Lookout®

LIVRE BLANC

Comment sécuriser les données dans un monde extra-périmétrique

QU'EST-CE QU'UN MONDE EXTRA-PÉRIMÉTRIQUE ?

Dans un monde où le cloud et le mobile prédominent de plus en plus, les entreprises doivent tenir compte de 3 grandes réalités pour protéger leurs ressources contre toute fuite de données et attaque informatique :

1. Le périmètre a disparu.
2. Les technologies de sécurité existantes sont insuffisantes.
3. Aucun appareil n'est digne de confiance.

Étant donné que les employés continuent d'utiliser indifféremment des appareils gérés et non gérés pour accéder aux ressources de leur entreprise, l'installation d'une nouvelle architecture de sécurité s'impose :
la sécurité extra-périmétrique.

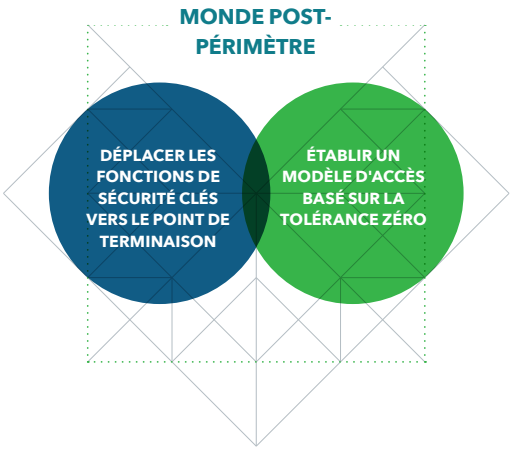
PROBLÈME : le périmètre a disparu

Les méthodes de travail ont considérablement changé. Les données stratégiques sont désormais disponibles sur le Cloud et les employés peuvent y accéder depuis n'importe quel réseau et où qu'ils se trouvent dans le monde. Par exemple, les employés se connectent très rarement à un VPN pour consulter leurs e-mails professionnels ou pour afficher/télécharger des documents sensibles lors de leurs déplacements.

Les attaques, telles que le phishing, ont également évolué et profitent désormais du fait que les protections périmétriques actuelles n'offrent plus de visibilité sur le trafic des utilisateurs. De même, les appareils appartenant à l'entreprise sont désormais utilisés à des fins personnelles. C'est la raison pour laquelle, les applications de réseaux sociaux et de messagerie créent un environnement dans lequel les employés peuvent être la cible de tentatives de phishing et de vol d'identifiants professionnels.

La mobilité et l'accès direct à des données sont un véritable atout pour la productivité des entreprises, au plus grand désarroi des équipes chargées de la sécurité, qui ne jurent que par les dispositifs existants au sein du périmètre de leur entreprise, tels que les pare-feux et les passerelles Web sécurisées.

En réalité, les données des entreprises sont stockées ailleurs. Elles sont devenues mobiles et accessibles partout. Cette révolution de l'écosystème a fait apparaître deux nouveaux besoins en matière de sécurité :



Déplacer les fonctions de sécurité clés vers les terminaux.

Tout d'abord, au lieu de cacher les points de terminaison derrière le système de sécurité classique d'un périmètre ou d'utiliser un VPN pour capter le trafic à l'intérieur du périmètre, la sécurité même doit être déplacée vers le terminal. La sécurité doit suivre les données, où qu'elles se trouvent, tout en préservant la vie privée des utilisateurs finaux.

Établir un modèle d'accès basé sur la tolérance zéro

Même lorsque le point de terminaison est protégé, la présomption d'innocence est un principe qui ne doit en aucun cas s'appliquer à un appareil. Ce nouveau monde implique que la santé des appareils soit constamment contrôlée pour pouvoir accéder aux données d'une entreprise, toujours en préservant la vie privée des utilisateurs finaux.

LA NOUVELLE ARCHITECTURE EST NÉCÉSSAIRE :

En pratique, les entreprises ont besoin d'un nouveau modèle d'architecture de sécurité appelé « sécurité extra-périmétrique ».[1] À la base, elle se compose de trois pièces de puzzle différentes, mais assemblées les unes aux autres :

- Protection du terminal
- Accès au Cloud
- Gestion des identités et des accès

L'architecture de la sécurité extra-périmétrique repose sur l'évaluation des risques d'un appareil à l'aide d'une solution de protection des points de terminaison. Cette protection permet d'identifier de manière constante les menaces et les risques pesant sur un appareil. La solution détermine alors si l'appareil d'un employé est suffisamment sain pour l'autoriser à s'authentifier et à accéder aux ressources de l'entreprise. Grâce à cette protection, une entreprise peut alors appliquer en temps réel des politiques en fonction de sa tolérance face à des risques spécifiques.

