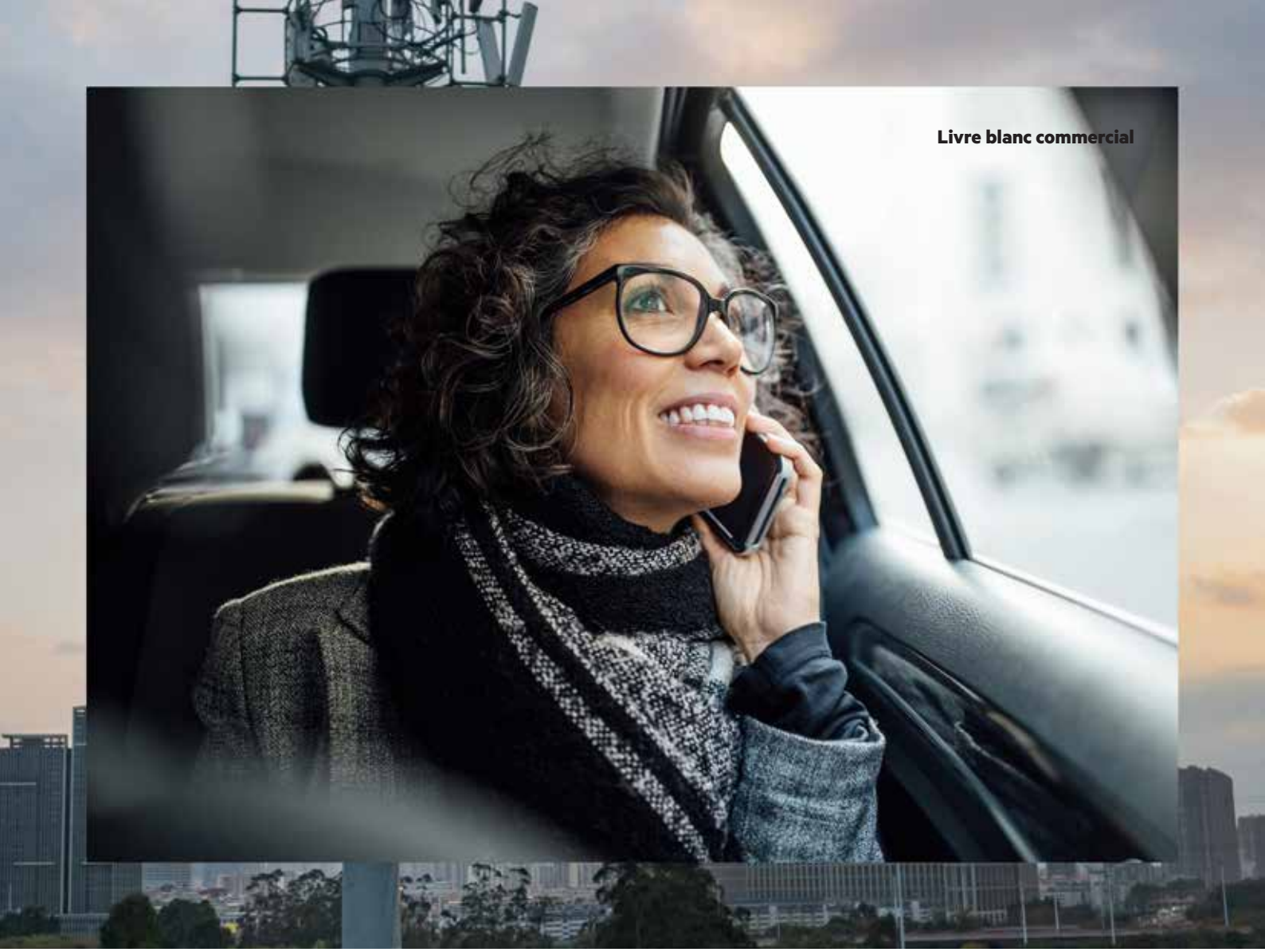

Livre blanc commercial

HPE aruba networking

Guide complet pour l'adoption du ZTNA

HPE GreenLake

77 %

77 % des entreprises prévoient de mettre en place un environnement de travail hybride.

