Red Hat

Créer une base sécurisée avec l'automatisation et le modèle Zero Trust

Comment mettre en pratique le modèle Zero Trust

Red Hat

Sommaire

Introduction

L'activité de votre entreprise ne s'arrête pas après 17h, ni celle des cybercriminels et autres acteurs malveillants. Ces derniers cherchent en permanence des occasions de dérober des données ou de causer des dégâts qui pourraient nuire à votre entreprise, à vos partenaires et à vos clients.

Aujourd'hui, les organisations sont submergées par les menaces. Les équipes informatiques, de sécurité et d'exploitation restent constamment en alerte. Ces menaces touchent les organisations de toutes tailles et engendrent des pertes de plusieurs milliards de dollars. Selon un rapport d'IBM, le coût moyen d'une fuite de données causée par une cyberattaque augmente. Il s'élevait à 4,24 millions de dollars en 2021, contre 3,86 millions de dollars en 2020[1].

Ces attaques ne proviennent d'ailleurs pas uniquement de l'extérieur. Dans son rapport « Data Breach Investigations Report » de 2021, Verizon avait montré que 30 % des failles impliquaient des membres du personnel qui accédaient à des systèmes sans autorisation[2].

L'augmentation de la quantité et de la sévérité des attaques est alimentée par différents facteurs, notamment l'évolution rapide de l'infrastructure réseau, les migrations vers le cloud et l'essor des modèles de travail à distance depuis 2020.

Avec l'évolution des lieux de travail, les utilisateurs accèdent aux systèmes sensibles aussi bien avec des équipements appartenant à l'entreprise qu'avec leurs propres appareils, souvent via des réseaux domestiques, voire publics. Résultat : la surface d'attaque s'est étendue. En outre, puisque les membres du personnel travaillent avec des collègues qu'ils ne connaissent que virtuellement, on observe une augmentation et une complexification des attaques par hameçonnage, qu'elles soient ciblées ou non.

La migration vers des solutions basées dans le cloud a apporté de nombreux avantages aux entreprises, allant d'une réduction des coûts à une forte diminution du stockage des documents physiques. Ces avantages s'accompagnent cependant du coût inévitable de la gestion de la sécurité de l'infrastructure, des applications et des utilisateurs qui se comptent par milliers dans les systèmes sur site et dans le cloud.

Avec le travail à distance et la migration vers le cloud, l'approche de sécurité basée sur les écosystèmes fermés et les réseaux privés virtuels est devenue complètement obsolète. Outre le fait que le personnel utilise davantage d'appareils pour se connecter à un plus grand nombre de systèmes, de nouveaux potentiels vecteurs d'attaques sont apparus avec l'essor de l'IoT (Internet des objets) et de l'edge computing.

En plus d'adapter les moyens d'accès aux systèmes qu'utilise le personnel, les organisations ont aussi fait évoluer leurs équipes afin qu'elles puissent gérer des réseaux et des systèmes de sécurité disparates. Les équipes InfoSec, SysOps, NetOps et d'autres services travaillent souvent simultanément et indépendamment les unes des autres pour appliquer les politiques de sécurité et traiter les menaces. Ces équipes travaillent tout de même séparément et utilisent des systèmes et des processus différents, ce qui les empêche de répondre de manière coordonnée aux incidents. Et en matière de menaces de sécurité, chaque seconde compte.

1 « Cost of a data breach report 2021 », IBM, consulté le 16 juin 2022
2 « 2022 Data Breach Investigations Report », Verizon, consulté le 16 juin 2022

Vous voulez en savoir plus sur le modèle Zero Trust ? Lisez la suite.

Vous connaissez déjà le modèle Zero Trust et souhaitez savoir comment l'automatiser ? Passez directement à la section **Mettre à l'échelle l'architecture Zero Trust avec l'automatisation**.

Il existe d'autres risques de cyberattaques, liés au manque de compatibilité entre les solutions qui font fonctionner et protègent l'infrastructure de l'entreprise. Si les équipes qui gèrent ces solutions ne communiquent pas efficacement entre elles, des goulets d'étranglement supplémentaires apparaissent et empêchent le traitement efficace des incidents de sécurité.

Les responsables de la sécurité ne sont plus les seuls à s'intéresser à ces risques de cyberattaques. Les organisations, entreprises et fournisseurs se sont adaptés pour se conformer aux réglementations, notamment la loi californienne sur la protection de la vie privée des consommateurs (California Consumer Privacy Act, CCPA) et le Règlement général sur la protection des données (RGPD) de l'Union européenne. En 2021, le gouvernement des États-Unis a reconnu l'augmentation des menaces et a fait paraître un décret sur le renforcement de la cybersécurité des agences gouvernementales.

