Protégez et fortifiez votre datacenter Zero Trust

Le datacenter abrite, sur site ou dans le cloud, ce que votre organisation a de plus précieux : ses données et ses applications les plus sensibles. Quel que soit l'emplacement où elles résident, il est essentiel de les protéger. Vous devez avoir une bonne compréhension des différentes composantes du datacenter Zero Trust et vous assurer que vous avez mis en place les mesures de protection nécessaires pour protéger votre organisation et vos données.

Manque de visibilité

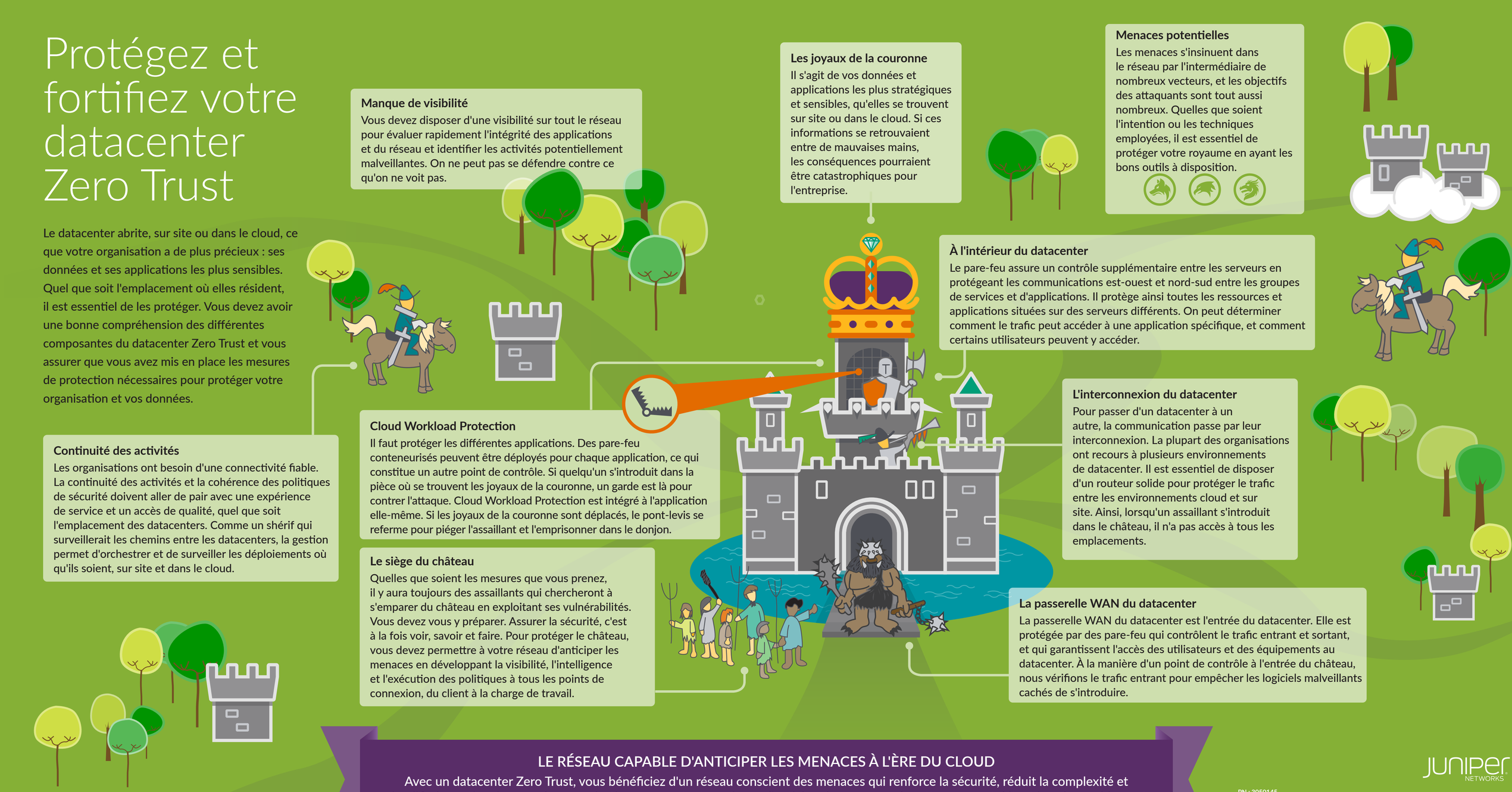
Vous devez disposer d'une visibilité sur tout le réseau pour évaluer rapidement l'intégrité des applications et du réseau et identifier les activités potentiellement malveillantes. On ne peut pas se défendre contre ce qu'on ne voit pas.