Cette architecture repose également sur la protection de l'accès au Cloud d'entreprise, et à Internet dans son ensemble, sans avoir recours aux dispositifs de défense mis en place au sein d'un périmètre. Et pour que cela soit possible, certaines de ces fonctions de sécurité critiques doivent être déplacées vers le terminal, telles que la surveillance des liens et sites Web malveillants et, par conséquent, la protection des employés en empêchant tout accès à des contenus dangereux.

Ces deux aspects vont de pair avec une solution d'identification, telle qu'un fournisseur SSO (Single Sign-on), pour autoriser un employé à s'authentifier et à accéder aux ressources de son entreprise ou, au contraire, lui refuser le droit de s'authentifier. Une fois l'employé authentifié, le risque associé au terminal sera évalué en permanence et son accès révoqué dès qu'un nouveau risque sera détecté. Dans certains scénarios, l'accès peut être géré via une solution EMM (Enterprise Mobility Management. Par ex., pour les appareils gérés) ou via une solution MAM (Mobile Application Management. Par ex. pour les applications gérées).

POURQUOI SE DIRIGER VERS UNE SÉCURITÉ EXTRA-PÉRIMÉTRIQUE

Les données d'entreprise sont de plus en plus hébergées sur le Cloud et les utilisateurs y accèdent de plus en plus par des points de terminaison connectés à des réseaux qui échappent au contrôle des services informatiques, comme les réseaux cellulaires mobiles et les réseaux Wi-Fi publics. Les données ne circulent plus d'un serveur à terminal au sein des réseaux gérés par les entreprises. Au contraire, une grande partie des données d'entreprise ne passe même plus par l'entreprise physique. Les données d'entreprise doivent désormais pouvoir circuler sur tout type de réseau et être accessibles à partir de n'importe quel appareil.

> **« Gartner prévoit que 80 % des employés travailleront sur un appareil mobile d'ici 2020. »**
>
> - Gartner, « Prepare for Unified Endpoint Management to Displace MDM and CMT », juin 2018

L'essor des outils de productivité basés sur le Cloud

Aujourd'hui, de nombreuses applications de productivité sont fournies par le biais du modèle SaaS (Software as a Service, logiciel en tant que service), associé à une solution de gestion des identités et des accès. Les licences des applications SaaS ne sont plus attribuées à un appareil unique mais à l'identité d'un utilisateur. Cela permet aux utilisateurs d'accéder à ces applications sur n'importe quel appareil, qu'il s'agisse d'un ordinateur portable ou d'un appareil mobile, sans contrainte de lieu ni de temps. Le revers de la médaille, c'est que les entreprises ne peuvent plus se contenter des stratégies de sécurité traditionnelles pour contrôler les accès et le trafic des données d'entreprise.

LA NÉCESSITÉ DES SOLUTIONS DE GESTION ET DE CONTRÔLE AVANCÉES

Dans un monde sans périmètre, les employés sont plus libres de choisir les outils qu'ils utilisent dans leur travail et tendent à délaisser les applications et services professionnels mis en place par leur service informatique au profit d'outils grand public offrant une meilleure expérience utilisateur et favorisant la productivité. Il s'agit alors pour les services informatiques de garantir un accès sécurisé aux données d'entreprise sans gêner l'utilisateur. Le problème est d'autant plus complexe avec l'essor du phénomène BYOD (Bring Your Own Device) puisqu'il empêche bien souvent d'imposer le contrôle des appareils eux-mêmes. En plus de gérer les appareils et les applications lorsque cela est possible (par exemple à l'aide d'une solution de gestion des appareils mobiles et d'une solution de gestion des applications mobiles), il est maintenant indispensable de protéger l'accès aux données d'entreprise grâce à des outils de contrôle de l'identité et des applications SaaS.

La sécurité extra-périmétrique s'appuie sur les stratégies existantes

À l'heure où les technologies mobiles et Cloud sont omniprésentes, il n'est plus question d'autoriser automatiquement l'accès aux données lorsqu'un utilisateur ou un terminal se connecte à un réseau d'entreprise. C'est cette problématique qui a conduit l'analyste Jon Kindervag de Forrester Research à élaborer le cadre de sécurité Zero Trust en 2009[2]. Partant du principe qu'aucun terminal se connectant aux données de l'entreprise n'est fiable, l'approche Zero Trust se concentre sur l'inspection et l'enregistrement de tout le trafic pour vérifier les actions des utilisateurs.

