ivanti

Cybersecurity
INSIDERS

Rapport 2021 sur la progression du Zero Trust

ivanti.fr

Vue d'ensemble

L'adoption par les entreprises du modèle de sécurité Zero Trust s'accélère, car la majorité des entreprises prévoient d'implémenter des fonctions Zero Trust pour limiter les cybermenaces toujours plus présentes, surtout après le passage massif au télétravail. Son principe : vérifier l'utilisateur et le périphérique avant d'octroyer un accès conditionnel, basé sur les moindres privilèges. Le Zero Trust tient ainsi ses promesses d'amélioration significative de la facilité d'utilisation, de protection des données et de gouvernance.

Le rapport 2021 sur le Zero Trust montre comment les entreprises implémentent la sécurité Zero Trust dans leur enceinte, et précise les principales motivations, les tendances d'adoption, les technologies, les investissements et les avantages de cette approche.

Pour collecter ces informations, nous avons interrogé différents professionnels de la cybersécurité, des responsables techniques aux techniciens de sécurité IT, pour constituer un panel représentatif d'entreprises de toutes tailles dans plusieurs secteurs d'activité.

Principaux résultats de l'enquête :

- Gagner la confiance via la vérification des entités, notamment des utilisateurs, des périphériques et des composants d'infrastructure (64 %) arrive en tête de la liste des principaux composants du Zero Trust. Viennent ensuite la protection des données (63 %) et l'authentification/l'autorisation en continu (61 %).
- Déterminer les privilèges d'accès actuels de tous les utilisateurs peut s'avérer difficile, pour vérifier que l'accès des utilisateurs est limité aux niveaux appropriés. Plus de 3/4 des entreprises (88 %) reconnaissent que leurs utilisateurs peuvent disposer de privilèges d'accès supérieurs à ce dont ils ont besoin.
- Lorsqu'on leur demande leurs priorités actuelles en matière de sécurité, les professionnels de la cybersécurité mentionnent l'amélioration de l'IAM (gestion des accès et des identités) le plus souvent (68 %), puis la prévention des pertes de données (56 %) et l'accès sécurisé aux applications (46 %).

Merci beaucoup à Ivanti pour son soutien à cet important projet de recherche.

Nous espérons que les informations de ce rapport vous intéresseront et vous aideront à poursuivre vos efforts de protection de vos environnements IT.

Merci,

Holger Schulze

Holger Schulze
PDG et fondateur
Cybersecurity Insiders

Cybersecurity INSIDERS

Les facettes du Zero Trust

Nous avons demandé aux entreprises les aspects du Zero Trust qui les attiraient le plus. Gagner la confiance via la vérification des entités, notamment des utilisateurs, des périphériques et des composants d'infrastructure (64 %) arrive en tête de la liste des principaux composants du Zero Trust. Viennent ensuite la protection des données (63 %) et l'authentification/l'autorisation en continu (61 %).

Quelles facettes du Zero Trust sont les plus attractives pour vous et votre entreprise ?[1]

64%

Gagner la confiance via la vérification des entités
(utilisateurs, périphériques, infrastructure, etc.)

63%

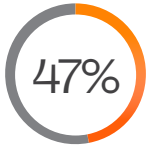
Protection des données
(ex., connexion sécurisée)

61%

Authentification/ autorisation en continu

Visibilité de bout en bout et audit des accès

Facilitation des accès avec moindres privilèges



Stratégie d'accès centralisée et détaillée

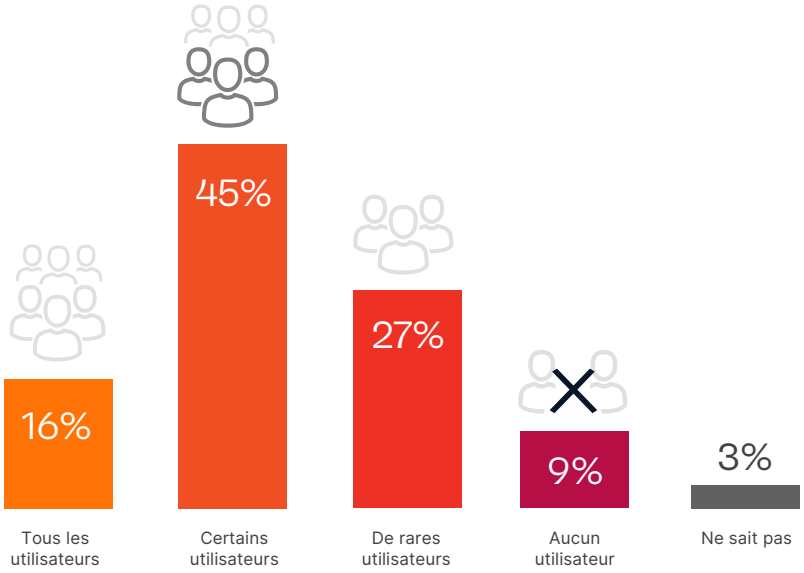
Aucune différence de confiance entre les réseaux internes et externes