Pour traiter ces menaces, les organisations doivent adopter une approche axée sur la sécurité concernant les politiques, les réseaux et les applications. De nombreuses organisations considèrent l'architecture Zero Trust comme la solution, à l'instar du gouvernement fédéral des États-Unis qui s'est donné pour mission de mettre en œuvre le modèle Zero Trust dans l'ensemble de ses réseaux.

La mise en œuvre d'une architecture Zero Trust n'est cependant que la première étape des stratégies de sécurisation, surtout dans les grandes organisations qui opèrent dans plusieurs endroits et qui disposent de systèmes sur site, dans le cloud ou en périphérie du réseau. La mise à l'échelle d'une architecture Zero Trust nécessite d'automatiser les processus dans toute l'entreprise. Dans ce livre numérique, vous découvrirez pourquoi Red Hat® Ansible® Automation Platform est la solution idéale pour votre entreprise.

Le Zero Trust, la solution ?

Les modèles de sécurité traditionnels ont été créés autour de systèmes auxquels les membres du personnel accédaient depuis un lieu physique. Avec l'évolution des moyens d'accès à distance, des modems aux connexions à haut débit disponibles en continu, les accès externes ont été régulés par l'utilisation de réseaux privés virtuels (VPN). Même si ces VPN sécurisent l'authentification aux réseaux, ils laissent la possibilité aux utilisateurs d'accéder à un plus grand nombre de ressources et de systèmes que nécessaire, ce qui engendre de potentiels risques pour la sécurité.

Aujourd'hui, les VPN et les autorisations standard basées sur les utilisateurs n'offrent cependant plus le niveau de sécurité requis pour les architectures de solutions basées dans le cloud, sur site ou hybrides, dont dépendent les activités des entreprises. Cette situation nécessitait la création d'un nouveau modèle, capable de faire évoluer les bases de notre approche en matière de sécurité. Ce nouveau modèle repose sur l'architecture Zero Trust.

Reconnu en 2010 comme configuration de sécurité, le modèle Zero Trust part du principe que les attaques peuvent provenir à la fois de l'intérieur et de l'extérieur du réseau. Sur cette base, le modèle Zero Trust considère par défaut qu'aucune interaction n'est fiable au départ.

Au lieu de s'appuyer uniquement sur les autorisations basées sur les utilisateurs ou les rôles, le modèle Zero Trust exige la vérification de l'utilisateur, de l'appareil et de l'application pour que l'état de l'interaction soit considéré comme fiable. La mise en œuvre d'une architecture Zero Trust favorise une approche complètement nouvelle de la sécurité, qui exige des architectes système qu'ils authentifient les utilisateurs ou les appareils pour chaque transaction, et qui autorise uniquement l'accès aux données et aux systèmes sur la base du principe de moindre privilège.

Authentifier chaque transaction

L'architecture Zero Trust repose sur le principe que chaque interaction est une menace potentielle, provenant de l'intérieur ou de l'extérieur du réseau. Afin que l'interaction puisse se dérouler, les composants doivent être authentifiés. Chaque architecture Zero Trust dispose de ses propres composants requis, avec les éléments de base suivants :

- **L'utilisateur :** il faut vérifier que l'utilisateur qui tente d'accéder à un réseau, une l'application ou un système basé dans le cloud possède les autorisations requises.
- **L'application :** il faut vérifier que l'utilisateur possède les autorisations requises pour accéder aux données ou à l'application.
- **L'appareil :** il faut confirmer que l'utilisateur interagit avec la ressource depuis un appareil autorisé à accéder au réseau et à l'application.
- **La posture :** il faut vérifier que l'appareil autorisé dispose des mises à jour, des correctifs et des capacités de chiffrement nécessaires pour accéder de manière sécurisée au réseau et à l'application.

La transition vers le modèle Zero Trust s'effectue aussi dans le secteur public, notamment au sein du gouvernement fédéral des États-Unis. Le décret paru en 2021 sur le renforcement de la cybersécurité des agences gouvernementales comprend de multiples missions, de la migration vers des solutions sécurisées basées dans le cloud à l'adoption d'architectures Zero Trust dans l'ensemble de l'infrastructure du gouvernement.