500 %

Cette nouvelle réalité a entraîné une augmentation de 500 % des menaces pour la sécurité en l'espace d'un an.

4 %

Les équipes informatiques ont vu leurs responsabilités s'accroître considérablement, mais leurs budgets n'augmentent que de 4 % par an.

Le défi de l'accès sécurisé aujourd'hui

Vous lisez peut-être ce guide chez vous, dans votre bureau ou ailleurs. Il ne fait aucun doute que le secteur dans lequel nous évoluons aujourd'hui fonctionne de manière très différente de ce que l'on pouvait voir il y a seulement quelques années. Le paysage des entreprises a changé, ce qui a introduit tout un ensemble de défis que les équipes informatiques doivent relever, l'un des plus importants étant la méthode de connectivité sécurisée aux applications professionnelles.

Cela peut sembler assez simple, mais si l'on utilise la mauvaise technologie, obtenir un « accès sécurisé » devient une gageure insurmontable, à l'heure où les problèmes liés au cloud computing et à la mobilité se démultiplient. Sans surprise, nous voyons des acteurs malintentionnés se frotter les mains et s'employer à tirer profit des technologies qui assuraient autrefois la sécurité des entreprises, mais introduisent aujourd'hui des risques.

C'est la raison pour laquelle les responsables informatiques et commerciaux recherchent une nouvelle solution d'accès offrant une connectivité fluide aux utilisateurs et une gestion simplifiée pour leurs équipes. Pour Gartner, cette solution d'accès moderne est l'accès réseau Zero Trust (ZTNA), et nous ne pouvons que valider cette affirmation.

D'ici 2023, 60 % des entreprises abandonneront leurs réseaux privés virtuels (VPN) d'accès à distance au profit du ZTNA.

– Guide Gartner du marché du ZTNA

Qu'est-ce que le ZTNA – et pourquoi maintenant ?

Les VPN ont été conçus pour résoudre un problème plus simple à une époque elle aussi plus simple : fournir à une petite partie du personnel un accès sécurisé à des applications contrôlées par le service informatique dans un datacenter local. Cela semble effectivement simple, n'est-ce pas ? C'était il y a vingt ans : les utilisateurs installaient des clients complexes sur leurs ordinateurs de bureau et bénéficiaient d'un accès à quelques applications au niveau réseau. Cela impliquait un certain niveau de confiance, les utilisateurs se limitant à utiliser les seules applications auxquelles ils avaient accès. En outre, les acteurs malintentionnés n'étaient pas à l'affût pour infiltrer les réseaux et exfiltrer des données.

Aujourd'hui, en revanche, les VPN commencent à montrer des signes d'obsolescence : les connexions instables, l'évolutivité et les performances limitées, ainsi que la complexité de la configuration et de la maintenance ne sont qu'une petite partie des problèmes liés aux VPN d'accès à distance. En outre, les entreprises doivent prendre en compte d'autres facteurs lorsqu'elles cherchent à mettre en œuvre une solution de sécurité d'accès moderne : vérification d'identité et d'appareil, accès et implémentation de règles au niveau application, et flexibilité pour les employés dispersés géographiquement et les tiers (qui représentent environ 1/3 du personnel pris en charge).

