

**A C C É L É R É R**

**LE ZERO TRUST AVEC UNE**

**AUTHENTIFICATION  
SOLIDE**



# Table des matières

<b>1</b>	<b>Les défis post-pandémiques de la cybersécurité</b>	<b>2</b>
	i. Absence d'un périmètre bien défini	2
	ii. Shadow IT	2
	iii. Manque de visibilité du réseau	3
<b>2</b>	<b>Atténuer les problèmes de cybersécurité post-pandémie</b>	<b>3</b>
<b>3</b>	<b>Les principes du Zero Trust</b>	<b>3</b>
	i. Ne jamais faire confiance, toujours vérifier	3
	ii. Sécuriser les données à l'aide de stratégies granulaires basées sur le contexte	4
	iii. Surveillance continue	4
<b>4</b>	<b>Pourquoi utiliser le Zero Trust ?</b>	<b>5</b>
<b>5</b>	<b>Authentification : le premier pas vers le Zero Trust</b>	<b>6</b>
<b>6</b>	<b>Capacités IAM pour accélérer le Zero Trust</b>	<b>7</b>
	i. Authentification unique (SSO)	7
	ii. Authentification multifactorielle (MFA)	7
	iii. Authentification contextuelle	8
	iv. Authentification adaptative	8
<b>7</b>	<b>IAM et Zero Trust : Un duo compatible</b>	<b>8</b>
<b>8</b>	<b>Le Zero Trust - la technique de ManageEngine</b>	<b>9</b>

La pandémie mondiale a eu un impact profond sur de nombreuses infrastructures. Plus de deux ans se sont écoulés, et les entreprises continuent de fonctionner entièrement à distance ou s'orientent lentement vers un un modèle hybride. Cette évolution massive s'est accompagnée d'un risque important danger : une augmentation record du nombre de cybermenaces.

Selon le rapport

**Global Cybersecurity  
Outlook 2022,**

les attaques de ransomware ont connu une augmentation significative au cours des six premiers mois de 2021, le volume global des attaques ayant

augmenté de

**151%**

Le système de sécurité traditionnel pré-pandémique est inadéquat pour gérer la main-d'œuvre actuelle en mouvement constant. Un modèle de sécurité basé sur l'identité est nécessaire pour sécuriser la main-d'œuvre sans périmètre, qui peut être mis en œuvre par une architecture de Zero Trust. Dans cet e-book, nous examinerons les défis de la cybersécurité qui sont apparus après la pandémie, pourquoi le Zero Trust est la clé pour résoudre ces problèmes de sécurité modernes, et comment l'authentification, parmi tous les outils, joue un rôle clé dans la création d'un environnement de Zero Trust efficace.

# 1

## Les défis post-pandémiques de la cybersécurité

Les organisations ont dû adopter d'autres modèles de main-d'œuvre et d'infrastructure pour survivre aux conséquences de la pandémie, comme une dépendance accrue à l'égard de l'informatique en cloud et une évolution vers une main-d'œuvre hybride et entièrement à distance. Ces changements ont apporté de nombreux avantages, comme l'amélioration de l'évolutivité des réseaux, l'accélération de la transformation numérique et la personnalisation de l'expérience des employés, mais ils se sont accompagnés d'un inconvénient majeur de lacunes en matière de sécurité, comme les suivantes :



### i. Absence d'un périmètre bien défini

De nombreux employés travaillent désormais avec une certaine flexibilité quant à leur localisation, potentiellement de n'importe où dans le monde. Cette flexibilité a rendu la sécurisation du réseau et des actifs critiques d'une organisation encore plus difficile en raison de l'absence d'un périmètre bien défini.

Les mesures de sécurité traditionnelles sont orientées vers la sécurisation des périmètres physiques, mais ne sont pas bien préparées pour un réseau sans frontières. Les approches modernes de la cybersécurité doivent être étendues et couvrir tous les terminaux connectés au réseau, quel que soit l'endroit d'où ils sont connectés.



### ii. Shadow IT

Une [enquête menée par Bitglass en 2021](#) a révélé que plus de 82 % des entreprises ont adopté, dans une certaine mesure, des **politiques de BYOD** (Bring Your Own Device).

