

•

Étape 2 : accès à distance complet depuis n'importe quel périphérique

Accès interne par le biais de la stratégie « Tout périphérique » de Cisco

Étape 1 : priorité au contrôle des programmes malveillants sur le réseau

Les périphériques appartenant à la société sont des outils importants pour le maintien de la sécurité et de l'intégrité des données d'entreprise. Cisco effectue un travail colossal pour la protection de nos environnements d'hébergement administrés en installant et en gérant différents niveaux de défense sur les ordinateurs déployés de l'entreprise (notamment un programme anti-pourriel, une protection anti-logiciel espion, un antivirus administré, un programme de prévention des intrusions sur l'hôte et une solution de gestion des correctifs). Toutefois, dans la mesure où Cisco abandonne progressivement les environnements d'hébergement administrés et les périphériques détenus par l'entreprise, ces contrôles doivent s'éloigner des termin ux de déea so52rise, c 51grits et les pmesure0657213-43.G8335Q24523g51f28402.7

