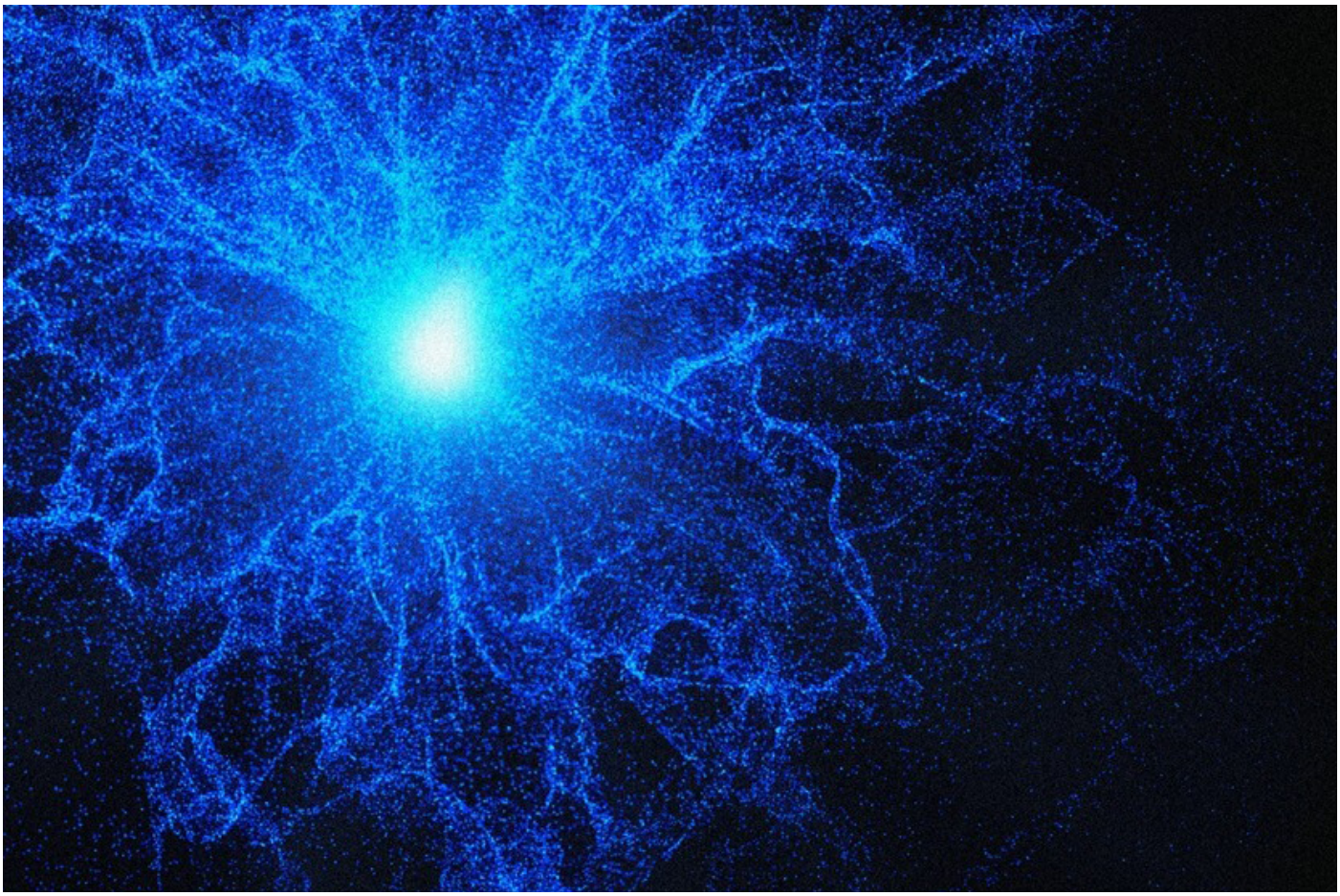
BlackBerry
Intelligent Security. Everywhere.

Livre blanc



L’imparable ascension du modèle Zero Trust :

Garantir la fiabilité des activités sans perturber le flux de travail des utilisateurs

Maîtriser la confiance

L'une des légendes qui entourent les origines du jeu d'échecs montre parfaitement pourquoi les solutions de cybersécurité modernes ne peuvent s'appuyer sur les modèles de confiance traditionnels. Selon cette histoire, l'inventeur des échecs a présenté un échiquier à son roi. Très impressionné, le souverain lui propose de choisir sa récompense, quelle qu'elle soit. « Un grain de riz », répond le créateur du jeu d'échecs. Il pose alors le grain de riz sur la première case de l'échiquier, et demande au roi de placer deux grains de riz sur la deuxième case et ainsi de suite, en doublant à chaque fois le nombre de grains, jusqu'à la 64e et dernière case.