L'accès réseau Zero Trust (ZTNA) est l'un des principaux éléments d'une plateforme Security Service Edge (SSE) (ZTNA, SWG, CASB et DEM) ; il offre aux équipes informatiques une alternative moderne aux solutions traditionnelles de sécurité réseau. Le ZTNA, devenu aujourd'hui la technologie d'accès de référence, permet aux organisations de toutes tailles de connecter en toute sécurité les utilisateurs (quel que soit leur emplacement ou leur appareil)

aux applications basées sur le cloud ou dans le datacenter. Le ZTNA implémente le principe Zero Trust « ne faire confiance à personne » en demandant à tous les utilisateurs de s'authentifier et d'authentifier leurs appareils avant d'obtenir un accès, ce qui réduit considérablement le risque que des logiciels malveillants ou des acteurs malintentionnés obtiennent un accès non autorisé. En outre, le ZTNA applique le principe du moindre privilège, qui limite l'accès aux applications spécifiques autorisées, en incorporant une segmentation fondée sur des règles et en réduisant au maximum le risque de migration de données d'un serveur à l'autre en cas d'intrusion d'un programme malveillant.

Contrairement aux solutions de sécurité traditionnelles telles que les VPN, le ZTNA offre des avantages significatifs, notamment les suivants :

- Intégration rapide des employés, des sous-traitants et des tiers sans les casse-tête et la complexité associés à l'intégration des utilisateurs via des VPN
- Accès simplifié aux applications pour les employés travaillant dans des emplacements géographiques différents, afin d'améliorer la productivité et la collaboration
- Accès sans client à de nombreuses applications Web, RDP, SSH, Git et DB
- Client simple disponible pour n'importe quel port/protocole d'accès (sans formation complexe ni besoin d'assistance du service de support technique)
- Fonctionnalités de sécurité Zero Trust, avec notamment l'authentification et l'autorisation permanentes des utilisateurs et des appareils afin d'empêcher les utilisateurs non autorisés ou la pénétration de programmes malveillants

ZTNA	VPN
✓ Prise en charge des travailleurs hybrides	⊘ Prend en charge les travailleurs à distance
✓ Expérience fluide avec la conception « toujours en service » et l'intégration IDP	⊘ Expérience frustrante avec des demandes de connexion répétées
✓ Accès direct aux ressources de l'entreprise avec négociation automatique	⊘ Expérience lente en raison de la liaison au datacenter
✓ Accès utilisateurs aux applications autorisées, pas au réseau d'entreprise	⊘ Employés et tiers à risque placés sur le réseau d'entreprise
✓ Applications et réseau invisibles pour les utilisateurs non autorisés	⊘ Infrastructure VPN exposée à des menaces (p. ex. ransomware)
✓ Gestion simple avec une politique granulaire Zero Trust	⊘ Segmentation réseau complexe à gérer

Figure 1. Comparaison des technologies ZTNA et VPN

L'architecture ZTNA

Les solutions de ZTNA, comme HPE Aruba Networking ZTNA, reposent sur un point de contrôle basé sur le cloud. Il s'agit d'un point d'authentification distribuée, d'autorisation et d'application de politiques, qui régit les transactions entre les utilisateurs et les applications. Le ZTNA filtre toutes les connexions en interdisant toute connexion entrante vers les applications, ce qui renforce la sécurité des applications et réduit le degré d'exposition aux attaques.

