Gigamon®

RÉSUMÉ

Le paysage de l'IT et de la sécurité pour 2020 et les années à venir, et le rôle du modèle Zero Trust

Note de synthèse

L'étude Gigamon sur l'architecture Zero Trust est née de l'idée que les perceptions du modèle Zero Trust évoluent et suscitent aujourd'hui un intérêt bien particulier. L'architecture Zero Trust a souvent eu une connotation négative en raison de son message « ne jamais faire confiance, toujours vérifier » qui entraverait la productivité des employés. Pour autant, l'étude vient en opposition à cette théorie puisque **87%** des personnes qui ont entamé leur transition vers un modèle Zero Trust déclarent que son adoption a amélioré leur productivité.

De plus, **84%** des décideurs soulignent que le climat économique actuel a considérablement modifié les pratiques de travail, créant de nouveaux défis et une augmentation des menaces de sécurité. Le modèle Zéro Trust est aujourd'hui considéré comme une approche stratégique pour aider les entreprises à faire face aux nouveaux défis post-pandémie.

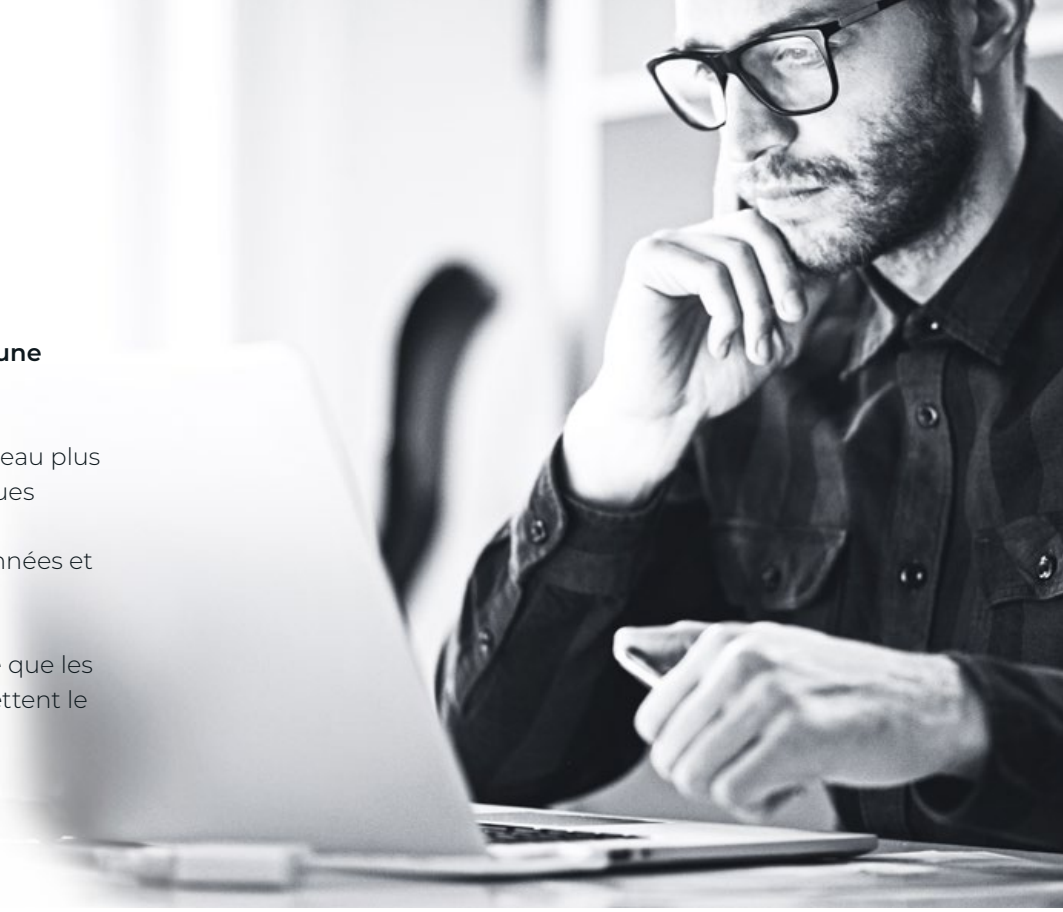
97% des personnes interrogées ayant entamé leur transition vers une architecture Zero Trust ont en effet déclaré que la mise en place de ce modèle a aidé ou pourrait aider leur entreprise à faire face à la situation mondiale actuelle.

