DELL Technologies

5 Recommandations pour répondre à vos besoins en matière de Zero-Trust

1	2	3	4	5
Planifier le changement de paradigme vers la confiance zéro et la vérification systématique	**Choisir sa stratégie**	**L’entreprise gère l’environnement Zero-Trust, et non l’inverse**	**Se concentrer sur les données**	**Appliquer le principe de confiance zéro et de vérification systématique dans tout l’écosystème IT**
Déterminer le compromis acceptable entre atténuation des risques et impact sur l’entreprise	Amélioration de la sécurité incrémentielle	Mettre en place des contrôles en fonction des besoins de l’entreprise	Veiller à ce que chaque activité au niveau du réseau, des appareils et des utilisateurs soit consignée	Les mesures Zero-Trust telles que l’authentification multifacteur et la gestion des identités doivent être appliquées de manière universelle pour éviter les failles critiques
Tenir compte des coûts, de l’impact sur les opérations et les parties prenantes, ainsi que des exigences de conformité et réglementaires	Hyperscalers	Documenter les processus, les rôles, les responsabilités et les classifications de données	Utiliser l’IA et le ML pour analyser les données et identifier les anomalies pouvant révéler une menace	Inclure les chaînes logistiques physiques et numériques tierces dans le cadre Zero-Trust
Passer d’une sécurité basée sur le périmètre à un modèle micro-segmenté axé sur les données	Environnement dédié	L’expérience utilisateur reste essentielle	Garder à l’esprit que la protection des données et des applications est la principale mission d’une architecture Zero-Trust	
Faire appel à un prestataire externe en cas de besoin	L’identité est le nouveau périmètre	Les avancées en matière de sécurité telles que le cadre Zero-Trust ne peuvent pas se faire au détriment de la convivialité		
		Les objectifs organisationnels tels que la croissance et l’innovation restent essentiels		

Le Zero-Trust apparaît aujourd'hui comme la bonne pratique à adopter pour l'architecture de sécurité.

Les données montrent que la plupart des entreprises ont commencé à envisager ou sont en train de mettre en œuvre le modèle Zero-Trust[1]. Bien que le passage au Zero-Trust soit important, certaines questions pratiques vous aideront à orienter votre stratégie.

L'experte Dell Technologies Tracy Emmersen, Director of Solution Adoption for Project Fort Zero, et Justin Vogt, Principal Security Engineer, ont partagé leurs recommandations et leur point de vue avec Ash Lakshmanan, Security Services Product Manager. Leurs principales suggestions sont résumées ci-dessous, et vous retrouverez l'intégralité de l'échange sur dell.com/cybersecuritymonth.

> « Lorsque nous considérons le Zero-Trust d'un point de vue holistique, lorsque nous prenons du recul, tout repose sur les données. »
>
> ***Tracy Emmersen***
> *Director of Solution Adoption for Project Fort Zero, Dell Technologies*

Planifier le changement (important) de paradigme vers la confiance zéro et la vérification systématique

Fondamentalement, l'adoption d'un environnement Zero-Trust représente un changement majeur par rapport aux modèles de sécurité classiques, qui reposent sur les principes suivants : la confiance zéro, la vérification systématique et le principe du moindre privilège. « Nous devons faire évoluer notre posture de sécurité en nous éloignant des solutions de sécurité réseau traditionnelles basées sur le périmètre et en nous orientant davantage vers une architecture micro-segmentée et centrée sur les données », remarque Mme Emmersen.

