Résumé exécutif d'ESG

Rapport sur l'impact du modèle Zero Trust (vérification systématique) : Principaux résultats en France

Date : Juin 2022 **Auteur :** John Grady, analyste senior ; Adam DeMattia, directeur de recherche personnalisée

Avec des surfaces d'attaque grandissantes, l'intérêt pour le modèle Zero Trust augmente

L'hyperconnectivité, créée par la transformation numérique entre les utilisateurs, les applications, les données et les objets, agrandit massivement la surface d'attaque et accroît les risques. En cherchant à exploiter ces tendances, les agresseurs utilisent diverses méthodes pour compromettre les cibles, ce qui provoque souvent des perturbations importantes dans l'activité. Pour résoudre ces problèmes, beaucoup d'organisations ont commencé à mettre en œuvre des architectures Zero Trust, afin de moderniser leurs programmes de cybersécurité et limiter l'impact de ces attaques. Pour obtenir des informations plus approfondies sur la position des organisations vis-à-vis du modèle Zero Trust en général, et en particulier sur la manière dont la segmentation s'intègre dans leur stratégie, Illumio a demandé à Enterprise Strategy Group (ESG) de mener une enquête au niveau mondial, auprès de 1 000 organisations situées en Amérique du Nord, en Europe, en Asie-Pacifique et au Japon. Voici quelques-unes des principales réponses constatées parmi les répondants français :

- Seuls 30 % des répondants français estiment que leur organisation est prête à gérer une violation. Cela peut être dû à des expériences passées, 82 % signalant des impacts négatifs tels qu'une atteinte à la réputation de la marque ou à la valeur pour les actionnaires (36 %), une perte de données sensibles (33 %) ou des problèmes de conformité/juridiques (32 %) qui résultent d'une attaque.

- En ce qui concerne les ransomwares, plus de la moitié (54 %) des organisations françaises, qui ont vu des données et des systèmes pris en otage par une attaque de ransomware, ont été forcées de payer la rançon, soit directement, soit par l'intermédiaire d'un fournisseur de cyberassurance. La rançon moyenne versée en France s'élevait à plus de 370 000 €.

- Les organisations en France donnent la priorité au modèle Zero Trust ; 90 % des répondants indiquent qu'il s'agit d'une des trois plus hautes priorités en matière de cybersécurité et qu'ils allouent en moyenne 33 % de leur budget général de sécurité à des projets Zero Trust.

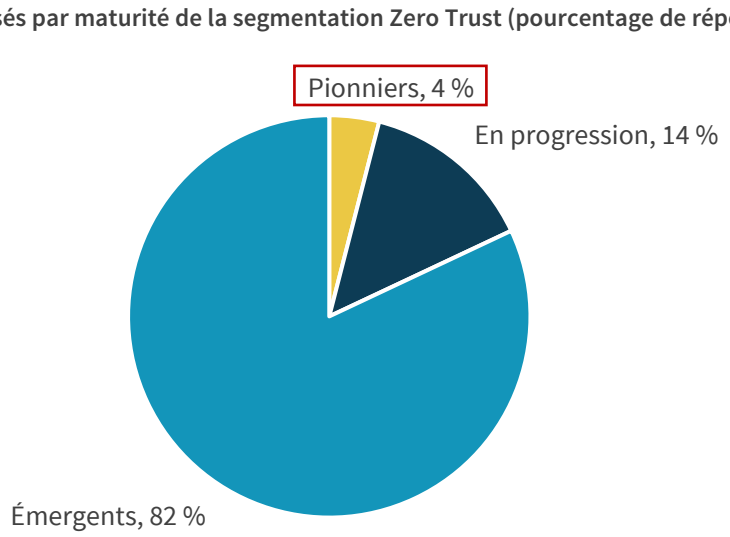
- En dépit de la prévalence du modèle Zero Trust et de la probabilité résiduelle de subir une attaque, 60 % des organisations françaises, dans leurs activités, ne font pas l'hypothèse qu'elles subiront des violations. Elles ont un retard important sur leurs homologues britanniques (46 %) et américains (39 %), ce qui souligne un écart flagrant entre ce que les organisations françaises disent qu'elles font et leur fonctionnement réel.