**82%** des entreprises ont adopté

La généralisation du BYOD a suscité des inquiétudes quant au shadow IT, qui désigne l'utilisation non autorisée de systèmes, d'appareils et de logiciels informatiques au sein des réseaux organisationnels. Les employés utilisent leurs appareils personnels non gérés pour télécharger toutes sortes d'informations et d'applications, dont certaines peuvent contenir des logiciels malveillants.

L'absence d'alignement de ces appareils sur les politiques informatiques de l'organisation peut entraîner l'afflux de trafic non autorisé, la corruption de données et de logiciels et, finalement, l'accès de pirates et de logiciels malveillants au réseau de l'organisation.



### iii. Manque de visibilité du réseau

L'ère de l'infrastructure de travail hybride a rendu la gestion du réseau encore plus difficile. Lorsqu'une organisation dispose de la plupart des terminaux ou des dispositifs connectés à son réseau répartis dans le monde entier, il est pratiquement impossible de surveiller l'activité du réseau à partir d'une plateforme centrale. Outre la difficulté accrue de surveiller le trafic provenant de ces dispositifs, certains de ces terminaux peuvent fonctionner à partir de réseaux externes compromis, ce qui augmente le risque d'attaque.

## 2

# Atténuation des problèmes de cybersécurité post-pandémie

La transition progressive vers une main-d'œuvre hybride entraîne une charge de vérification et de surveillance d'un ensemble mixte de terminaux en fonction des politiques informatiques spécifiques de l'entreprise. Pour optimiser les avantages d'un modèle hybride, les entreprises doivent adopter une approche de cybersécurité qui protège tous les terminaux et leurs applications au sein du réseau, qu'ils soient gérés ou non. Une solution consiste à adopter une architecture de réseau "Zero Trust", qui comprend des méthodes permettant d'atténuer les problèmes de cybersécurité post-pandémie.

## 3

# Les principes de Zero Trust

Il est plus facile de relever les défis de la cybersécurité post-pandémique avec le Zero Trust, car elle part du principe qu'aucune entité du réseau n'est digne de confiance et qu'elle doit donc être authentifiée, autorisée et surveillée en permanence afin de conserver l'accès au réseau de l'organisation. Voici quelques-uns des principes fondamentaux qui sous-tendent le Zero Trust :



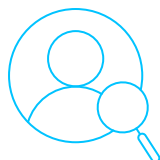
### **i. Ne jamais faire confiance, toujours vérifier**

Par rapport aux systèmes de sécurité traditionnels, qui s'appuient sur la création d'un périmètre physiquement défini pour définir les terminaux autorisés, Zero Trust élargit la portée des périmètres de sécurité. Il adopte l'approche " Ne jamais faire confiance, toujours vérifier ", ce qui signifie que chaque entité, quel que soit l'endroit où elle se trouve sur le réseau, doit se soumettre à un processus de vérification fin avant d'accéder aux ressources de l'organisation.



### **ii. Sécuriser les données à l'aide de politiques granulaires basées sur le contexte**

L'architecture fondamentale de Zero Trust est établie avec micro-segmentation. La micro-segmentation divise le réseau en zones, jusqu'au niveau de la charge de travail individuelle. Cette segmentation facilite la définition et la sécurisation des données et des accès de chaque zone en mettant en œuvre des politiques de sécurité spécifiques basées sur le contexte, telles que le principe du moindre privilège. Cette politique garantit que chaque utilisateur n'obtient que le minimum d'accès nécessaire à l'exécution de ses tâches. En rendant la sécurité aussi granulaire que possible, Zero Trust réduit finalement la surface d'attaque des menaces potentielles.



### **iii. Surveillance continue**

Les employés se voient confier des données sensibles et ont un accès légitime aux actifs de l'entreprise. Ils sont l'un des éléments clés d'une organisation, mais aussi l'une des plus grandes sources de vulnérabilités et de menaces. Par conséquent, le troisième ingrédient, tout aussi important, de la confiance zéro est l'atténuation des risques par une surveillance continue.

La mise en œuvre de la gestion des informations et des événements de sécurité (SIEM) permet de collecter les activités numériques des employés. Une fois que ces données sont centralisées et qu'elles contiennent suffisamment d'informations historiques, une base de référence du comportement habituel de chaque utilisateur et de chaque machine peut être établie à l'aide de solutions d'analyse du comportement des utilisateurs et des entités (UEBA). Toute déviation par rapport aux lignes de base établies pour chaque utilisateur et entité est identifiée comme anormale et est ensuite envoyée pour une évaluation du profil pour d'autres risques potentiels. Si le score de risque dépasse un seuil particulier en raison d'un nombre croissant d'activités anormales, le système déclenche une alerte de sécurité pour avertir les administrateurs du réseau.