Modèle conceptuel de ZTNA sur l'initiative d'un service

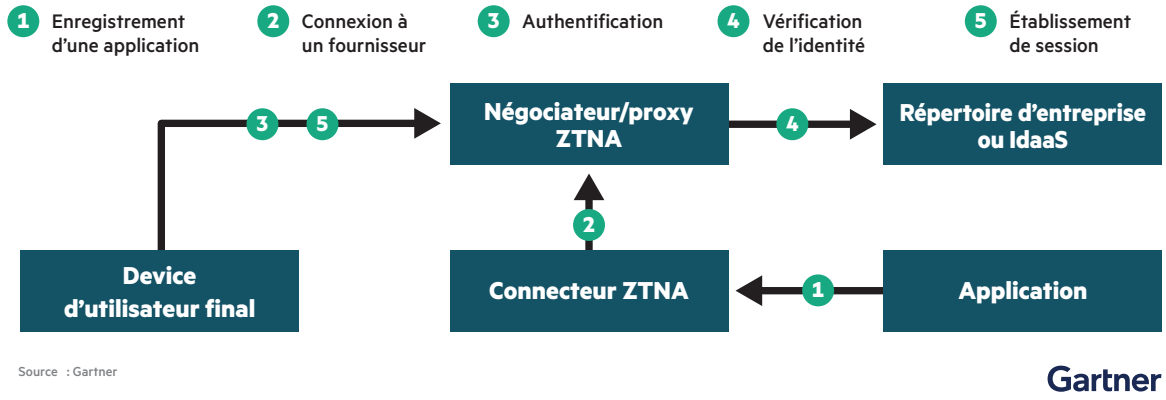

Figure 2. Fonctionnement d'une plateforme ZTNA sur l'initiative d'un service

1. Un utilisateur tente d'accéder à une application d'entreprise

Offrez un accès sécurisé aux principales applications (y compris VoIP et ICMP) avec ou sans client.

2. Le ZTNA assure la médiation de la requête

Évitez les connexions de passage risquées (tout le trafic des ressources de l'entreprise passe par un nœud cloud ZTNA).

3. Le ZTNA valide l'identité et la règle

L'identité est intégrée dans la plateforme ZTNA pour faciliter l'accès Zero Trust et l'adaptation automatique des droits d'accès en fonction des changements de contexte (posture de l'appareil, emplacement, etc.).

4. Le ZTNA se connecte à la ressource de manière sécurisée

La plateforme ZTNA établit automatiquement des connexions avec certaines applications spécifiques tout en empêchant les utilisateurs d'accéder au réseau. Les applications privées sont rendues invisibles sur Internet et les connexions aux applications SaaS sont rapides et fluides.

5. Le ZTNA inspecte le trafic et surveille l'expérience utilisateur

La plateforme ZTNA offre une visibilité sur l'activité des utilisateurs, permet de détecter toute activité malveillante et donne un aperçu de l'expérience d'accès pour l'utilisateur final.

Une fois qu'un utilisateur s'est authentifié au point de contrôle, des sessions individuelles sont établies pour certaines applications spécifiques avec un temps de vie donné. Toutes les sessions sont régies par des politiques établies par les administrateurs informatiques et suivent les utilisateurs indépendamment de leur emplacement. En outre, l'autorisation et l'authentification de chaque session, ainsi que l'évaluation de chaque appareil, sont assurées en continu ; si un appareil change d'emplacement, des mesures peuvent être prises pour limiter l'accès aux applications, restreindre les téléchargements de fichiers, voire mettre l'appareil en quarantaine en vue d'une remédiation.

L'expérience de l'utilisateur, quant à elle, est considérablement simplifiée par rapport aux VPN traditionnels et autres modèles de sécurité similaires. La plateforme SSE de HPE Aruba Networking permet de travailler avec le ZTNA avec ou sans client. De nombreuses transactions peuvent être traitées sans utiliser de client, notamment les sessions Web, RDP, SSH et autres. Pour accéder à un port/protocole donné, il n'est pas difficile de se procurer un client léger pour l'appareil de son choix, offrant ainsi un accès rapide et sécurisé aux applications et ressources nécessaires pour assurer la productivité.

Le réseau obtenu au final est beaucoup plus sûr qu'avec une stack de sécurité traditionnelle comprenant des pare-feu et des outils de détection d'intrusion et de gestion des points d'extrémité. De plus, grâce aux fonctions ZTNA telles que l'isolation des applications offerte par HPE Aruba Networking, les applications elles-mêmes sont

plus sûres et bénéficient de la sécurité inhérente à la microsegmentation, qui limite la migration de données d'un serveur à un autre, et donc les risques de prolifération de programmes malveillants.