L'enquête a rassemblé les réponses de **500 décideurs du secteur IT** et de la sécurité au Royaume-Uni, en France et en Allemagne, et a confirmé l'hypothèse selon laquelle l'architecture Zero Trust est un modèle résolument tourné vers l'avenir. De plus en plus d'entreprises s'y intéressent et commencent leur propre transition.

L'enquête révèle même que **89%** des personnes interrogées avaient/ont une connaissance du modèle Zero Trust.

Le modèle étant toujours plus adopté, ses avantages sont d'autant plus mis en avant par les entreprises. En effet, **76%** des décideurs ayant connaissance du modèle Zero Trust sont des adeptes ou potentiels adeptes du concept, positionnant ainsi cette architecture comme un réel différentiateur face à la concurrence.

Une architecture Zero Trust est principalement mise en place afin de renforcer la sécurité. En effet, **54%** des répondants déclarent avoir y avoir eu recours afin de sécuriser leur réseau et minimiser les risques. Le réseau



Principales raisons d'adopter une architecture Zero Trust

54% Pour rendre notre réseau plus sûr et réduire les risques

51% Pour protéger les données et faciliter leur gestion

49% Pour réduire le risque que les employés compromettent le système

étant en constante évolution, le modèle Zero Trust ne part pas du postulat qu'un utilisateur ou un appareil est sûr, sur la base d'informations d'identification préexistantes, mais examine plutôt le comportement des ressources et n'accorde l'accès au réseau et à ses ressources qu'en fonction de ces informations. La protection des données et la simplification de leur gestion sont les deuxièmes raisons les plus citées pour l'adoption de l'architecture Zero Trust (**51%**). Il est impossible de surveiller ce que l'on ne voit pas, c'est pourquoi les entreprises doivent avoir une vision claire de tout ce qui se passe sur leur réseau afin d'adopter un modèle Zero Trust. Ainsi, **59%** des répondants ont indiqué l'avoir adopté afin de réduire le risque de compromission du système par les employés.

Depuis quelques mois, les entreprises redoublent d'efforts pour adapter leurs pratiques et leurs processus et faire face à l'évolution sans précédent du paysage IT. Ce nouveau monde donne alors à l'architecture Zero Trust l'occasion de prouver sa juste valeur. Toutefois, les nouvelles formes d'organisations font naître de nouvelles menaces. Les cybercriminels cherchent en effet à tirer profit de la mise en place massive du télétravail et des nouveaux modes d'organisation du travail. Il est intéressant de noter que la culture d'entreprise et le comportement des employés ont été à la fois une motivation et un obstacle au lancement d'un programme Zero Trust.

Le Shadow IT ainsi que la formation des employés ont été citées comme les principaux défis à relever par les personnes interrogées. Les entreprises ont alors tout intérêt à envisager d'adopter le modèle Zero Trust afin de minimiser la menace interne. À l'inverse, **65%** des personnes interrogées qui ont décidé de ne pas adopter ce concept citent l'inadéquation avec la culture d'entreprise comme la principale raison de cette décision. L'adhésion des employés dans cette démarche a par ailleurs été citée comme la chose la plus importante à mettre en place avant de commencer la transition vers une architecture Zero Trust.

En cette période inédite, les entreprises doivent continuer à se transformer afin de préserver leur sécurité et rester compétitives. Avec l'architecture Zero Trust, les équipes InfoSec peuvent s'assurer que leur entreprise reste sécurisée sans compromettre la productivité ou l'expérience utilisateurs.

Pour en savoir plus, consultez le rapport d'enquête complet.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 www.gigamon.com

EMEA Headquarters
100 Brook Drive, Green Park, Reading, RG2 6UJ UK
+44 (0)118 304 0300 emea-info@gigamon.com

France
121 rue d'Aguesseau, 92100 Boulogne-Billancourt
+33 1 41 03 14 95 emea-info@gigamon.com

09.20_04