Face à cette mise à niveau des processus de sécurité et des infrastructures informatiques, les entreprises qui vendent des solutions ou des services aux agences gouvernementales doivent s'assurer de respecter les normes du modèle Zero Trust.

Défis relatifs à la mise en œuvre du modèle Zero Trust

Avec l'augmentation des menaces et des vecteurs d'attaque, il devient impératif de mettre en œuvre une architecture Zero Trust au sein des organisations. Si le modèle Zero Trust offre de nombreux avantages par rapport à une approche de sécurité traditionnelle, sa mise en œuvre dans l'infrastructure peut poser des problèmes.

D'abord, l'infrastructure existante peut être constituée de diverses solutions provenant de multiples fournisseurs. Bien que la majorité des fournisseurs se soient efforcés d'adopter les principes de l'architecture Zero Trust, tous les systèmes ne sont pas forcément compatibles avec ceux des autres fournisseurs. Les équipes internes (SysOps, NetOps) peuvent rencontrer des problèmes lorsque les solutions ne fonctionnent pas correctement ensemble. Pire, les équipes et systèmes déconnectés peuvent causer une interruption de la détection des menaces en cas de problèmes d'interopérabilité.

Ensuite, le modèle Zero Trust nécessite de modifier en profondeur la manière dont les dirigeants envisagent et abordent la sécurité. Pour passer d'un « château fort » à une approche de « rejet par défaut », les dirigeants doivent engager leurs organisations à respecter et suivre les principes et pratiques du modèle Zero Trust, même lorsque ces derniers semblent compliquer la tâche. Sans cet engagement, les équipes peuvent souvent réinstaurer d'anciennes pratiques, voire même favoriser le phénomène de shadow IT qui échappe à l'architecture, aux politiques et aux processus du modèle Zero Trust.

Comment poser des bases solides pour la sécurité avec une architecture Zero Trust

Les approches de sécurité traditionnelles, comme les VPN avec des jetons physiques ou numériques, ont été élaborées pour fournir un accès distant sécurisé au réseau local. Souvent comparée au modèle de protection des châteaux forts, cette approche reposait uniquement sur un point d'entrée qui ouvrait l'accès à toutes les ressources situées de l'autre côté.

Dans le domaine de la sécurité physique, on pourrait comparer ce modèle à une carte d'accès aux bâtiments et à toutes les zones sécurisées qui se trouvent à l'intérieur. Une organisation pourrait avoir le sentiment que sa sécurité physique est garantie avec l'utilisation de processus de sécurité basés sur les rôles pour le personnel qui entre dans les locaux ou pénètre dans différentes zones. Ces mesures de sécurité physique peuvent cependant échouer si un acteur malveillant utilise une technique d'ingénierie sociale, comme se faire passer pour un livreur, pour obtenir une autorisation d'accès auprès du personnel de sécurité.

Le Zero Trust par défaut

Selon les principes du modèle Zero Trust, la sécurité est placée au cœur de tous les projets, que ce soit pour le développement de nouveaux produits ou la mise en œuvre d'une nouvelle infrastructure. Au lieu de créer des processus de sécurité autour de l'accès au réseau, l'architecture Zero Trust s'applique à chaque interaction dans l'entreprise.

Bien démarrer avec le modèle Zero Trust

La mise en œuvre d'une architecture Zero Trust ne commence pas par la sélection de fournisseurs ou par la migration des plateformes de sécurité. À la place, les entreprises doivent se poser une question simple qui aura des implications considérables pour leurs stratégies Zero Trust : quelles données, quelles applications ou quels systèmes faut-il protéger ?

- **Création d'un inventaire :** les entreprises doivent bien identifier les éléments à protéger afin d'établir une base de référence qui servira à créer les règles et politiques à appliquer au réseau, aux utilisateurs, applications et charges de travail lors de la mise en œuvre de leur architecture Zero Trust. Cette base permet également aux équipes SysOps, NetOps et InfoSec de définir les analyses et outils d'analyse dont elles ont besoin pour détecter, identifier et traiter les incidents de sécurité.
- **Développement des processus et politiques :** une fois que les entreprises ont clairement identifié les éléments à protéger, les équipes internes peuvent collaborer pour créer des processus et politiques Zero Trust qui permettent au personnel de travailler de manière sécurisée.
- **Tests, modifications, déploiement :** parfois, les idées ne donnent pas le résultat attendu lors de leur mise en œuvre. En analysant les processus et les politiques en situation réelle, les équipes d'exploitation, de réseau et de sécurité peuvent ajuster l'architecture Zero Trust afin que cette dernière fonctionne dans toute l'entreprise.