Atteindre le Zero Trust avec le ZTNA

Il est important de souligner que la plupart des organisations ont déjà mis en place un certain niveau de Zero Trust, que ce soit sous la forme d'une authentification à deux facteurs ou plus, d'une connexion unique ou de l'application de politiques. Il est également important de souligner que la mise en œuvre du Zero Trust est un processus long (en effet, les topologies de réseau ne sont jamais identiques). Les équipes chargées de la sécurité et de l'architecture informatique sont bien souvent différentes, et doivent donc collaborer pour bénéficier des avantages considérables du ZTNA en termes de sécurité et de productivité, et ouvrir la voie vers une stratégie holistique Security Service Edge (SSE).

Vous trouverez ci-dessous une suggestion de processus d'« adoption » dont les étapes peuvent être suivies au fur et à mesure par les organisations désireuses de renforcer leur profil de sécurité, de manière à rationaliser l'accès de leur personnel itinérant et à réduire les risques de pénétration de programmes malveillants et d'exfiltration de données.

La checklist de l'adoption du ZTNA

La première étape recommandée par Gartner pour moderniser l'accès sécurisé aux entreprises consiste à abandonner les architectures de sécurité traditionnelles au profit du ZTNA. Cela permet également aux utilisateurs (et aux services informatiques) de s'affranchir des problèmes de connectivité complexes engendrés par les stacks de sécurité obsolètes. Les utilisateurs seront plus satisfaits et plus productifs, tandis que les services informatiques pourront se concentrer sur d'autres tâches essentielles. Les sections suivantes décrivent les meilleures pratiques permettant aux équipes informatiques d'assurer le passage d'une solution d'accès traditionnelle à un ZTNA moderne.

1. Comprendre votre environnement

Aujourd'hui, les entreprises utilisent souvent des centaines, voire des milliers d'applications (connues ou non), notamment des systèmes CRM et ERP, ainsi que des postes de travail distants tels que RDP et VDI. Disposer d'un inventaire des applications actuellement utilisées peut s'avérer utile pour déterminer qui peut accéder à quelles applications ; cela étant, les meilleures solutions ZTNA bénéficient de fonctionnalités de découverte d'applications, qui permettent aux services informatiques de découvrir toutes les applications de shadow IT présentes dans leur système.

En outre, déterminer la manière dont les utilisateurs accèdent aux applications de votre organisation peut vous donner des informations précieuses. Par exemple, certains utilisateurs tirent-ils davantage parti du BYOD que d'autres ? Inversement, les utilisateurs accèdent-ils encore aux applications hébergées sur site ?

Il est important de disposer d'une visibilité initiale de votre environnement actuel afin d'éviter tous les écueils potentiels lors du déploiement.

2. Commencez par les points les plus à risque (autrement dit, l'accès à distance)

Aujourd'hui, les équipes sont constituées d'employés, de tiers, de clients et d'utilisateurs fusionnés ou acquis, dont beaucoup travaillent à distance. Les uns comme les autres doivent bénéficier d'un accès bien pensé aux ressources de l'entreprise, idéalement sans avoir besoin d'une configuration complexe ou d'un client sur leur terminal. Envisagez de commencer votre déploiement avec un petit échantillon de ces utilisateurs distants (par exemple, votre équipe de direction, vos développeurs ou des utilisateurs tiers), et apprenez à configurer et à appliquer des politiques d'accès sur le principe du moindre privilège avec le ZTNA. Par la suite, vous poursuivrez votre déploiement avec le reste de votre personnel distant.

3. Élargir l'accès aux employés travaillant dans les locaux (et ailleurs)

À l'heure où 77 % des organisations adoptent le travail hybride sous une forme ou une autre, il est important que l'accès au ZTNA s'étende également pour prendre en charge les utilisateurs travaillant au bureau. Étant donné que les employés qui vont et viennent constamment au bureau ont accès à des données sensibles, il est important que le Zero Trust et le principe du moindre privilège soient appliqués de manière globale, afin de ne pas créer de failles de sécurité susceptibles de mettre votre réseau en danger. En outre, cela permet à vos équipes hybrides de bénéficier d'une expérience d'accès totalement fluide et cohérente, à domicile comme au bureau.