Les joyaux de la couronne

Il s'agit de vos données et applications les plus stratégiques et sensibles, qu'elles se trouvent sur site ou dans le cloud. Si ces informations se retrouvaient entre de mauvaises mains, les conséquences pourraient être catastrophiques pour l'entreprise.

Menaces potentielles

Les menaces s'insinuent dans le réseau par l'intermédiaire de nombreux vecteurs, et les objectifs des attaquants sont tout aussi nombreux. Quelles que soient l'intention ou les techniques employées, il est essentiel de protéger votre royaume en ayant les bons outils à disposition.



À l'intérieur du datacenter

Le pare-feu assure un contrôle supplémentaire entre les serveurs en protégeant les communications est-ouest et nord-sud entre les groupes de services et d'applications. Il protège ainsi toutes les ressources et applications situées sur des serveurs différents. On peut déterminer comment le trafic peut accéder à une application spécifique, et comment certains utilisateurs peuvent y accéder.

Continuité des activités

Les organisations ont besoin d'une connectivité fiable. La continuité des activités et la cohérence des politiques de sécurité doivent aller de pair avec une expérience de service et un accès de qualité, quel que soit l'emplacement des datacenters. Comme un shérif qui surveillerait les chemins entre les datacenters, la gestion permet d'orchestrer et de surveiller les déploiements où qu'ils soient, sur site et dans le cloud.

Cloud Workload Protection

Il faut protéger les différentes applications. Des pare-feu conteneurisés peuvent être déployés pour chaque application, ce qui constitue un autre point de contrôle. Si quelqu'un s'introduit dans la pièce où se trouvent les joyaux de la couronne, un garde est là pour contrer l'attaque. Cloud Workload Protection est intégré à l'application elle-même. Si les joyaux de la couronne sont déplacés, le pont-levis se referme pour piéger l'assaillant et l'emprisonner dans le donjon.

L'interconnexion du datacenter

Pour passer d'un datacenter à un autre, la communication passe par leur interconnexion. La plupart des organisations ont recours à plusieurs environnements de datacenter. Il est essentiel de disposer d'un routeur solide pour protéger le trafic entre les environnements cloud et sur site. Ainsi, lorsqu'un assaillant s'introduit dans le château, il n'a pas accès à tous les emplacements.

Le siège du château

Quelles que soient les mesures que vous prenez, il y aura toujours des assaillants qui chercheront à s'emparer du château en exploitant ses vulnérabilités. Vous devez vous y préparer. Assurer la sécurité, c'est à la fois voir, savoir et faire. Pour protéger le château, vous devez permettre à votre réseau d'anticiper les menaces en développant la visibilité, l'intelligence et l'exécution des politiques à tous les points de connexion, du client à la charge de travail.

La passerelle WAN du datacenter

La passerelle WAN du datacenter est l'entrée du datacenter. Elle est protégée par des pare-feu qui contrôlent le trafic entrant et sortant, et qui garantissent l'accès des utilisateurs et des équipements au datacenter. À la manière d'un point de contrôle à l'entrée du château, nous vérifions le trafic entrant pour empêcher les logiciels malveillants cachés de s'introduire.

LE RÉSEAU CAPABLE D'ANTICIPER LES MENACES À L'ÈRE DU CLOUD

Avec un datacenter Zero Trust, vous bénéficiez d'un réseau conscient des menaces qui renforce la sécurité, réduit la complexité et simplifie la gestion. Lorsque les organisations permettent au réseau d'anticiper les menaces, les attaques sont détectées plus rapidement et les assaillants ont moins de chances de s'immiscer dans le réseau, ce qui protège les utilisateurs, les applications, l'infrastructure et, bien sûr, les joyaux de la couronne.

JUNIPER NETWORKS

PN : 3050145