Pour mettre à l'échelle une architecture Zero Trust par le biais de l'automatisation, il faut commencer par connaître les éléments à protéger.

Mettre à l'échelle l'architecture Zero Trust avec l'automatisation

Apprenez-en davantage sur l'automatisation de la sécurité avec Ansible, et découvrez où vous en êtes dans le parcours d'automatisation de la sécurité dans ce webinar.

Dans les architectures Zero Trust, toutes les ressources, notamment les appareils, les données et les applications, doivent être protégées de la même manière, où qu'elles se trouvent. Par exemple, si une charge de travail est déplacée d'un datacenter sur site vers un cloud public ou privé, l'architecture Zero Trust exige que les mêmes règles de gestion de la sécurité soient appliquées. Dans une architecture Zero Trust, les décisions sont séparées de la charge de travail en elle-même, de sorte que le code déployé ne change pas.

Dans les organisations de grande taille ou les entreprises au développement rapide, l'automatisation permet de mettre à l'échelle les politiques, règles et processus lorsque de nouveaux outils sont adoptés ou qu'une nouvelle infrastructure est mise en place. Avant de nous intéresser à la manière dont la solution Red Hat® Ansible® Automation Platform permet d'automatiser l'architecture Zero Trust, voyons cinq avantages de l'automatisation de ce modèle :

Les avantages de l'automatisation

- **Connaissance des éléments à protéger :** la connaissance des éléments à protéger est cruciale pour la mise à l'échelle de l'architecture Zero Trust sur l'ensemble des appareils, réseaux et applications de l'entreprise. L'automatisation aide les entreprises à surveiller et enregistrer ces ressources dans divers emplacements et dans le cloud.
- **Conformité permanente :** pour faire face à l'utilisation de bots et d'autres outils d'automatisation par les cybercriminels, il faut un système de sécurité qui recherche en permanence la présence de nouvelles menaces. L'automatisation de l'architecture Zero Trust assure l'application en continu des politiques, 24 heures sur 24, 365 jours par an.
- **Risques réduits :** les équipes InfoSec peuvent adopter des politiques et des règles au fur et à mesure que les incidents se produisent. Ces processus peuvent ensuite être codifiés dans des workflows et exécutés de manière automatisée, ce qui réduit le risque d'erreurs humaines que peuvent commettre les administrateurs lors de leur mise en œuvre.
- **Meilleure réactivité :** plus le délai de réponse à un incident est long, plus les risques de failles ou de cyberattaques augmentent. L'automatisation de l'architecture Zero Trust permet aux organisations de réagir rapidement aux événements, qu'elles comptent 1 000 ou 100 000 utilisateurs, en créant des actions automatisées pouvant être exécutées à la demande ou via des processus automatisés orientés événements.
- **Accélération du prototypage :** l'automatisation permet aux organisations de créer des prototypes, d'effectuer des tests et d'apporter des changements à l'infrastructure de sécurité, quelle que soit sa complexité.

Automatiser l'architecture Zero Trust au-delà de la sécurité

En déployant le modèle Zero Trust au-delà du réseau et des processus de sécurité, les organisations peuvent véritablement placer la sécurité au cœur de chaque projet ou système. L'automatisation de ces processus confère encore plus de valeur au modèle Zero Trust, par l'application et la vérification des politiques et processus dans le but de réduire les risques de cyberattaques ou d'autres failles.

Cohérence dans la sécurité et la conformité

L'automatisation aide à appliquer les règles de sécurité et de conformité en gérant les configurations, le déploiement d'applications et les vérifications de conformité qui enrichissent les processus de développement. Les entreprises peuvent automatiser le provisionnement, la configuration, le déploiement d'applications et bien d'autres processus.

L'automatisation apporte bien plus que la simple sécurisation des applications et des composants. Elle peut également servir à assurer le bon fonctionnement de ces éléments ainsi qu'à effectuer des vérifications et des contrôles réguliers de la conformité. L'automatisation permet l'application continue et de bout en bout de la posture de sécurité pour le cycle CI/CD (intégration et développement continus) de l'entreprise.

Sécurité globale des logiciels

Les principes du modèle Zero Trust peuvent également s'appliquer aux logiciels et systèmes d'une organisation. Les équipes et les services ont souvent besoin de différentes applications, appareils et solutions qui ne sont pas immédiatement interopérables. L'automatisation aide à intégrer différents systèmes provenant de fournisseurs variés, en permettant la création de workflows automatisés afin d'orchestrer l'interopérabilité de manière efficace et sécurisée.

