10 améliorations essentielles de la productivité

96 % des responsables de la sécurité déclarent que l'élaboration d'une stratégie Zero Trust est leur priorité absolue.[1] Découvrez comment la sécurité Zero Trust offre de la valeur aux organisations.

L'approche Zero Trust dynamise la productivité de l'ensemble de l'organisation

Pour les administrateurs informatiques et de sécurité

65 % des décideurs informatiques et des professionnels de la sécurité déclarent que la sécurité Zero Trust renforce la productivité des équipes de sécurité informatique [2]

↓80 % diminution du temps consacré à la résolution des tickets informatiques liés au télétravail avec l'accès Zero Trust par rapport à l'accès par VPN [3]

↑50 % augmentation moyenne de l'efficacité opérationnelle des équipes de sécurité dans cinq organisations déployant l'approche Zero Trust [4]

35 % probabilité accrue de déclarer des SecOps fiables pour les organisations disposant de déploiements Zero Trust/SASE matures [6]

↓29 % réduction de la complexité de la solution et du nombre de points d'intégration avec une plateforme Zero Trust par rapport à l'architecture existante [7]

Facteurs de productivité

- Des contrôles granulaires sans frais supplémentaires
- Simplification du déploiement initial, de la gestion continue des politiques et du déploiement d'utilisateurs et d'applications
- Réduction de la complexité par la consolidation des services ponctuels existants sur une plateforme cloud unique
- Réduction du temps consacré à la résolution des problèmes et des vulnérabilités des systèmes existants

Pour les utilisateurs finaux

53 % des décideurs informatiques et professionnels de la sécurité déclarent que la sécurité Zero Trust améliore l'expérience des utilisateurs [2]

↑60 % accélération de l'intégration des nouveaux employés grâce au provisionnement de l'accès Zero Trust par rapport à l'accès par VPN aux applications [3]

85 % des responsables informatiques affirment qu'une augmentation des revenus résulte d'une meilleure expérience des employés [5]

3 jours économies annuelles réalisées grâce au déploiement d'un accès BYOD et Zero Trust sécurisé aux ressources essentielles pour le personnel en première ligne [4]

65 % des employés estiment qu'ils seraient plus productifs s'ils disposaient de technologies plus performantes [8]

Facteurs de productivité

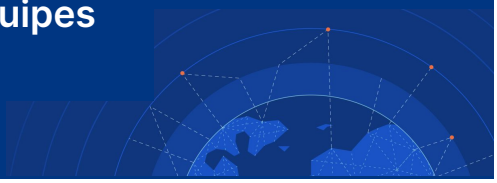
- Des contrôles de sécurité plus transparents et moins intrusifs
- Intégration/désactivation plus rapide des employés, sous-traitants, fournisseurs et tiers
- Flux de travail d'authentification simplifiés, sans réacheminement du trafic par des équipements sur site
- Réduction des temps d'inactivité dus à des problèmes liés à la connectivité, à l'accès ou aux politiques de sécurité

L'approche Zero Trust est un changement de mentalité stratégique pour votre organisation

Sécurité informatique traditionnelle : le périmètre détermine la confiance		Zero Trust : pas de périmètre, vérification systématique
Périmètre sécurisé, sécurité au sein du réseau (« le château et ses douves »)	Protection	Assumer le risque, réduire l'impact (chiffrer, inspecter, micro-segmenter)
Journaliser uniquement les connexions au périmètre	Visibilité	Journaliser chaque connexion et chaque requête, partout
Autorisation par défaut, accès statique en fonction de l'emplacement réseau	Contrôle	Refus par défaut, moindre privilège en fonction de l'identité et du contexte

Commencez à dynamiser la productivité de vos équipes avec l'approche Zero Trust

Demander un entretien



Vous n'êtes pas encore prêt pour votre entretien ?

- Découvrez comment l'approche Zero Trust réduit les risques et améliore l'efficacité des technologies : lisez le dossier
- Découvrez comment les organisations semblables à la vôtre gèrent le travail hybride : lisez le dossier
- Explorez une feuille de route agnostique vis-à-vis des fournisseurs pour déployer la sécurité Zero Trust : lisez le livre blanc

1. « Microsoft Zero Trust Adoption Report », juillet 2021 (Lien)
2. « Global Study on Zero Trust Security for the Cloud », Ponemon Institute LLC, juillet 2022 (Lien)
3. Études de cas Cloudflare (Lien)
4. « The Total Economic Impact ™ of Zero Trust Solutions from Microsoft »" Forrester Research, décembre 2021 (Lien)
5. Loomis, Amy and Webber, Alan, « Driving Bottom-Line Value by Linking Customer Experience to Employee Experience », IDC Research, janvier 2022 (Lien)
6. « Security Outcomes Study », Cisco, décembre 2021 (Lien)
7. « Realizing Cybersecurity Value », Palo Alto Networks, septembre 2022, (Lien)
8. « The need for improved digital employee experience: How technology enables better employee retention and productivity », Ivanti, 2022, (Lien)