Le ZTNA est également profitable dans les contextes de fusion/acquisition. Des solutions telles que HPE Aruba Networking ZTNA permettent rapidement et simplement de bénéficier d'un accès sûr et Zero Trust aux applications et aux ressources de différentes organisations, avant la fusion des topographies de réseau. Grâce à des technologies basées sur le cloud, HPE Aruba Networking ZTNA offre des services hautement évolutifs qui permettent de fournir (avec ou sans agent) un accès aux ressources, où qu'elles se trouvent, tout en les isolant des utilisateurs, des appareils et des réseaux potentiellement compromis. Son déploiement est rapide et ne nécessite pas de modifications importantes du réseau, tandis qu'une console cloud centrale gère l'ensemble du système par le biais de politiques inter-applications, de sorte que seuls les utilisateurs autorisés ont accès aux applications auxquelles ils ont droit.

4. La prochaine étape du déploiement du SSE

À ce stade, 1/4 du déploiement global du SSE est terminé ! Vous avez réussi à réduire au maximum les risques d'accès dans les zones les plus problématiques, et vous pouvez envisager de poursuivre le déploiement de votre SSE en évaluant les contrats existants et en élaborant

un plan d'élimination progressive des technologies basées sur le modèle du périmètre de sécurité. Les services informatiques peuvent consolider des contrats en sélectionnant un fournisseur unique de SSE, capable de fournir les technologies ZTNA, SWG, CASB et DEM. Ces décisions n'auront pas seulement un impact sur l'infrastructure du siège de l'entreprise, mais pourront également contribuer à l'accélération des projets de transformation des agences locales, et ce, en aidant à réduire les coûts de MPLS superflus et en favorisant l'investissement dans des services de sécurité sur l'edge, basés sur le cloud, au niveau des filiales.

La sécurité des accès à distance réinventée grâce au ZTNA

Les entreprises d'aujourd'hui ont besoin d'un niveau de développement rapide, mais aussi d'un degré élevé de collaboration/travail en équipe et de sécurité/d'intégrité des données. L'élément central permettant de répondre à chacun de ces besoins est un réseau moderne, flexible, évolutif et sécurisé, qui facilite la communication au lieu de l'entraver. Si les architectures traditionnelles telles que les VPN peuvent encore avoir une pertinence limitée pour certains utilisateurs, la complexité de la gestion et de la maintenance d'une infrastructure obsolète ne fait qu'accaparer des ressources qui pourraient être mieux utilisées.

Le ZTNA est l'avenir de l'accès moderne et permet de relever les défis de mobilité des équipes, de sécurité de l'accès au réseau et d'évolutivité, en éliminant les problèmes complexes de configuration et de déploiement. Un lieu de travail moderne exige un accès transparent et des ressources sécurisées, et HPE Aruba Networking ZTNA permet d'atteindre ces deux objectifs.

Avec HPE Aruba Networking ZTNA, les équipes informatiques peuvent :

- Déployer leur système en quelques minutes ou en quelques heures, plutôt qu'en quelques semaines ou en quelques mois
- Assurer la productivité et la collaboration d'équipes évoluant dans le monde entier
- Améliorer la visibilité et l'expérience de gestion grâce à des informations détaillées sur l'activité des utilisateurs et des applications
- Réduire les risques de perte de données et de pénétration de programmes malveillants tout en améliorant la conformité
- Simplifier la gestion informatique grâce à des politiques intuitives de Zero Trust et à des contrôles d'accès rigoureux

Modernisez dès aujourd'hui l'accès à votre lieu de travail grâce à HPE Aruba Networking SSE. Inscrivez-vous et testez la plateforme HPE Aruba Networking Security Service Edge (SSE).

En savoir plus

arubanetworks.com/sse-test-drive/

Visiter **ArubaNetworks.com**

Faites le bon achat.
Contactez nos spécialistes.

Nous contacter

BWP_ZTNA-Adoption_A4_RB_011124 a00136926fre

Hewlett Packard Enterprise