Privilèges d'accès excessifs

Déterminer les privilèges d'accès actuels de tous les utilisateurs peut s'avérer difficile, pour vérifier que l'accès des utilisateurs est limité aux niveaux appropriés. Plus de 3/4 des entreprises (88 %) reconnaissent que leurs utilisateurs peuvent disposer de privilèges d'accès supérieurs à ce dont ils ont besoin.

Dans quelle mesure pensez-vous que les utilisateurs de votre entreprise ont des privilèges d'accès supérieurs à leurs besoins ?

88% reconnaissent que leurs utilisateurs peuvent disposer de privilèges d'accès supérieurs à ce dont ils ont besoin.



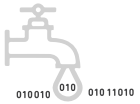
Priorités pour la sécurité

Lorsqu'on leur demande leurs priorités actuelles en matière de sécurité, les professionnels de la cybersécurité mentionnent l'amélioration de l'IAM (gestion des accès et des identités) le plus souvent (68 %), puis la prévention des pertes de données (56 %) et l'accès sécurisé aux applications (46 %).

Quelles sont les priorités actuelles de votre entreprise en matière de sécurité ?[2]

68%

Améliorer la gestion des identités et des accès (IAM)

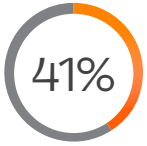


56%

Prévention des pertes de données (DLP)

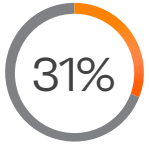
46%

Garantir l'accès sécurisé aux applications hébergées par des fournisseurs de services de Cloud (Microsoft, Amazon, Google, etc.)



Permettre l'EMM (Gestion des terminaux mobiles)/le BYOD (utilisateurs, périphériques, etc.)

Mener une inspection SSL en profondeur (ex., décryptage de session sécurisé pour l'analyse antimalware et filtrage Web/e-mail)



Simplifier la mise en place de l'accès sécurisé (ex., expérience utilisateur, administration)

Améliorer ou remplacer les outils d'accès distant existants (ex., VDI, VPN, RDP)

Priorités pour la gestion des identités/accès et le Zero Trust

Nous avons demandé aux entreprises dans quels aspects du contrôle des identités/accès et de la sécurité Zero Trust elles investissaient. La priorité, en matière d'investissement, est l'authentification multifacteur (58 %), suivie de la gestion et de la gouvernance des identités (48 %), et du SSO (45 %).

Parmi les contrôles des identités/accès et Zero Trust suivants, quelles sont les priorités de votre entreprise en matière d'investissement pour les 12 prochains mois ?[3]

58%

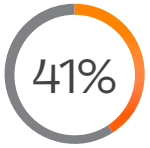
Authentification multifacteur (MFA)

48%

Gestion et gouvernance des identités

45%

Connexion avec identification unique (SSO)



Gestion des accès avec privilèges (PAM), microsegmentation

Réseaux privés virtuels (VPN)

Microsegmentation

Contrôle des accès réseau (NAC), pare-feu d'application Web (WAF)

Priorités en matière d'accès sécurisé

Quand on effectue une analyse en cascade (drilldown) des priorités spécifiques en matière d'accès sécurisé, les entreprises, là encore, priorisent l'authentification multifacteur/la gestion des comptes avec privilèges (69 %). Viennent ensuite la détection et l'élimination des activités anormales (58 %), et la sécurisation de l'accès depuis les périphériques personnels non gérés (55 %).

Quelles sont les priorités de votre entreprise en matière d'accès sécurisé pour les 12 ou 24 mois à venir ?

69%

Authentification multifacteur/ gestion des comptes avec privilèges

58%

Détection et élimination des activités anormales

55%

Sécurisation de l'accès depuis les périphériques personnels non gérés

Réévaluation de l'infrastructure de sécurité traditionnelle et, peut-être, passage à l'accès défini par logiciel

Meilleure visibilité et meilleures mesures de sécurité pour les dirigeants

Microsegmentation

Difficultés de l'accès sécurisé

Les principales inquiétudes concernant la sécurisation de l'accès aux applis et ressources sont d'abord l'accès avec privilèges trop élevés (60 %), puis la fourniture d'un accès sécurisé aux partenaires (50 %). Ces deux aspects sont directement solutionnés par le Zero Trust.