Au début, la demande ne pose guère de problème, mais il apparaît rapidement qu'il est impossible de la satisfaire. Cette multiplication par deux du nombre de grains de riz case après case s'accompagne en effet d'une augmentation exponentielle qui se chiffre en milliards de milliards de grains de riz (264 – 1). Incapable d'honorer sa promesse, le roi aurait puni l'inventeur pour son insolence.

Le problème de l'échiquier et des grains de riz est similaire au dilemme que rencontrent de nombreuses entreprises souhaitant garantir la sécurité de leurs terminaux. Aux premiers temps de l'informatique, sécuriser le poste de travail d'un employé n'avait rien de sorcier. Mais lorsque plusieurs postes de travail se sont connectés à un réseau, voire à plusieurs réseaux connectés — puis à terme, à Internet —, la sécurisation de l'environnement devint nettement plus complexe. Aujourd'hui, avec l'essor de l'Internet des objets (IoT), il est pratiquement impossible de sécuriser toutes les technologies en contact avec les ressources mises en œuvre sur le lieu de travail.

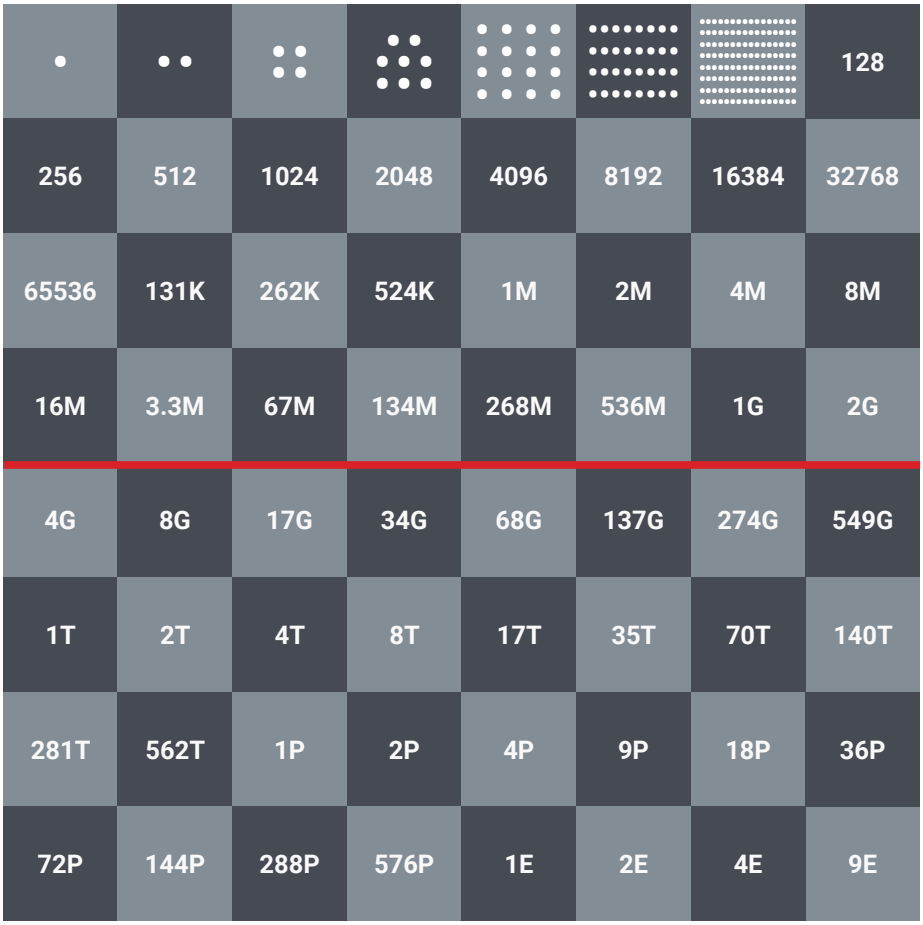


Figure 1. Un grain de riz multiplié par deux à chaque case atteint rapidement des proportions inimaginables.

