

PROTÉGER DES SECRETS COMMERCIAUX ET DE CONCEPTION

Cas d'un constructeur aéronautique : éviter l'espionnage industriel et commercial



Les postes de travail sont hétérogènes : PC portables, tablettes 2 en 1 de type Surface Pro, tablettes tactiles durcies pour un environnement d'atelier.

EXIGENCES

La sécurité des données sur le poste de travail doit être assurée **en cas de vol ou de copies de disque dur**. La solution doit donc assurer le **chiffrement intégral du poste de travail**.

L'utilisateur doit par ailleurs posséder, en plus des droits d'accès Windows, **le droit-d'en-connaître sur les partages réseau** auxquels il souhaite accéder via le VPN en place.

Enfin, pour garantir un niveau de sécurité élevé, **un token cryptographique**, déjà en place au sein de l'entreprise, doit être utilisé pour **contenir la clé de chiffrement de l'utilisateur**.

SOLUTION

Le client a décidé de déployer **CRYHOD** et **ZONECENTRAL** pour chiffrer :

- + Les partitions du poste de travail,
- + (et) Les partages réseau accédés via le VPN.

EXPÉRIENCE

IT

Déploiement télédistribué de **CRYHOD** et **ZONECENTRAL** sur les postes de travail via SCCM.

UTILISATEURS

L'expérience utilisateur est simplifiée avec une saisie de PIN unique au démarrage du poste : la session utilisateur est ouverte automatiquement par Smartcard Logon et ne nécessite aucune saisie additionnelle.

DÉPARTEMENT SÉCURITÉ

Génération d'un certificat de chiffrement par utilisateur.

AVANTAGES

CRYHOD et **ZONECENTRAL** permettent de **s'interfacer avec tous types de tokens**, et un certificat dédié aux opérations de chiffrement a été ajouté à celui en place.

De plus, **les solutions choisies utilisent et partagent le contexte cryptographique**, ce qui évite les saisies de PIN redondantes et facilite ainsi l'expérience de l'utilisateur.



CRYHOD



ZONECENTRAL