En 2011, Google a créé BeyondCorp, un nouveau modèle de sécurité d'entreprise[3]. Au départ, BeyondCorp était un projet interne de Google qui visait à permettre chaque employé de travailler à partir de réseaux non fiables sans passer par un VPN. Les conditions d'accès sont organisées par niveaux de confiance correspondant à des niveaux de sensibilité croissants. Avec BeyondCorp, les appareils mobiles sont traités comme des plateformes de qualité qui doivent bénéficier des mêmes niveaux d'accès et fonctionnalités.

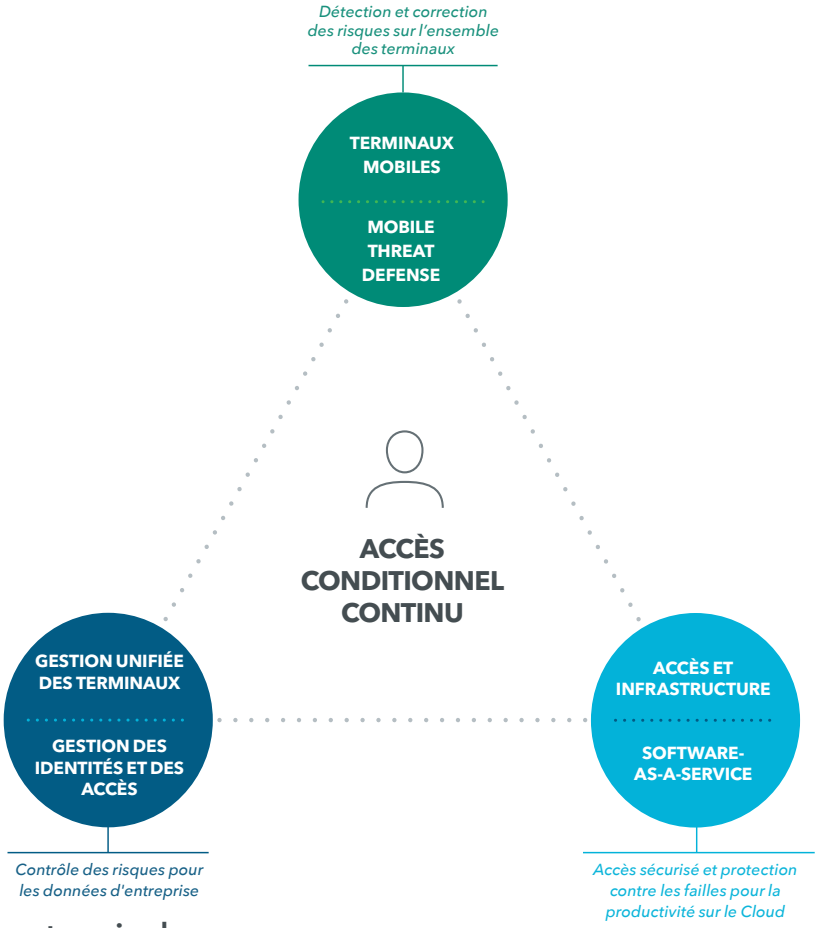
En 2017, le modèle CARTA (Continuous Adaptive Risk and Trust Assessment) de Gartner s'est étendu à Zero Trust et BeyondCorp. Selon Gartner, les vérifications de sécurité initiales (par exemple au moment de la connexion) autorisant ou bloquant l'accès sont insuffisantes et exposent les entreprises à des menaces zero-day, à des attaques ciblées, à des vols d'identifiants et à des menaces internes[4]. Le modèle CARTA repose sur une vision dynamique et non statique de la confiance et du risque associés aux entités commerciales numériques et à leurs actions. Cela signifie que les interactions doivent être évaluées en permanence, à mesure que le contexte se développe.

C'est en s'appuyant sur ces principes fondamentaux de la sécurité extra-périmétrique moderne, dans un monde orienté Cloud et mobile, que l'on peut construire une architecture permettant aux entreprises d'établir un accès conditionnel continu aux ressources de l'entreprise en fonction du risque dynamique associé aux terminaux non fiables et de garantir des protections essentielles pour les utilisateurs, qui constituent bien souvent le point d'entrée des cyberattaques..

COMMENT FAIRE DE LA SÉCURITÉ EXTRA-PÉRIMÉTRIQUE UNE RÉALITÉ

Avec la multiplication des applications, des appareils et des réseaux se trouvant hors du périmètre qu'offrent les outils de sécurité, de nombreuses sociétés informatiques cherchent à adopter les modèles Zero Trust, BeyondCorp et CARTA. Pour la plupart, il s'agit d'étendre et d'intégrer les services existants.