Plus important encore, les solutions développées par les équipes internes et externes peuvent inclure des composants Open Source qui, s'ils ne sont pas surveillés dans le but de détecter les vulnérabilités, peuvent être source de nouveaux vecteurs d'attaque pour les cybercriminels. Les mêmes processus automatisés créés pour gérer l'interopérabilité peuvent être utilisés pour maintenir la sécurité des applications.

Automatisation de la conformité

L'automatisation peut être utilisée pour limiter les erreurs humaines lors de la réalisation de tâches liées à la conformité. Par exemple, elle peut s'avérer utile pour les entreprises qui traitent des transactions par carte de crédit. De multiples processus et contrôles du matériel et des logiciels sont nécessaires pour vérifier la conformité avec la norme PCI DSS (Payment Card Industry Data Security Standard). Ces audits nécessitent des données exactes et à jour, issues de ces différents systèmes. Au lieu de confier la surveillance de ces processus à un ou plusieurs membres d'une équipe, l'automatisation peut être utilisée afin de diminuer les erreurs humaines et libérer du temps que le personnel pourra consacrer à d'autres projets plus stratégiques.

Automatiser l'architecture Zero Trust et plus encore avec Red Hat Ansible Automation Platform

Pour en savoir plus sur la manière dont l'automatisation peut vous être utile, consultez le livre numérique Red Hat Ansible Automation Platform : le guide du débutant.

Pour que le modèle Zero Trust fonctionne, les organisations doivent savoir avec précision où se déroulent les transactions. La solution Red Hat Ansible Automation Platform permet de déployer le modèle Zero Trust et l'automatisation dans toute l'entreprise. Cette plateforme offre un retour sur investissement rapide en éliminant les obstacles à l'automatisation au niveau de la sécurité, du réseau, des applications, du cloud et de l'edge computing.

Modèle Zero Trust	Automatiser l'architecture Zero Trust avec Red Hat Ansible Automation Platform
Le modèle Zero Trust repose sur une approche de « rejet par défaut ».	La solution Red Hat Ansible Automation Platform permet aux administrateurs d'appliquer des contrôles d'accès pour attribuer des autorisations, des privilèges et des rôles aux utilisateurs. Elle automatise également le chiffrement, notamment le protocole mTLS (Mutual Transport Layer Security), ainsi que les journaux d'audit et les contrôles d'inventaire.
Le modèle Zero Trust se base sur des politiques d'autorisation pour restreindre l'accès aux applications et ressources.	La solution Red Hat Insights for Ansible Automation Platform peut aider les organisations à surveiller et identifier les pannes ou risques potentiels pour lesquels l'intervention des équipes SysOps or NetOps pourrait s'avérer nécessaire.
Le modèle Zero Trust garantit que des correctifs sont appliqués aux ressources avant que les utilisateurs y accèdent.	La solution Red Hat Ansible Automation Platform garantit que des correctifs et des mises à jour sont appliqués aux ressources des applications dans l'ensemble de l'infrastructure de l'entreprise.

La solution Red Hat Ansible Automation Platform joue le rôle de lien entre les technologies diverses et variées, qui ne communiqueraient pas bien entre elles autrement. Il existe plus de 100 collections de contenus Ansible Content Collections, prises en charge par Red Hat et ses partenaires. Ces contenus certifiés par Red Hat permettent d'automatiser de manière cohérente tous les composants de l'infrastructure, qu'elle soit hybride, dans le cloud ou sur site.

Commencer l'automatisation de l'architecture Zero Trust

L'équipe de consulting Red Hat peut vous aider à adopter le modèle Zero Trust dans le cadre de votre parcours d'automatisation. Effectuez cette auto-évaluation rapide, ou contactez notre équipe de consulting dès aujourd'hui.

Apprenez-en davantage sur l'automatisation informatique et démarrez un essai dès maintenant.

À propos de Red Hat

Premier éditeur mondial de solutions Open Source, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et à automatiser des environnements complexes. Conseiller de confiance auprès des entreprises du Fortune 500, Red Hat propose des services d'assistance, de formation et de consulting reconnus qui apportent à tout secteur les avantages de l'innovation ouverte. Situé au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, Red Hat participe à la croissance et à la transformation des entreprises et les aide à se préparer à un avenir toujours plus numérique.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
F32053