# 4

## Pourquoi utiliser le Zero Trust?

Pour expliquer pourquoi le Zero Trust devrait être utilisée, examinons le modèle traditionnel de sécurité des réseaux : La stratégie du château et des douves.

Cette stratégie est inspirée d'une stratégie de défense médiévale consistant à sécuriser un château en construisant des douves pour entourer les murs du château. Pour faire le lien avec la sécurité du réseau, le modèle du château et des douves garantit que personne en dehors du périmètre du réseau ne peut accéder aux données de l'organisation. L'utilisation de pare-feu, de systèmes de détection des intrusions (IDS) et de systèmes de prévention des intrusions (IPS) contribue à sécuriser le périmètre du réseau.

Cependant, qu'en est-il d'une menace interne, comme un employé mécontent ou une personne extérieure qui accède au réseau en volant des informations d'identification ? Comment une stratégie de type "château et douves" peut-elle sécuriser un réseau sans périmètre ? Au fil du temps, il est devenu évident que le modèle des châteaux et des douves ne répond pas à ces préoccupations, ce qui a donné naissance à l'architecture de Zero Trust. Le Zero Trust prend en charge tous les pires scénarios en ne se contentant pas de sécuriser l'ensemble du réseau, comme dans le cas de l'approche "château et douves", mais en allant au-delà du périmètre du réseau.

En évitant de placer la confiance sous une forme binaire, le Zero Trust est impartiale lorsqu'il considère qui ou quoi autoriser l'accès. La confiance binaire implique qu'il faut faire confiance à un utilisateur pour tout ou rien. Mais dans une organisation, tout le monde n'a pas besoin d'avoir accès à tout. Rendre les données sensibles accessibles à tous revient à augmenter leur vulnérabilité. Pour protéger une organisation contre les attaques de l'intérieur, une vérification et un contrôle continus des employés sont nécessaires, ce qui signifie également qu'il ne faut pas leur accorder une confiance permanente.

Une autre raison pour laquelle votre organisation devrait utiliser le Zero Trust est qu'il est guidé par le contexte. Le contexte aide Zero Trust à assurer la mise en œuvre appropriée des stratégies de sécurité et des niveaux d'accès. Par exemple : Si un utilisateur légitime se connecte à partir d'un nouvel emplacement géographique, au lieu de bloquer complètement son accès, Zero Trust permet à cet utilisateur d'accéder au réseau, mais seulement après avoir utilisé l'authentification contextuelle ou adaptative (que nous explorerons dans une section ultérieure). Les indices contextuels basés sur l'utilisateur et le réseau - tels que le type d'appareil utilisé, le département auquel l'utilisateur appartient, l'emplacement géographique du dispositif d'accès, le type d'emploi de l'utilisateur, les ressources auxquelles il accède et ce qu'il fait avec la ressource - aident Zero Trust à surveiller et à évaluer la sécurité du réseau.

Selon le rapport [State of Cloud Security 2021](#), "36 % des professionnels du cloud déclarent que leur organisation a subi une grave fuite de données dans le cloud ou une violation au cours de l'année écoulée." Bien que cette statistique soit préoccupante, les organisations ne doivent pas se sentir impuissantes lorsqu'il s'agit de sécuriser le cloud. Zero Trust permet de limiter les fuites de données dans le cloud en offrant une meilleure visibilité et une meilleure gestion des accès à l'infrastructure du cloud. Les politiques de sécurité de Zero Trust permettent de sécuriser l'architecture du cloud en régissant l'accès aux ressources et en auditant en permanence les serveurs du cloud.

En résumé, Zero Trust est une stratégie de cybersécurité globale qui peut être adoptée pour les infrastructures informatiques en cloud et sur site. Il soutient et sécurise la main-d'œuvre moderne en validant et en autorisant chaque utilisateur et chaque appareil du réseau, à l'aide d'un ensemble exhaustif de politiques. La micro-segmentation aide les organisations à obtenir une visibilité d'entreprise à grain fin et à mettre en œuvre des stratégies de sécurité. En outre, la surveillance et l'audit continus des utilisateurs et des entités permettent de suivre les activités inhabituelles et de déterminer le niveau de risque. Avec chacun de ces éléments de Zero Trust mis en œuvre, une organisation peut toujours avoir une longueur d'avance sur les menaces de cybersécurité.