Les indispensables de la sécurité extra-périmétrique



Protection de chaque terminal

Le rôle de la protection du terminal est d'évaluer en permanence le risque associé aux actions et aux appareils de l'utilisateur, auxquels cette nouvelle architecture ne fait jamais confiance. Elle doit couvrir les appareils à la fois fixes et mobiles que les utilisateurs utilisent indifféremment pour accéder aux applications d'entreprise. En outre, la protection des terminaux doit intégrer des arbitres d'accès tels que les solutions de gestion des identités et des accès et/ou les applications Cloud elles-mêmes afin d'appliquer des actions correctives en cas de risque trop important. Dans certains scénarios, des actions correctives peuvent être menées grâce aux intégrations de la gestion de la mobilité de l'entreprise.

Sécurité et productivité sur le Cloud

Comme nous recourons de plus en plus aux services et à l'infrastructure Cloud, nous devons impérativement sécuriser l'accès aux applications et aux données hébergées. Les solutions de sécurité pour le Cloud assurent un accès sécurisé et une protection contre les failles pour les données et services hébergés, mais les fournisseurs de services Cloud doivent également intégrer la gestion des identités et des accès et la protection des terminaux afin de faire face aux risques potentiels associés aux demandes d'accès. Pour protéger les utilisateurs contre les sites malveillants qui se font passer pour des sites d'entreprise, il est nécessaire de protéger le terminal lui-même.

Gestion des identités et des accès

L'identité est considérée comme le « nouveau périmètre » qui détermine l'accès aux données de l'entreprise. Les plateformes de gestion de l'identité simplifient l'accès grâce à des fonctionnalités, telles que l'authentification unique, qui permettent aux utilisateurs de naviguer facilement entre différents services et applications. Si les fournisseurs de solutions de gestion des identités et des accès proposent des fonctionnalités de sécurité majeures, comme l'authentification multifacteur, pour protéger l'accès aux données sur le Cloud et sur site, ils doivent aussi intégrer la protection du point de terminaison afin d'évaluer en permanence le risque associé aux appareils non fiables. En combinant la gestion des identités et la protection du terminal, les organisations sont en mesure de vérifier en continu le niveau de confiance des utilisateurs et des appareils.

POST-PERIMETER SECURITY ALLIANCE

La Post-Perimeter Security Alliance rassemble des entreprises leaders dont l'objectif commun est de garantir la sécurité et d'améliorer la productivité dans un monde moderne, sans périmètre, et axé sur le cloud et la confidentialité. Aujourd'hui, il est difficile d'assurer une sécurité extra-pérmétrique complète par le biais d'un fournisseur unique. Grâce à ses fonctionnalités de sécurité intégrées au niveau du terminal, du Cloud et de l'identité, cette alliance protège l'accès aux données d'entreprise tout en favorisant la productivité. Les solutions offertes par la Post-Perimeter Security Alliance évaluent en permanence les risques pour les données d'entreprise et peuvent mener les actions correctives nécessaires.

Les membres de la Post-Perimeter Security Alliance étant des leaders dans les domaines de la protection des terminaux, de la gestion des identités et des accès, de la gestion de la mobilité d'entreprise et des outils de productivité sur le Cloud, il est probable qu'une organisation ait d'ores et déjà recours à un ou plusieurs de ces fournisseurs. Ainisi, de nombreuses entreprises se dirigent déjà consciemment ou non vers une stratégie de sécurité extra-périmétrique.

Découvrez comment faire de la sécurité extra-périmétrique une réalité pour votre entreprise ici.

> **« Une initiative intersectorielle telle que la Post-perimeter Security Alliance est tout à fait logique à l'heure actuelle, dans la mesure où elle peut aider les entreprises qui souhaitent mettre en place une architecture extra-périmétrique sans vraiment savoir comment s'y prendre. »**
>
> – Phil Hochmuth, Directeur du programme, Mobilité d'entreprise chez IDC

[1] Instaurer la confiance dans un environnement Zero Trust : la sécurité extra-périmétrique amorce une nouvelle ère dans le monde de l'informatique (1er novembre 2018)
Source : https://www.lookout.com/info/lookout-post-perimeter-lp

[2] Getting Started with Zero Trust: Never trust, always verify
Source : https://drive.google.com/file/d/1y_bexOdulUAr8M9wZxTqAGv21T3Vchor/view?ts=5c361c31

[3] Barclay Osborn, Justin McWilliams, Betsy Beyer, et Max Saltonstall. (2016, Printemps) BeyondCorp, Design to Deployment at Google
Source : https://storage.googleapis.com/pub-tools-public-publication-data/pdf/44860.pdf

[4] Gartner Seven Imperatives to Adopt a CARTA Strategic Approach (10 avril 2018)
Source (abonnement requis) : https://www.gartner.com/doc/3871363/seven-imperatives-adopt-carta-strategic