« Le problème de l'échiquier et du riz est comparable au dilemme de la sécurité des terminaux auquel sont confrontées de nombreuses organisations aujourd'hui. »

Les vecteurs d'attaque augmentent à mesure que s'ajoutent des dispositifs

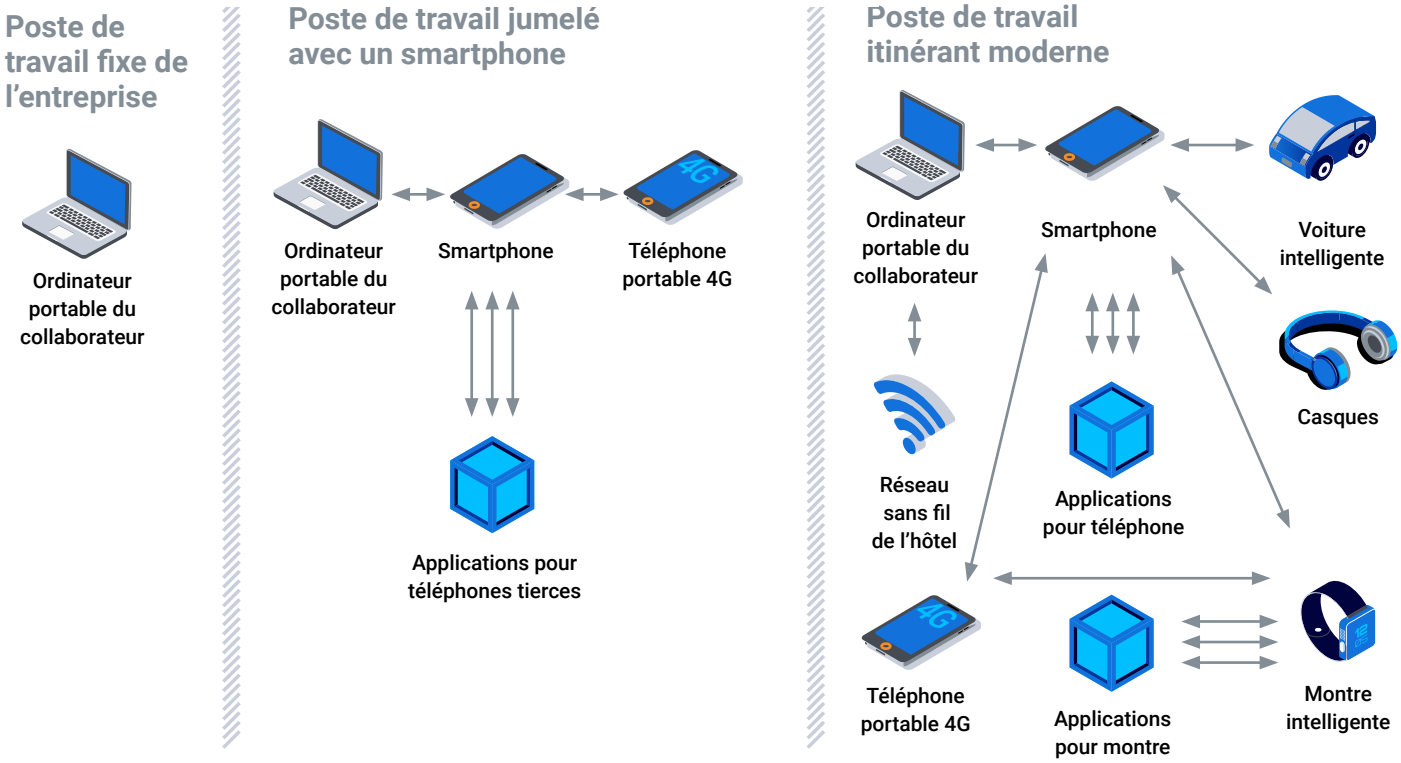


Figure 2. Les vecteurs d'attaque (représentés par des flèches grises) augmentent avec chaque appareil, application et connexion réseau supplémentaire.

Prenons l'exemple d'un employé qui possède un unique ordinateur portable fourni par son entreprise. Il n'est guère compliqué de le sécuriser, mais il se trouve que cet employé accède également aux ressources de l'entreprise à l'aide de son smartphone. Quel est le niveau de sécurité des différentes applications installées sur le smartphone ? Personne ne le sait. Il arrive également que notre employé écoute de la musique sur son smartphone à l'aide d'un casque Bluetooth avancé (connecté à l'IoT) de marque inconnue.