## 5

# L'authentification : le premier pas vers le Zero Trust

L'authentification est le processus de vérification de l'identité d'un utilisateur. Elle contribue au pilier de l'architecture de sécurité du réseau d'une organisation. Si le processus d'authentification de l'organisation est inefficace, l'ensemble de la sécurité du réseau finira par s'effondrer.

Comme nous l'avons déjà dit, une main-d'œuvre hybride s'accompagne d'un ensemble de réseaux et de dispositifs non gérés ; par conséquent, afin de combler les lacunes existantes en matière de sécurité, il est essentiel de protéger l'identité de l'utilisateur et de la machine.

La granularité est ce qui rend l'authentification Zero Trust plus sûre. Grâce à la micro-segmentation, elle décompose les accès multiples et applique le bon niveau d'authentification pour protéger chacun de ces segments. Ce processus permet de supprimer l'accès inutile aux données de l'entreprise pour les employés non concernés.

En outre, en fournissant une méthode d'authentification flexible basée sur le contexte, le Zero Trust assure une entrée sans friction des employés légitimes dans le réseau de l'organisation.

# Les capacités IAM pour accélérer le Zero Trust

La gestion des identités et des accès (IAM) est un ensemble de politiques, de processus et d'outils qui permettent d'authentifier la bonne identité des utilisateurs et de leur fournir le bon niveau d'accès. Avant de choisir une solution de gestion des identités et des accès, les administrateurs de la sécurité informatique devraient rechercher les fonctions d'authentification indispensables pour démarrer avec le Zero Trust :



## i. L'authentification unique (SSO)

Même si les professionnels de la sécurité insistent sur la création d'un mot de passe fort, il est assez difficile de se souvenir de dizaines de mots de passe pour plusieurs applications différentes, ce qui conduit finalement à la lassitude des mots de passe

Selon le rapport [Verizon Data Breach Investigations 2022](#), les informations d'identification sont l'une des principales voies d'accès à une violation de données.

Avec le SSO, un utilisateur s'authentifie en utilisant un seul ensemble d'identifiants de connexion pour accéder à plusieurs applications. Il élimine le besoin de demandes d'authentification multiples sur diverses plateformes, ce qui minimise la fatigue liée aux mots de passe et augmente la productivité des employés.



## ii. Authentification multifactorielle (MFA)

En raison de la sophistication croissante des cyberattaques, les systèmes d'authentification basés sur le nom d'utilisateur et le mot de passe sont insuffisants. En ajoutant une couche de sécurité au processus d'authentification de l'utilisateur, la MFA protège de la vulnérabilité des mots de passe. Les couches de sécurité les plus courantes ou les facteurs de vérification sont les suivants :

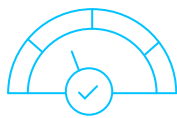
- Quelque chose que vous connaissez ; par exemple, les mots de passe.
- Quelque chose que vous avez ; par exemple, la vérification du mot de passe à usage unique (OTP) par le biais du téléphone portable.
- Quelque chose que vous êtes ; par exemple, la vérification biométrique.

Même si le mot de passe est compromis, en obligeant une tentative d'authentification à être validée par plus d'une méthode, la MFA garantit un accès sécurisé au réseau.



### iii. Authentification contextuelle

Il est possible d'améliorer le processus d'authentification MFA grâce à l'authentification contextuelle. Au cours du processus d'authentification, chaque profil est évalué en fonction du contexte de sa demande d'accès, comme le lieu, l'heure, le dispositif, le réseau et l'application. Si le contexte de l'utilisateur correspond aux conditions définies par la sécurité informatique, le système authentifie l'utilisateur et lui donne un accès complet aux fonctions qui lui ont été attribuées. En cas d'anomalie mineure, l'accès peut n'être que partiel et si le contexte de l'utilisateur ne répond pas aux conditions de sécurité, son accès sera bloqué.



### iv. Authentification adaptative

L'authentification adaptative réunit sous un même toit les techniques d'apprentissage automatique et celles basées sur le contexte. L'authentification adaptative, également appelée authentification basée sur le risque, consiste à sélectionner un niveau d'authentification approprié en fonction du score de risque d'un employé.

