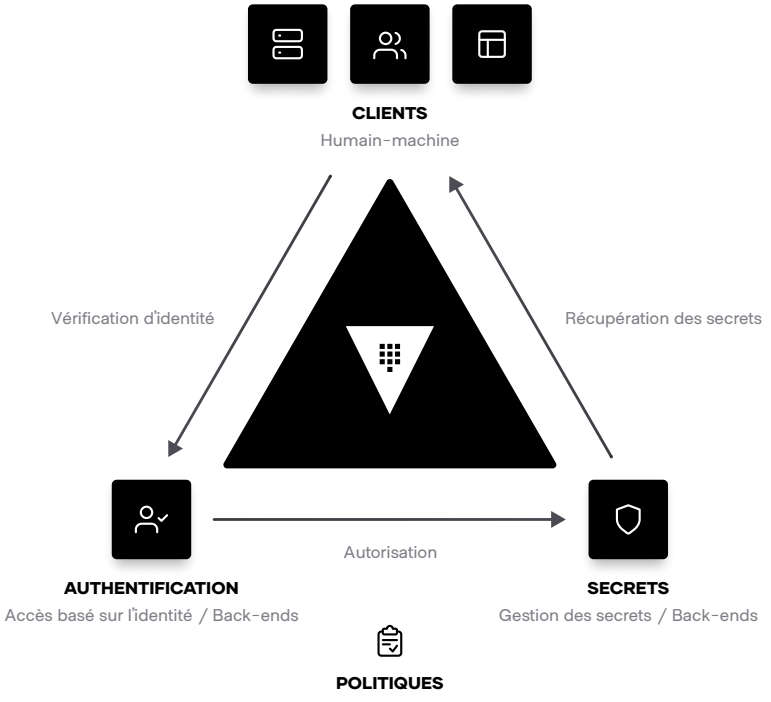
une sécurité évolutive et dynamique à travers les clouds

Il existe quatre piliers en matière de sécurité multi-cloud dans un monde Zero Trust : l'authentification et l'autorisation des machines, l'accès machine-machine, l'authentification et l'autorisation pour les utilisateurs humains et l'accès humain-machine.

Le dénominateur commun de ces quatre piliers est l'exigence constante de contrôles basés sur l'identité. Chez HashiCorp, notre modèle de sécurité repose sur le principe d'un accès et d'une sécurité basés sur l'identité. Pour que des machines ou utilisateurs soient en mesure de faire quoi que ce soit, ils doivent authentifier qui ils sont ou ce qu'ils sont, et leur identité ainsi que les politiques qui leur sont applicables définissent ce qu'ils sont autorisés à faire. Voici comment les offres HashiCorp peuvent vous aider avec chaque pilier et faire en sorte que la sécurité Zero Trust soit vraiment efficace :

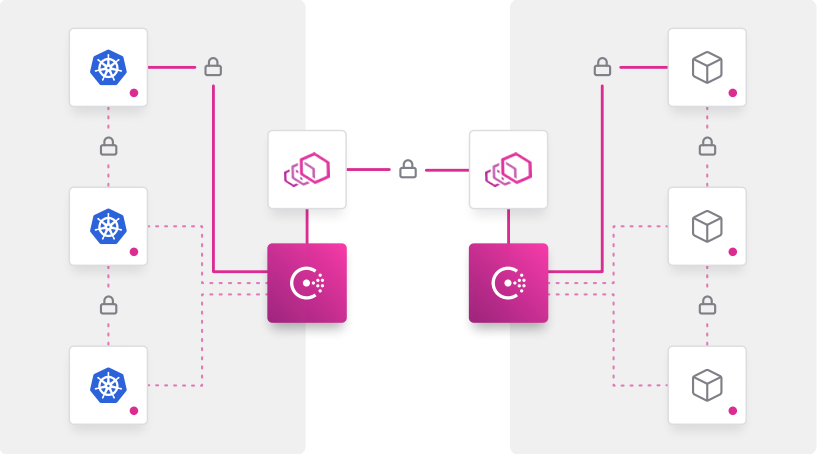
Authentification et autorisation concernant les machines

HashiCorp Vault permet aux professionnels et aux entreprises de sécuriser, de stocker, d'accéder et de distribuer de manière centralisée des secrets dynamiques tels que des jetons, des mots de passe, des certificats et des clés de chiffrement dans n'importe quel environnement de cloud public ou privé. Vault fournit un flux de travail automatisé pour les personnes et les machines afin de gérer de manière centralisée l'accès aux informations d'identification et de chiffrer les données sensibles via une API unique. Avec HCP Vault, bénéficiez de toute la puissance et de la sécurité dont vous avez besoin, et cela sans complexité ni problème de surcharge concernant son exécution.