Maturité de la segmentation Zero Trust

Dans le cadre de l'étude, ESG a évalué la position des répondants en ce qui concerne leur progression vers la segmentation Zero Trust. La segmentation Zero Trust est une approche moderne visant à empêcher les violations de se propager dans l'informatique hybride, du centre de données jusqu'au cloud. Il s'agit notamment d'obtenir une visibilité complète sur tous les types d'applications, de sites et de points de terminaison ; de contenir rapidement et efficacement les attaques qui ont lieu ; de segmenter correctement les différentes parties de l'environnement (comme l'IT de l'OT et le développement de la production) ; et enfin d'étendre ces capacités à l'ensemble de l'environnement, afin de mettre à l'abri les ressources de haute priorité et appliquer la micro segmentation dans toutes les applications pour empêcher les mouvements latéraux dans l'environnement.

Les répondants à l'enquête ont été classés en trois catégories en fonction de leurs réponses à cinq questions clés évaluant leur technologie et leurs pratiques de segmentation en ce qui concerne : les intégrations avec les solutions SIEM et SOAR, la séparation environnementale, la capacité à contenir les infections, ainsi que la visibilité et la mise en application cohérentes dans l'environnement. Les membres du groupe Émergents ont démontré d'excellentes capacités dans 0 à 2 domaines, ceux du groupe En progression dans 3 à 4 domaines et ceux du groupe Pionniers dans les 5 domaines. Seulement 4 % des organisations françaises ont été placées dans la catégorie Pionniers, ce qui signifie que, même si bon nombre d'entre elles reconnaissent l'importance du modèle Zero Trust, il reste un long chemin à parcourir pour mettre en œuvre la segmentation, en vue d'assurer une mentalité « faire l'hypothèse d'une violation ». À titre de comparaison, 10 % des répondants allemands et 9 % des répondants américains ont été classés dans la catégorie Pionniers.

Figure 1. Maturité de la segmentation Zero Trust en France



Source : ESG, une division de TechTarget, Inc.

Pourquoi ces classifications sont-elles importantes ? Les organisations classées dans la catégorie Pionniers ont démontré des avantages significatifs en matière de sécurité et d'activité par rapport à leurs pairs. Parmi les répondants au niveau mondial, les Pionniers de la segmentation Zero Trust ont démontré :

- Une meilleure visibilité. Les Pionniers étaient 4,3 fois plus susceptibles d'avoir une visibilité complète sur le trafic dans leur environnement, et 5 fois plus susceptibles d'avoir une visibilité complète sur tous les types d'architectures d'applications.

- **Une réduction du coût annuel lié aux temps d'arrêt**. Les Pionniers étaient deux fois plus susceptibles d'éviter une panne sévère due à une attaque, et ils indiquaient un temps moyen de rétablissement (MTTR) plus court de 68 %. En évitant les pannes et en récupérant plus rapidement en cas d'attaque, ces organisations bénéficient d'une réduction de 20,1 millions de dollars sur le coût annuel lié aux temps d'arrêt.

- **Une transformation numérique plus rapide.** Au cours de l'année à venir, les Pionniers migreront 14 applications de production vers le cloud, ce qu'ils ne feraient pas autrement à cause d'un manque de confiance en matière de sécurité. Ceci leur permettra de libérer en moyenne 39 heures-personnes par semaine.

- **De la confiance dans la prévention des cyber-catastrophes.** Les Pionniers étaient plus de deux fois plus susceptibles de se sentir prêts à gérer des cyber-attaques, et ils ont déclaré prévenir cinq cyber-catastrophes chaque année.

Pour en savoir plus sur la réussite de la segmentation Zero Trust que constatent les Pionniers et sur ce qu'ils font pour atteindre ces résultats, consultez le rapport complet.

Enterprise Strategy Group est une société intégrée d'analyse, de recherche et de stratégie technologiques, qui fournit à la communauté informatique mondiale des renseignements sur le marché, des informations exploitables, ainsi que des services de commercialisation de contenu.

www.esg-global.com contact@esg-global.com +1 508 482 0188