La connexion de l'utilisateur et son comportement en ligne sont évalués pour chaque profil, puis classés avec un score de risque. En fonction de ce score de risque, l'outil de vérification décide s'il faut demander des informations d'identification supplémentaires, comme un OTP par e-mail ou SMS, ou s'il faut accorder l'accès avec moins d'informations d'identification.

# 7

## IAM et le Zero Trust : Un duo compatible

La capacité d'optimiser le profil d'identité d'un utilisateur est une caractéristique partagée par Zero Trust et IAM. Bien qu'une stratégie IAM de gouvernance des identités constitue la base de l'architecture Zero Trust, nous ne pouvons pas nous lancer dans une stratégie Zero Trust sans tenir compte de l'IAM. Voici comment l'IAM soutient le Zero Trust :

- ✓ Que l'employé se connecte depuis son bureau ou à distance, IAM valide l'identité de chaque utilisateur. En combinant l'approche du Zero Trust "ne jamais faire confiance, toujours vérifier" avec des stratégies IAM fortes, une organisation garantit un accès sécurisé à la bonne identité chaque fois que quelqu'un essaie d'entrer dans le réseau.

- ✔ Outre la vérification, l'IAM lie également le bon niveau d'accès à la bonne identité, en veillant à ce que chaque employé ne puisse récupérer que le strict minimum de données nécessaires à l'accomplissement de son travail. C'est une façon de mettre en œuvre des stratégies qui respectent le principe de moindre privilège de Zero Trust.
- ✔ Les outils IAM contrôlent et audient de manière exhaustive les journaux d'accès. Ces informations peuvent permettre aux équipes de sécurité informatique d'avoir une visibilité fine du comportement de chaque utilisateur et de chaque appareil.
- ✔ Avec le SSO et le MFA, l'IAM renforce le jeu des justificatifs d'identité d'une organisation, dynamisant ainsi le processus de vérification.
- ✔ Zero Trust surveille en permanence les utilisateurs et évalue leurs privilèges d'accès. L'IAM soutient ce principe avec la gestion automatisée du cycle de vie et la gouvernance des identités, qui permettent toutes deux de gérer les identités des utilisateurs et de mettre à jour leurs accès tout au long de leur cycle de vie.

## 8

# Zero Trust - la méthode ManageEngine

La première étape et le fondement de toute stratégie de Zero Trust est l'identité. Avec AD360 de ManageEngine, tous les besoins en matière de gestion des identités et des accès peuvent être satisfaits en un seul endroit. Il permet de réaliser toutes les opérations critiques de gestion des identités et des accès, telles que l'attribution des utilisateurs, la gestion des mots de passe en libre-service, la surveillance des changements dans Active Directory, le MFA, le SSO, etc. avec une interface simple et facile à utiliser.

Ses principales fonctionnalités comprennent l'évaluation automatique des risques et la veille sur les menaces, ainsi que l'authentification adaptative et la gestion automatisée du cycle de vie des utilisateurs et des droits pour une meilleure gouvernance des identités. En automatisant les tâches IAM de routine, comme l'attribution, la modification et le retrait d'utilisateurs, AD360 contribue à éliminer les erreurs humaines et les redondances. Il permet d'appliquer l'accès le moins privilégié possible, ce qui est essentiel pour détecter et prévenir les abus de privilèges. En outre, il facilite la surveillance et l'audit continu de l'activité des employés. Qu'il s'agisse d'une solution sur site, en cloud ou hybride, AD360 peut rendre une infrastructure informatique plus sûre et facile à gérer.



## À propos de ManageEngine AD360

AD360 est une solution unifiée de gestion des identités et des accès qui permet de gérer les identités, de sécuriser les accès et de garantir la conformité. Elle est dotée de puissantes fonctionnalités telles que la gestion automatisée du cycle de vie des identités, le SSO sécurisé, le MFA adaptatif, les flux de travail basés sur l'approbation, la protection contre les menaces liées aux identités basée sur l'UBA et les rapports d'audit historiques pour AD, Exchange Server et Microsoft 365. L'interface intuitive et les puissantes fonctionnalités d'AD360 en font la solution idéale pour tous vos besoins en matière d'IAM, notamment pour favoriser un environnement de Zero Trust.

[\\$ Obtenir un devis](#)

[↓ Télécharger](#)