



Comment sécuriser vos postes de travail pour le VDI et le DaaS

Chez ZeeTim, la notion de *security by design* est clé dans tout ce que nous faisons. Fournir aux organisations le poste de travail cloud le plus sécurisé possible est ce qui nous a poussés à développer notre solution poste de travail ZeeTerm, composée du système d'exploitation ZeeOS et de la console de gestion ZeeConf.

Que votre ZeeTerm fonctionne sur notre matériel ou qu'il s'agisse d'un PC que vous avez converti à l'aide de ZeeTransformer, les standards de sécurité seront exactement les mêmes.

Au-delà des avantages en termes de sécurité bien connus qu'offrent les clients légers, l'offre de postes de travail de ZeeTim va encore plus loin pour vous offrir l'une des solutions client léger les plus sécurisées du marché.

Voici comment.

Aucune action ne peut être effectuée localement

- Système d'exploitation en lecture seule, aucune action possible sur le client léger de la part de qui que ce soit
- Aucune configuration locale autorisée pour quiconque
- L'utilisateur ne peut lancer qu'un programme qui a été préalablement autorisé : si les utilisateurs téléchargent des binaires depuis Internet, ceux-ci ne s'exécuteront pas.
- Aucune donnée ne peut être téléchargée ou stockée localement

Un système d'exploitation breveté

- Système d'exploitation basé sur Linux
- Système d'exploitation renforcé avec structure brevetée : chaque package d'application s'exécute dans sa sandbox dédiée plutôt que sur un seul fichier. Par conséquent, un package peut être mis à jour de façon individuelle, cette granularité permettant ainsi de réduire considérablement la surface d'attaque lors des opérations de mise à jour
- Plus besoin d'antivirus

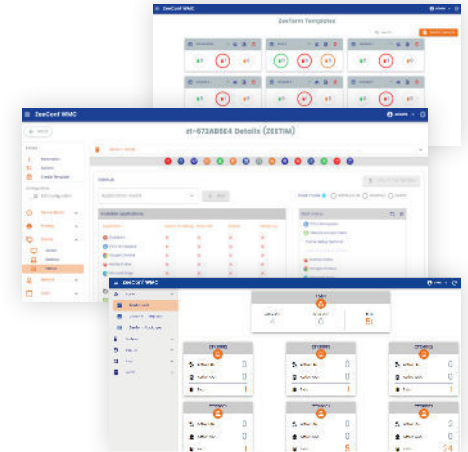
Toutes les communications sont chiffrées

- La connexion Client – Serveur est sécurisée via HTTPS
- Toutes nos communications VNC étant chiffrées avec SSH, l'utilisation de Teamviewer n'est donc pas nécessaire, la communication étant déjà 100% sécurisée
- Les déploiements et les mises à jour / mises à niveau PXE sont possibles via Internet, plus besoin d'utiliser des protocoles de bas niveau conçus pour le réseau local tels que DHCP ou TFTP

- La connexion au terminal est assurée via SSH par défaut, l'un des protocoles de sécurité les plus robustes du marché aujourd'hui, et sécurisée par une paire de certificats et de clés de chiffrement. Il n'y a aucun moyen de se connecter à un poste de travail ZeeTim autrement que via ce flux de connexion sécurisé par SSH. Cette architecture empêche la plupart des attaques réseau telles que les attaques de type « Bagle malware ».

Une console de gestion pour gérer la sécurité des postes de travail de manière centralisée, avec suivi des actions effectuées

- La partie serveur de la console de gestion agit comme une base de confiance, vérifiant à intervalles réguliers la liste des packages présents sur le système d'exploitation ZeeOS. En cas de différence avec les données enregistrées sur le serveur, ZeeConf remplace automatiquement sur l'OS les fichiers ayant été modifiés.
- Administration basée sur les rôles avec deux niveaux d'accès administrateur
- Authentification administrateur basée sur Active Directory
- Possibilité de choisir les paramètres auxquels un administrateur peut accéder, le ZeeTerm ou le groupe de ZeeTerm pouvant être gérés en fonction des groupes de sécurité Active Directory
- Responsabilité des actions administrateur avec possibilité d'enregistrer et de vérifier qui a fait quoi, quand et sur quel poste
- Options de reporting avec graphiques, indiquant le statut des terminaux ainsi que des informations clés pour les administrateurs
- Prise en charge native des protocoles VPN tels que Cisco Anyconnect, Open VPN, Wireguard
- Gestion sécurisée des postes de travail distants grâce à ZeeConf Gateway
- Possibilité de désactiver les périphériques USB



Sécurité du matériel

- Sécurité du poste physique : nous fournissons un Kensington lock sur nos appareils
- Le télétravail devenant la norme de nos jours, ZeeTim assure un BYOD sécurisé grâce à la solution basée sur clé USB ZeeTransformer

Enfin, ZeeTim contribue à sécuriser le poste de travail dans sa globalité grâce aux outils complémentaires suivants :



Authentification multifacteur conçue pour le VDI



Un coffre-fort de mots de passe pour une connexion / déconnexion rapide aux espaces de travail virtuels sur les postes de travail ZeeOS et Windows



Technologie d'optimisation d'impression qui compresse, accélère et sécurise les flux d'impression