Tous ces appareils sont couplés à un véhicule qui stocke de la musique, des listes de contacts et d'autres informations sur son propre système interne. Lorsque l'employé se déplace, il connecte son ordinateur portable et son smartphone à différents réseaux publics pour consulter ses e-mails et travailler à ses projets.

Dans quelle mesure les ressources professionnelles sont-elles sécurisées ? La surface d'attaque correspondant aux ressources de l'entreprise augmente avec chaque application, chaque appareil et chaque connexion réseau supplémentaire. Ce dilemme démontre clairement que les entreprises doivent adopter une approche de sécurité conforme au modèle Zero Trust marqué, comme son nom l'indique, par l'absence de toute confiance.

Faire confiance à des entités par défaut ou sur la base d'une confirmation ponctuelle ne constitue en aucun cas une stratégie de sécurité viable. Pour limiter les risques, la meilleure approche consiste à ne jamais faire confiance à qui ou quoi que ce soit par défaut, mais à établir et maintenir la confiance avec les acteurs (utilisateurs et ressources) sur la base d'engagements durables.

Cybersécurité : un problème compliqué ou complexe ?

Pour créer ou mettre en œuvre des solutions de cybersécurité efficaces, il importe de bien comprendre la nature du problème de confiance que soulève l'utilisation d'appareils connectés à l'Internet des objets et l'interconnectivité de masse. Aujourd'hui, la création d'environnements de travail sécurisés ne constitue pas un problème compliqué, mais un problème complexe1 !

En résumé, les problèmes compliqués impliquent plusieurs éléments qui interagissent de manière prévisible. Il est possible de prédire le résultat d'un système compliqué si l'on en connait les intrants. Par exemple, la construction d'un sous-marin est une entreprise compliquée. Un sous-marin embarque en effet de nombreux systèmes interconnectés qui doivent opérer d'une manière particulière pour que le submersible fonctionne. Dans la mesure où chaque système connecté se comporte de manière finalement prévisible, les ingénieurs peuvent créer un sous-marin très compliqué à condition de disposer de suffisamment de temps et de moyens.

Certes, les problèmes complexes comportent eux aussi de nombreux systèmes interconnectés, mais leurs interactions sont imprévisibles. Même en connaissant les intrants, les extrants ne peuvent, au mieux, qu'être devinés. Par exemple, des systèmes tels que les marchés financiers ou le climat mondial sont des problèmes on ne peut plus complexes. Dans le cas de systèmes complexes, il est parfois possible de comprendre différentes pièces d'un vaste puzzle, mais sans pouvoir prédire avec fiabilité ce qui en sortira.

Par le passé, lorsque les postes de travail étaient isolés des environnements métier, la cybersécurité représentait peut-être un problème compliqué. Aujourd'hui, avec l'essor des appareils connectés à l'Internet des objets, la rapidité de l'innovation technologique et le volume considérable de nouveaux codes logiciels, la cybersécurité représente un problème effectivement complexe — en d'autres termes, un problème qui dépasse la capacité de prédiction des êtres humains.

En revanche, la technologie est capable d'effectuer des calculs et des opérations avec une rapidité et une efficacité que nous ne sommes pas en mesure d'égaler. En ayant recours à la modélisation prédictive, à l'intelligence artificielle (IA), à l'apprentissage automatique et à l'authentification continue, les analystes disposent de moyens efficaces pour s'attaquer aux problèmes de sécurité les plus complexes.

Qu'est-ce que le Zero Trust ?

Comme son nom anglais l'indique, le modèle de sécurité Zero Trust repose sur le principe selon lequel il ne faut faire confiance à rien ni personne, à l'intérieur comme à l'extérieur d'une entreprise. Cette architecture a vu le jour dans le cadre du Jericho Forum, un think tank actif au début des années 2000, où des spécialistes de la sécurité discutaient du cloud computing et de la notion de « dépérimétrisation[1]. L'expression « Zero Trust » a été inventée en 2010 par John Kindervag, analyste chez Forrester Research Inc[2].