Choisir sa stratégie

Mme Emmersen distingue trois stratégies pour tirer parti du Zero-Trust :

- **Incrémentiel :** une approche itérative qui intègre les principes clés du Zero-Trust à l'environnement actuel
- **Hyperscaler :** tirer parti des fonctionnalités Zero-Trust des principaux fournisseurs de Cloud
- **Environnement dédié et entièrement conforme :** environnement privé sur site entièrement dédié et strictement conforme aux normes Zero-Trust

Outre ces trois stratégies, les PME présentes en ligne peuvent également suivre une approche nommée « L'identité est le nouveau périmètre ». Cette méthodologie repose sur la gestion des identités et des accès et exploite les outils SaaS pour mettre en place une protection basée sur le Zero-Trust. L'un des composants essentiels de cette méthode est l'application systématique de l'authentification multifacteur, illustrant l'impact de cette capacité Zero-Trust unique.

Les approches par l'identité et l'hyperscaler sont généralement moins coûteuses, tandis que les environnements incrémentiels et dédiés nécessitent un investissement plus important.

L'entreprise favorise l'adoption du Zero-Trust, et non l'inverse

Par essence, une architecture Zero-Trust est conçue pour administrer et sécuriser les workflows, les rôles d'utilisateur et les privilèges associés, les appareils, les données, les applications et les réseaux d'une entreprise. La première étape de la mise en œuvre nécessite donc une documentation solide de ces aspects. Ensuite, le plan de contrôle et l'infrastructure sont créés pour appliquer les stratégies qui les régissent.

Si l'environnement Zero-Trust inhibe ou modifie considérablement les opérations au détriment de l'entreprise, cela ne vaut pas la peine de renforcer la sécurité. Comme le souligne M. Vogt, « si [la sécurité]… entrave la mission principale de l'entreprise… nous ne valons pas mieux que les adversaires que nous cherchons à repousser. Nous venons de créer notre propre déni de service ».

Se concentrer sur les données

Comme le souligne Mme Emmersen, « lorsque nous considérons le Zero-Trust d'un point de vue holistique, lorsque nous prenons du recul, nous constatons que tout repose sur les données ». La protection des données de l'entreprise est l'un des avantages les plus précieux du passage au Zero-Trust. De plus, des principes tels que la vérification continue et la segmentation protègent les données et les applications en empêchant les menaces de se déplacer latéralement au sein du réseau.

La journalisation et la surveillance continue sont des composants essentiels du Zero-Trust. Les données et la télémétrie sont analysées pour identifier les anomalies susceptibles d'indiquer un risque ou une menace. Par exemple, un changement dans les modèles d'utilisation des données peut être le signe d'une tentative d'exfiltration ou d'une attaque par ransomware.

1. D'après une étude réalisée à la demande de Dell par Enterprise Strategy Group, « Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust », novembre 2023

DELL Technologies

Compte tenu de la grande quantité de données générées par la journalisation des activités, les outils d'analyse modernes doivent utiliser l'IA et le ML pour être efficaces.

Confiance zéro et vérification systématique dans tous les domaines

Bien que l'accent soit mis sur les données, les applications, les utilisateurs et les appareils en interne, la surveillance inhérente à une architecture Zero-Trust doit s'appliquer tout au long du cycle de vie IT. Dans le cas contraire, l'entreprise s'exposerait à des failles de sécurité critiques.

La chaîne logistique en est un bon exemple, et M. Vogt invite à se poser un certain nombre de questions clés sur les solutions matérielles et logicielles tierces :

- Qui d'autre y avait accès ?
- Quels en sont les composants ?
- Quels sont les processus sous-jacents ?
- Comment pouvons-nous adopter ces principes de confiance zéro [et] mettre en place un processus de vérification ainsi que le principe du moindre privilège (POLP) vis-à-vis de la technologie que nous utilisons ? Même si cela est mis en œuvre en amont dans la chaîne logistique technologique ?

L'adoption d'une architecture Zero-Trust ou la mise en œuvre de ses principes est le meilleur moyen utilisé actuellement pour faire progresser sa maturité en matière de cybersécurité. Différents compromis entre coût, risque et niveau d'amélioration de la sécurité sont possibles. La première étape consiste à déterminer la position de l'entreprise qui guidera ensuite les décisions technologiques.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **dell.com/cybersecuritymonth**