Quelles sont les principales difficultés de votre entreprise en matière de sécurisation de l'accès aux applications et aux ressources ?

60%

Accès des collaborateurs avec des privilèges trop élevés

50%

Accès non sécurisé aux applis et ressources de la part des partenaires

47%

Cyberattaques
(ex., refus de service, scripts intersites, « man-in-the-middle », hameçonnage)

Shadow IT

Processus manuels complexes qui empêchent de réagir rapidement

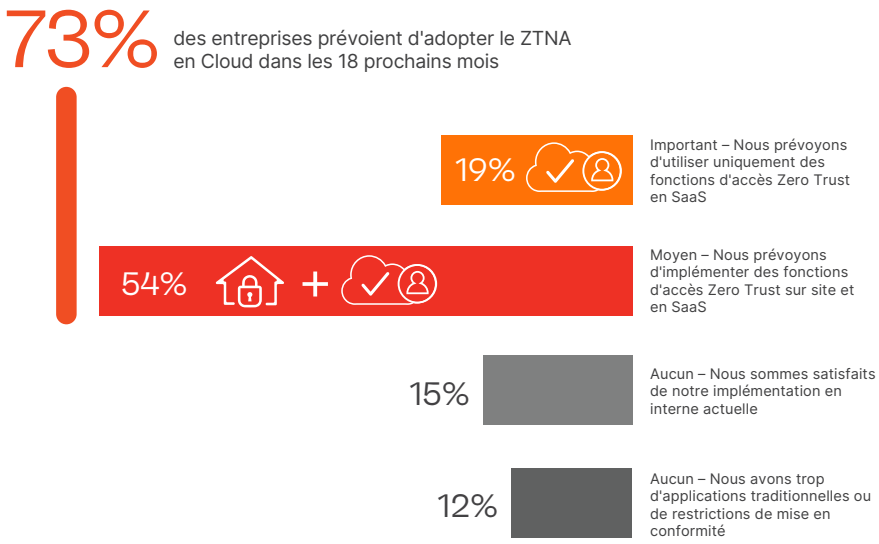
Périphériques mobiles vulnérables, débridés ou perdus accédant aux ressources

Périphériques à risques accédant aux ressources réseau
(terminaux inconnus, non approuvés, non conformes)

Zero Trust en SaaS

La sécurité s'oriente vers le Cloud et l'accès réseau Zero Trust (ZTNA) ne fait pas exception. Près de trois quarts des personnes interrogées prévoient d'adopter une solution de ZTNA en Cloud dans les 18 prochains mois.

Sur les 18 mois à venir, dans quelle mesure vous et votre entreprise prévoyez-vous d'adopter des fonctions d'accès Zero Trust en SaaS ?



Accès aux applis privées

Nous avons demandé aux entreprises quelles étaient leurs plus grandes difficultés en matière de sécurisation des applis privées. Pour plus de la moitié des personnes interrogées, la sécurisation de l'accès aux applications déployées dans les environnements de Cloud public constitue la principale difficulté aujourd'hui (54 %).

Concernant la sécurisation de l'accès aux applis privées, classez les difficultés suivantes par ordre d'importance aujourd'hui ?

54% Accès aux applis dans le Cloud public

29% Accès aux applis dans mon centre de données

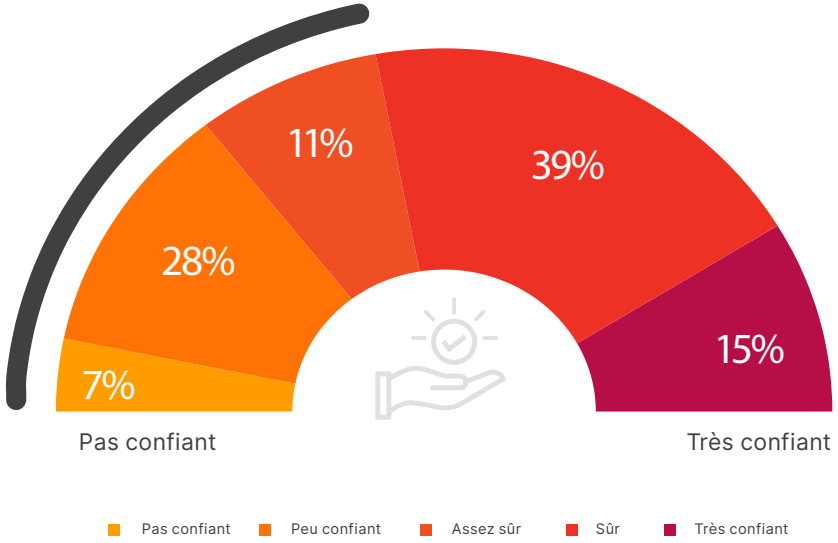
17% Accès aux applis dans mon siège social

Confiance dans le Zero Trust

Lorsqu'on leur demande si elles ont confiance en leur capacité à appliquer le Zero Trust, près de la moitié des équipes de sécurité IT des entreprises manque de confiance (46 %).