> « Avec des systèmes complexes, nous sommes peut-être capables de comprendre les pièces du grand puzzle, mais nous restons incapables de prédire de manière fiable des résultats concluants. »

Le rôle de l'IA dans le Zero Trust

L'un des avantages de l'IA est sa capacité à traiter et à trouver rapidement des corrélations dans d'énormes ensembles de données. C'est précisément cette capacité qui lui permet de prédire avec précision l'identité des utilisateurs, la sécurité des fichiers et la légitimité des activités. Voici quelques utilisations possibles de l'IA pour la mise en œuvre d'un environnement Zero Trust :

- **Analyse comportementale des utilisateurs et des entités :** L'IA peut surveiller l'activité, la position géographique et les données biométriques de l'utilisateur et les comparer à des modèles normaux pour déterminer si un acteur est digne de confiance. L'accès au compte peut être automatiquement modifié pour refléter les changements de confiance et les étapes de ré-authentification lancées lorsque les scores de confiance deviennent trop faibles.
- **Prévention contre les logiciels malveillants :** L'IA peut être programmée pour identifier des logiciels malveillants inconnus ou de type zero-day grâce à une simulation sur des millions ou des milliards de fichiers sûrs ou malveillants. Une IA hautement perfectionnée peut réussir à détecter les logiciels malveillants connus et précédemment inconnus en analysant les caractéristiques d'un fichier avant son exécution. Cette capacité donne aux agents de sécurité pilotés par IA un avantage prédictif sur les menaces et peut facilement remplacer les modèles traditionnels de sécurité des fichiers basés sur la confiance.
- **Traque des menaces :** Des modèles mathématiques peuvent être déployés directement sur les terminaux pour surveiller leur activité et signaler les comportements anormaux. Les fonctionnalités intégrées de détection des menaces permettent aux terminaux de signaler rapidement toute activité suspecte, de lancer des mesures correctives automatisées et de s'isoler des autres ressources pendant une attaque.

Le modèle Zero Trust bénéficie grandement de la capacité de l'IA à faire des prédictions basées sur l'agrégation et l'analyse des données. Cela permet aux organisations de s'éloigner des stratégies d'authentification à un ou deux facteurs qui ont longtemps été examinées et exploitées par les acteurs de la menace. La confiance, lorsqu'elle est vérifiée par l'IA, devient un processus continu d'engagements sûrs et attendus plutôt qu'une présentation ponctuelle d'informations d'identification.

« Le modèle Zero Trust bénéficie grandement de la capacité de l'IA à faire des prédictions basées sur l'agrégation et l'analyse des données. »

Le facteur humain dans le Zero Trust

Les spécialistes de la sécurité disposent de plusieurs outils pour mettre en œuvre un cadre Zero Trust. L'IA se chargeant principalement de la détection et de la réponse, les analystes peuvent se concentrer sur d'autres tâches, comme s'assurer que l'accès aux ressources de l'organisation est sécurisé. Face à la mobilité croissante de leur personnel, les entreprises doivent trouver de nouveaux moyens sûrs de fournir des services de travail à distance. Savoir sécuriser et surveiller une grande variété de technologies mobiles est un élément essentiel des solutions modernes de cybersécurité.

Les entreprises doivent tenir compte des facteurs suivants lors du choix des outils destinés à leur personnel de sécurité interne :

- Les collaborateurs peuvent-ils accéder à distance aux ressources de travail de manière fiable et sûre ?
- Les ressources de travail sont-elles accessibles en toute sécurité depuis n'importe quel appareil ?
- Une solution prend-elle en compte plusieurs modèles et plateformes de propriété, notamment Windows®, iOS®, Android™, macOS® et Linux® ?
- La solution est-elle évolutive et peut-elle facilement s'adapter aux nouvelles technologies ?
- Les ressources de travail sont-elles disponibles en ligne et hors ligne, et accessibles sans VPN ?
- Une solution offre-t-elle une interface unique pour effectuer les tâches de sécurité, ou les analystes seront-ils obligés de porter leur attention sur plusieurs interfaces ?
- Les analystes sécurité peuvent-ils s'assurer que les collaborateurs utilisent des applications fiables sur un terminal mobile sécurisé ?

Pour cultiver un environnement Zero Trust viable, les organisations doivent également s'adapter au rythme de l'innovation technologique et à l'évolution des pratiques commerciales. Le travail se fait de plus en plus souvent en dehors du bureau physique et sur des appareils personnels. Autrement dit, l'environnement Zero Trust ne peut pas se limiter aux périmètres des réseaux traditionnels. Il doit englober l'accès aux données des entreprises à partir de tout appareil, en tout lieu.