Accès machine-machine

HashiCorp Consul permet l'accès machine-machine en imposant l'authentification entre les applications et en s'assurant que seules les machines appropriées communiquent entre elles. Consul codifie les règles d'autorisation et relatives au trafic avec un trafic chiffré tout en automatisant l'accès basé sur l'identité pour une portée, une efficacité et une sécurité maximales. Avec Consul, les organisations peuvent découvrir des services, automatiser les configurations réseau et activer une connectivité sécurisée sur n'importe quel cloud ou environnement d'exécution à l'aide du service mesh fourni par Consul.

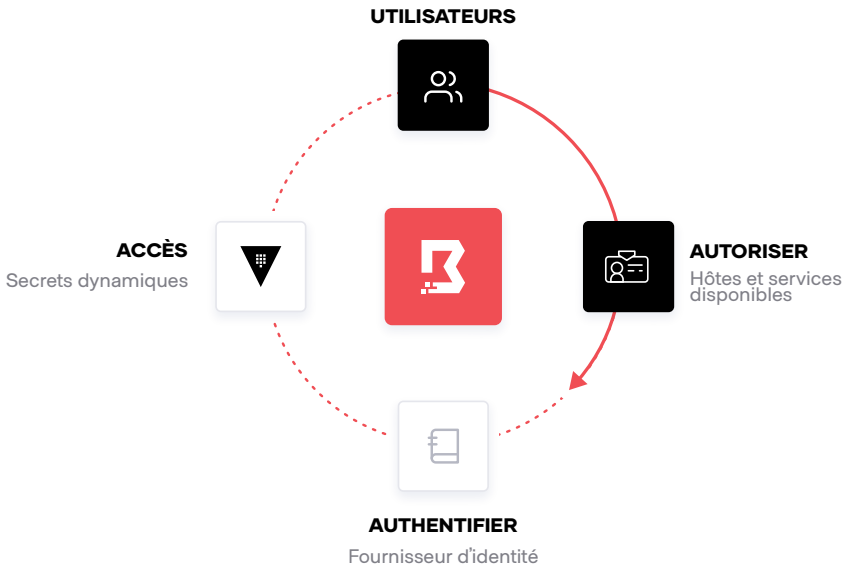


Accès et autorisation pour les utilisateurs humains

Les entreprises utilisent différentes plateformes d'identité pour les systèmes d'enregistrement fédérés. Tirer parti de ces fournisseurs d'identité de confiance constitue le principe de base en matière d'accès et de sécurité basés sur l'identité. Les produits HashiCorp permettent une intégration profonde avec les principaux fournisseurs d'identité.

Accès humain-machine

Les solutions traditionnelles de protection de l'accès des utilisateurs nécessitent la distribution et la gestion des clés SSH, des informations d'identification VPN ainsi que des bastions, ce qui implique des risques de diffusion des informations d'identification et d'accès d'utilisateurs à des réseaux et des systèmes entiers. HashiCorp Boundary fournit un accès à distance simple et sécurisé afin d'accéder en toute sécurité aux hôtes et services dynamiques sans besoin de gérer les informations d'identification et les adresses IP ou d'exposer votre réseau.



Impact
de la sécurité
multi-cloud
sur les entreprises

L'approche de HashiCorp en matière de sécurité et d'accès basés sur l'identité fournit une base solide aux entreprises leur permettant ainsi de migrer et sécuriser en toute sécurité leur infrastructure, leurs applications ainsi leurs données à mesure qu'elles s'engagent dans un monde multi-cloud.

Adoption plus rapide du cloud

Accélérez l'adoption du cloud avec des déploiements clé en main ainsi que les bonnes pratiques appliquées en standard.

Productivité accrue

Augmentez la productivité et réduisez les coûts grâce à une infrastructure entièrement gérée.

Flexibilité multi-cloud

Permettez une flexibilité multi-cloud grâce à un workflow unique pour l'ensemble des providers.


HashiCorp