Avez-vous confiance en votre capacité à appliquer l'ensemble des aspects/facettes du Zero Trust à votre architecture d'accès sécurisé ?

46% des équipes de sécurité IT des entreprises manquent de confiance en leur capacité à offrir le Zero Trust.



Accès aux applis dans le Cloud public

Les solutions traditionnelles d'accès à distance ne répondent pas aux besoins des environnements de Cloud actuels, dynamiques et distribués. Lorsqu'on demande aux professionnels de la cybersécurité les scénarios qu'ils rencontrent le plus souvent lors de la mise en place de l'accès sécurisé, la plupart mentionnent qu'ils contournent le problème en « épinglant » les utilisateurs distants et mobiles via les centres de données pour l'accès aux Clouds d'applis publics (47 %). Plus inquiétant : 37 % doivent exposer publiquement leurs applis de Cloud pour accepter les utilisateurs distants et mobiles, ce qui représente un risque important.

Parmi les scénarios suivants, lesquels avez-vous rencontrés lors de la mise en place d'un accès sécurisé aux applis de Cloud public pour les utilisateurs distants ou mobiles ?

47%

Je suis contraint d'« épingler » les utilisateurs distants via mon centre de données pour l'accès aux applis de Cloud public

37%

Je dois exposer publiquement mes applis privées dans le Cloud public pour fournir un accès

35%

Je suis incapable de déployer mon appliance de VPN distant favorite dans un environnement de Cloud public

Les motivations du Zero Trust

Qu'est-ce qui motive les entreprises à lancer ou à compléter leur système Zero Trust ? La sécurité des données arrive en tête de liste avec 82 %, suivie de la prévention des fuites de données (68 %) et de la réduction des menaces sur les terminaux (53 %).

Quelles sont, pour votre entreprise, les principales motivations pour le lancement/la poursuite d'un programme de gestion des accès/identités ou de Zero Trust ?[4]

82%

Sécurité/protection des données

68%

Prévention des fuites de données

53%

Limitation des menaces de sécurité sur les terminaux et les périphériques IoT

Limitation des menaces intérieures

Conformité avec les normes du secteur/ la réglementation (ex., HIPAA, GDRP, PCI DSS)

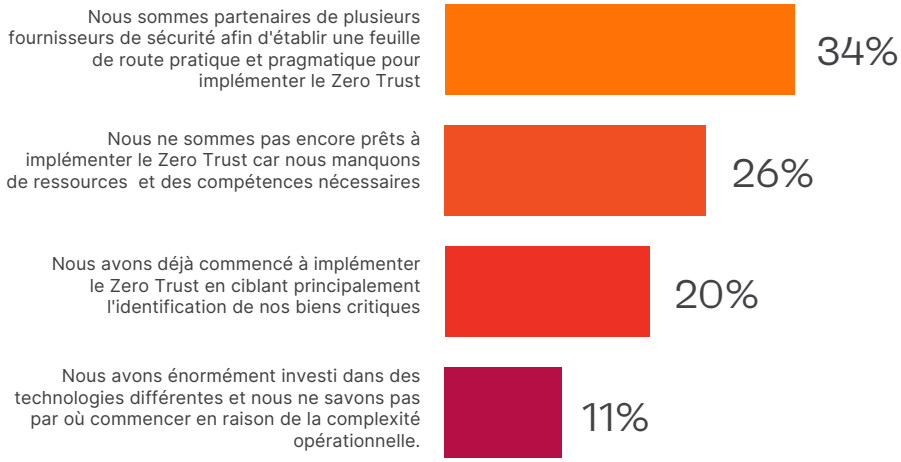
Répondre aux problèmes de sécurité de l'IT hybride

Efficacité opérationnelle

Implémentation du Zero Trust

Le Zero Trust s'accélère rapidement et les entreprises suivent différents parcours pour implémenter cette technologie. L'approche la plus souvent choisie par les entreprises est le partenariat avec plusieurs fournisseurs de sécurité afin d'établir une feuille de route pratique et pragmatique pour implémenter le Zero Trust (34 %). Cependant, le manque de ressources et des compétences nécessaires (26 %) reste un vrai frein au Zero Trust.