Parvenir à une approche Zero Touch dans un environnement Zero Trust

Une préoccupation majeure des organisations qui envisagent un modèle Zero Trust est l'impact d'une telle structure sur leurs utilisateurs. Les collaborateurs vont chercher à contourner les processus de vérification intrusifs ou perturbateurs et peuvent introduire de nouvelles vulnérabilités dans leurs tentatives de créer des raccourcis. Cela signifie que la création d'une expérience minimalement intrusive, ou Zero Touch, pour les utilisateurs est un élément clé d'une structure Zero Trust robuste.

L'utilisation de solutions pilotées par IA pour procéder à une authentification continue est un moyen viable de profiter du meilleur des deux mondes. L'analyse en temps réel des données contextuelles sur les utilisateurs, les terminaux et les emplacements peut garantir la fiabilité des activités sans interrompre le flux de travail. Les utilisateurs sont invités à revérifier leur identité uniquement lorsqu'ils effectuent des transactions particulièrement risquées ou se comportent de manière anormale. La grande majorité des tâches quotidiennes sont des opérations à faible risque, et ne déclencheront jamais une demande de ré-authentification.

« L'analyse en temps réel des données contextuelles sur les utilisateurs, les terminaux et les emplacements peut garantir la fiabilité des activités sans interrompre le flux de travail. »

Pourquoi opter pour le modèle Zero Trust ?

Quels sont les avantages pour une organisation à adopter un modèle de sécurité Zero Trust ? Pour comprendre les nombreux avantages de ce modèle, considérez ce qui suit :

- En quoi votre environnement gagnerait-il à ne traiter qu'avec des utilisateurs identifiés de manière positive et authentifiés en continu ?
  - Quels programmes, règles ou pratiques ne seraient plus nécessaires ?
  - Quelles nouvelles possibilités pourraient être exploitées dès lors que votre organisation a acquis une confiance totale dans l'identité des utilisateurs ?
- Quels changements pourraient survenir dans votre organisation si chaque terminal était vérifié comme étant digne de confiance tout au long de chaque engagement ?
  - Dans quelle mesure votre choix technologique changerait-il ?
  - De quelle manière la productivité des collaborateurs changerait-elle ?
- En quoi la posture de sécurité de votre organisation serait-elle améliorée si les droits d'accès pouvaient être modifiés en temps quasi réel pour refléter le niveau de confiance actuel des utilisateurs et des terminaux ?
  - Le ratio des collaborateurs travaillant sur site et à distance changerait-il ?
  - Le personnel chargé de la sécurité informatique pourrait-il être utilisé de manière nouvelle et efficace ?

Les organisations peuvent retirer de nombreux avantages surprenants du modèle Zero Trust, qui ne sont pas toujours visibles. Par exemple, en 2020, les attaques par phishing étaient à l'origine de plus de 80 % des incidents de sécurité signalés. Zero Trust limite le montant des dommages qu'un utilisateur compromis peut infliger en limitant son accès et en exigeant une nouvelle authentification en cas de comportements inattendus.

De même, avec Zero Trust, il est difficile pour les menaces de se propager dans l'environnement sans être détectées, car elles exploitent les ressources et modifient l'accès de manière très suspecte. Les vulnérabilités courantes comme la non-application des correctifs logiciels et des mises à jour système sont moins désastreuses sous l'examen continu et la posture restrictive du modèle Zero Trust.

Conclusion

Zero Trust est l'approche rationnelle à adopter dans les interactions avec les technologies et les systèmes modernes. La sécurisation de l'environnement des entreprises par des techniques traditionnelles devient intenable quand les terminaux présents sur le lieu de travail sont en interface avec un IoT tentaculaire. Les organisations doivent comprendre qu'elles ne peuvent pas contrôler chaque application, terminal et réseau extérieur rencontré par leurs collaborateurs.

Cependant, l'interaction avec des entités connues, fiables et authentifiées en continu est une solution viable aux problèmes de sécurité engendrés par les progrès technologiques. De même, l'IA peut considérablement renforcer les équipes de sécurité en effectuant des analyses par force brute et des mesures correctives à des vitesses et des volumes dépassant les capacités humaines.

La suite BlackBerry Spark® réunit les outils de sécurité, de gestion et de productivité pour répondre à vos objectifs Zero Trust avec une approche Zero Touch pour vos collaborateurs et sous-traitants.

Pour toute information complémentaire, veuillez visiter le site http://www.blackberry.com/sparksuite.

1 https://thearmyleader.co.uk/team-of-teams/

2 https://blog.banyansecurity.io/blog/the-evolution-of-zero-trust

3 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

4 https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear—to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

© Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry is not responsible for any third-party products or services.

MKTG20-0334 | 201014