Toyota Financial Services : un système d'information constamment à jour et sécurisé

Profil :

Présent dans une quarantaine de pays, Toyota Financial Services propose à ses clients une gamme complète de financements et de services associés via son réseau de concessionnaires.

Lieu :

Vaucresson (Hauts-de-Seine, France)

Solutions :

- Ivanti® Patch for Endpoint Manager, powered by Landesk
- Ivanti Device Control, powered by Heat
- Ivanti Application Control, powered by AppSense

Principaux bénéfices :

- Réduction importante du temps consacré au patching
- Réduction des risques d'erreur sur les mises à jour
- Correction d'erreurs antérieures
- Sécurité accrue des dispositifs mobiles (type clés USB)
- Aide à la conformité au RGPD des dispositifs mobiles
- Aide à la conformité aux audits de sécurité annuels
- Liste blanche et listes noires contextuelles et gestion des privilèges.

Le défi

Société internationale, Toyota Financial Services appuie sa stratégie IT sur des solutions globales pour l'ensemble de ses implantations, tout en conservant une certaine autonomie à chaque pays, en fonction de leurs enjeux et contraintes locales.

Ainsi, si les réseaux, les accès à distance, les liaisons et intersites et la messagerie sont globales, le cœur de réseau, les systèmes de stockage et de virtualisation, les outils bureautiques ou encore certaines solutions métiers relèvent entièrement de la compétence IT de chaque pays, dans le cadre d'objectifs globaux, et notamment de sécurité.

Pour répondre à ces directives sécuritaires de la maison-mère japonaise, l'équipe IT France a, pendant plusieurs années, traité le patching de façon manuelle, aidé par quelques outils sporadiques qui ne répondaient pas aux besoins de gestion des mises à jour sur l'ensemble du périmètre IT administré en local.

Car malheureusement, lorsque des correctifs sont appliqués manuellement, il arrive que des dysfonctionnements se produisent, empêchant la mise à jour de certains composants. « *C'est un problème que nous avions rencontré avec VMware Tools* » se souvient ~~le~~ Pierre NG, le Responsable de la Sécurité des Systèmes d'Information.

En parallèle, les audits de sécurité récurrents rendaient indispensable un meilleur contrôle des applications, tandis que, notamment pour répondre aux nouvelles obligations du RGPD, l'utilisation de dispositifs mobiles (clés USB par exemple) identifiés et chiffrés devenait obligatoire.

La solution

« *A l'automne 2017, dans le cadre de ma veille technologique, fondamentale en matière de sécurité notamment, Ivanti a souhaité nous présenter sa gamme de solutions* » détaille Pierre NG. « *La solution de patch management et l'automatisation qu'elle permet nous a immédiatement séduits* ».

Dès le début 2018, un POC est lancé pour tester la solution en situation réelle. Immédiatement, c'est la capacité d'inventaire automatique de Patch for Endpoint Manager, mais également le test des patches en amont de leur déploiement qui convainc Pierre NG : « *au départ, l'inventaire automatique nous a permis de constituer très rapidement la cartographie de nos matériels. Désormais, dès qu'un patch est publié, nous savons que Patch for Endpoint Manager s'occupe de tout le processus, après un test préalable par Ivanti* ».

Dès le mois de mars, la solution est déployée sur presque 300 matériels répartis sur 2 sites : 20 serveurs physiques, plus de 150 serveurs virtuels, 20 laptops, 100 postes de travail virtualisés, etc.

En complément, Toyota Financial Services France fait également appel à la solution Application Control d'Ivanti pour compléter la sécurisation de son SI, contre les risques d'exploitations Zéro-Day ou encore l'exécution d'applications non autorisées, en associant listes blanches dynamiques et gestion fine des privilèges.

Pour renforcer cette démarche préventive, la solution Ivanti Device Control permet à Toyota Financial Services d'identifier rapidement chaque dispositif mobile (clés USB notamment) et d'en renforcer la sécurité, afin qu'aucune application ne puisse être installée ou exécutée à partir d'un dispositif mobile inconnu, réduisant ainsi la surface d'attaque potentielle de l'entreprise. Également conçu pour encrypter les données stockées dans les dispositifs mobiles, Device Control protège contre la perte de données confidentielles.

Les résultats

Dès le départ, les résultats sont spectaculaires pour Toyota Financial Services, notamment en termes de temps passé sur le patching : « *au préalable, la gestion manuelle du patching sur l'ensemble du périmètre France occupait 60 % de mon temps* » détaille Pierre NG. « *Aujourd'hui, 1 journée par semaine est largement suffisante, contre trois auparavant* ».

Ivanti Patch for Endpoint Manager c'est aussi un véritable confort d'utilisation : là où une connexion individuelle à chaque serveur était indispensable, il suffit désormais de cocher les matériels à mettre à jour directement dans l'interface de la solution, et son catalogue de patches, le plus important du marché, s'occupe du reste.

Avec Application Control, c'est aussi toute la sécurité du SI qui est renforcée, grâce à une gestion automatisée des applications autorisées et non autorisées, sans intervention des équipes IT, tout en garantissant la conformité aux audits annuels.

« La gestion du patching occupait 60 % de mon temps. Avec Ivanti, 1 journée par semaine suffit »

- Pierre NG
RSSI, Toyota Financial Services

En outre, et grâce à sa gestion granulaire des privilèges utilisateurs associée à l'auto-évaluation des exceptions, Application Control est en mesure de changer un profil administrateur en utilisateur régulier, et assurer une mise à niveau des privilèges sur des points très précis : capacité d'installer des applications ou des imprimantes, ou encore utiliser un terminal (PowerShell). À l'inverse, un utilisateur peut devenir administrateur, et certains privilèges, inutiles pour son rôle, lui être supprimés. De cette façon, Ivanti offre aux utilisateurs les droits dont ils ont besoin pour remplir leurs missions, ni plus, ni moins.

Quant aux clés USB, régulièrement utilisées par les collaborateurs, elles ne présentent plus de menaces pour le réseau de la société, grâce à Ivanti Device Control, qui permet également une traçabilité complète des données stockées sur ces dispositifs, répondant ainsi aux nouvelles obligations du RGPD.

À peine quelques semaines après le déploiement des 3 solutions de sécurisation des systèmes client d'Ivanti, de nouvelles perspectives d'usage de la gamme de solutions se font déjà jour. Le prochain chantier de Toyota Financial Services pourrait ainsi être l'ITSM (IT Service Management), afin de définir, déployer et automatiser les workflows de l'entreprise, et notamment l'onboarding / offboarding des collaborateurs.

« *Grâce à la large gamme de solutions Ivanti, nous touchons du doigt ce qui est le rêve de beaucoup de membres des équipes IT : disposer d'un système d'information entièrement automatisé* », conclut Pierre NG.

www.ivanti.fr

+33 (0)1.49.03.77.80

contact@ivanti.fr