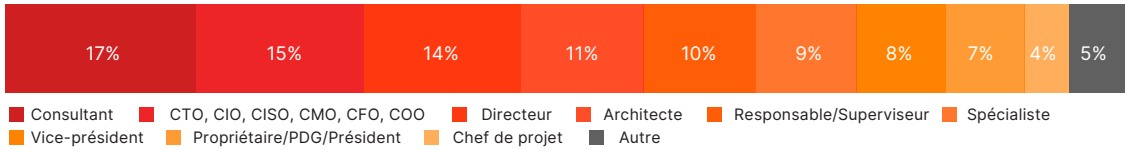
Si l'implémentation du Zero Trust est un processus progressif, comment prévoyez-vous d'implémenter le Zero Trust dans l'ensemble de votre environnement étendu ?[5]



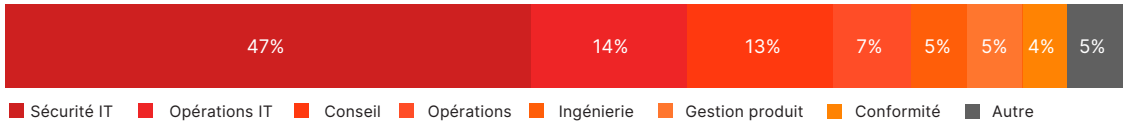
Méthodologie et personnes interrogées

Ce rapport repose sur les résultats d'une enquête en ligne complète portant sur 443 professionnels de l'IT et de la cybersécurité aux États-Unis, menée en juillet 2021 pour connaître les dernières tendances d'adoption, les difficultés, les manques et les solutions préférées des entreprises en matière de sécurité Zero Trust. Nous avons interrogé divers acteurs, des responsables techniques aux techniciens de sécurité IT, pour constituer un panel représentatif d'entreprises de toutes tailles dans plusieurs secteurs d'activité.

Postes

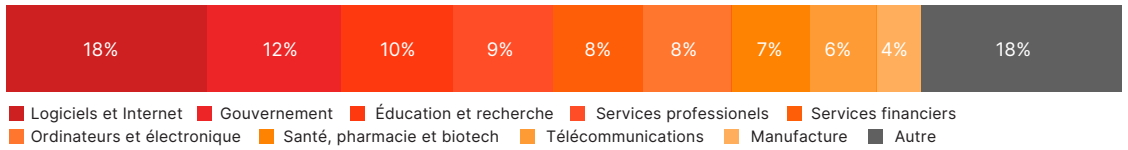


Département



Taille de l'entreprise

Secteur d'activité



ivanti

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr

Ivanti rend possible l'Everywhere Workplace. Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux données et applications IT sur différents réseaux, afin de rester productifs en travaillant de partout.

La plateforme d'automatisation Ivanti Neurons réunit les solutions Ivanti de gestion unifiée des terminaux (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin de créer une plateforme IT unifiée permettant l'autoréparation et l'autosécurisation des périphériques et le self-service aux utilisateurs. Plus de 40 000 clients, dont 78 des entreprises Fortune 100, ont choisi Ivanti pour découvrir, gérer, sécuriser et servir leurs biens IT, du Cloud à la périphérie, ainsi que pour fournir une expérience utilisateur final d'excellence aux collaborateurs, où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Pour en savoir plus, visitez le site ivanti.fr et suivez @GoIvanti.

1. Ségrégation des ressources 40 % | Autre 2 %
2. Complément à l'EDR (Détection et réaction aux menaces sur le poste client) 28 % | Renforcement de la sécurité SD-WAN 27 % | Amélioration de la correction des vulnérabilités (ex., gestion des vulnérabilités, gestion des correctifs) 5 % | Renforcer la protection contre les menaces mobiles (MDT/ antihameçonnage) 2 % | Aucun 2 % | Autre 4 %
3. Pare-feu d'application Web (WAF) 35 % | Gestion de la mobilité d'entreprise (MDM) 31 % | Broker de sécurité d'accès au Cloud (CASB) 30 % | Analyse des identités 27 % | Périmètre défini par logiciel (SDP) 26 % | Services d'annuaire d'entreprise 17 % | Contrôle complet de l'accès réseau Zero Trust 12 % | Gestion des vulnérabilités/des correctifs 9 % | Invisibilité des périphériques réseaux aux menaces 7 % | Antihameçonnage 7 % | Protection contre les menaces mobiles (MTD) 5 % | Autre 2 %
4. Conformité interne 28 % | Réaction aux audits ou incidents de sécurité 28 % | Autre 5 %
5. Autre 9 %