

Sécurité et mobilité Windows 8

pour les utilisateurs nomades

UEFI • BitLocker et AppLocker • DirectAccess • VPN
• SmartScreen • Windows Defender...

Arnaud Jumelet
Stanislas Quastana
Pascal Saulière

Préface de Bernard Ourghanlian



Table des matières

Avant-propos	XVII
À qui ce livre s'adresse-t-il ?	XVII
Comment ce livre est-il structuré ?	XVIII
Systèmes nécessaires	XIX
Remerciements	XXI
Arnaud Jumelet	XXI
Pascal Sauliere	XXI
Stanislas Quastana	XXII
 CHAPITRE 1	
Les contraintes du poste de travail mobile	1
Postes d'entreprise vs postes personnels	1
Portables, tablettes et hybrides	3
État des lieux : la fin du cloisonnement (déperimétrisation)	6
Risques pesant sur les postes en situation de nomadisme	7
La perte ou le vol d'informations	7
Vol d'identité par hameçonnage	9
Hameçonnage ciblé (spear phishing)	10
Infection persistante avancée (APT) et intelligence économique	10
Rappel sur les principaux vecteurs de menace	11
Poste de travail non à jour	11
Navigation Internet	11
Réseau	13
Périphérique amovible	14
Courrier électronique	15

CHAPITRE 2

Démarrage sécurisé	17
Qu'est-ce qu'un firmware ?	17
Les types de firmwares	18
Démarrage d'un ordinateur sous Windows 8	18
Démarrage d'une plate-forme compatible BIOS	19
Démarrage d'une plate-forme compatible UEFI	20
Configuration du gestionnaire de démarrage Windows	22
Qu'est-ce qu'un TPM ?	24
Unités fonctionnelles du TPM	25
Gérer le TPM	28
Préparer le module de plate-forme sécurisée (TPM)	29
Measured Boot	32
Secure Boot	32
Modes de fonctionnement	33
Base des signatures	34
Validation des images UEFI : liste blanche et liste noire	35
Implémentation du Secure Boot pour Windows 8	36
Administration du Secure Boot	38
Early-Launch of Anti-Malware (ELAM)	39
Windows Defender est compatible avec ELAM	39
Positionnement d'ELAM dans la séquence de démarrage	40
Code Integrity	41

CHAPITRE 3

Mécanismes d'ouverture de session	43
Authentification des utilisateurs	43
Ouverture de session	43
Les types de comptes reconnus par Windows 8	48
Les types de mots de passe acceptés par Windows 8	52
Authentification forte : combiner plusieurs méthodes	57
Contrôle d'accès	64
Identification, authentification, autorisations	64
Le jeton d'accès	65
Le descripteur de sécurité	66

Contrôle de compte utilisateur	67
Isolation des applications Windows 8	71
Modèle Windows Vista et Windows 7	71
Les AppContainers	72

CHAPITRE 4

Protection contre le code malveillant	77
Protection contre les programmes malveillants	77
Windows Defender, l'anti-malware de Windows 8	78
Windows SmartScreen ou comment prendre la bonne décision	80
Protection à l'échelle de l'entreprise avec System Center 2012 Endpoint Protection	87

CHAPITRE 5

Contrôle des applications	91
Les applications Windows 8	91
Les applications de Bureau	91
Les Windows Apps	92
Mises à jour automatiques sous Windows 8	92
Que sont les mises à jour automatiques ?	92
Windows Update	93
Téléchargement des fichiers avec BITS	94
Services de mises à jour en ligne pour Windows	95
Accéder à Windows Update	95
Configurer les paramètres de Windows Update	96
Configurer la période de maintenance	98
Afficher l'historique des mises à jour installées	99
Gestion des redémarrages sous Windows 8	99
Mises à jour des Apps	100
Infrastructure WSUS pour l'organisation	102
Contrôle des applications autorisées et bloquées	102
AppLocker	102
Principe de fonctionnement AppLocker	103
Choix d'une approche	104
Les règles AppLocker	104
Les règles AppLocker pour les Windows Apps	106

Construction des règles AppLocker.....	106
Commandes AppLocker.....	107
Les avertissements AppLocker.....	108
Le journal d'événements AppLocker.....	109

CHAPITRE 6

Protection des données.....	111
BitLocker et la protection des données.....	111
Protéger son ordinateur lorsque Windows 8 est éteint.....	112
Les nouvelles fonctionnalités BitLocker.....	113
Fonctionnement de BitLocker.....	118
Liste des protecteurs BitLocker.....	119
Intégration dans Active Directory.....	121
Préparer le disque pour BitLocker.....	125
Utiliser BitLocker.....	126
Contrôle d'accès dynamique.....	132
Une évolution naturelle.....	133
Fonctionnement.....	134
Avantages et mise en œuvre pratique de DAC.....	139

CHAPITRE 7

Donner l'accès au SI aux populations nomades.....	141
Quelles technologies d'accès ?.....	142
Points communs à toutes les solutions d'accès à distance – Bonnes pratiques.....	144
Identité et authentification forte.....	144
Contrôle de conformité pour l'accès aux réseaux.....	145
Quelles solutions d'accès distant côté serveur chez Microsoft ?.....	146
Réseaux privés virtuels dans Windows Server.....	146
Windows Server – Services de Bureaux à Distance.....	146
DirectAccess.....	147
Forefront Unified Access Gateway (UAG) 2010.....	148
Les solutions d'accès distants chez Microsoft en résumé.....	149

CHAPITRE 8

Publication d'applications et de Bureaux distants	151
Infrastructure de Bureaux virtuels	151
Topologie de déploiement d'une passerelle Bureau à distance	153
Gestion des accès au travers d'une passerelle Bureau à distance	154
Configuration d'une passerelle Bureau à distance	155
Installation du rôle RD Gateway sur Windows Server 2012.	155
Configuration des propriétés de la passerelle Bureau à distance	157
Configuration des stratégies d'autorisation de la passerelle Bureau à distance	161
Offrir l'accès aux utilisateurs nomades.	165
RD Web	166
Déploiement sur le poste client.	167
Flux RSS	168

CHAPITRE 9

Réseaux privés virtuels	173
Fonctionnement	173
Configuration d'un serveur de réseaux privés virtuels (VPN) avec Windows Server 2012	175
Surveillance des services VPN	183
Configuration manuelle d'une connexion VPN.	183
Création et utilisation d'un kit de connexion	186

CHAPITRE 10

DirectAccess pour les postes gérés	189
Architecture.	190
Composants d'une architecture DirectAccess.	191
IPv6	192
IPsec	199
Serveur d'emplacement réseau	202
Les serveurs d'infrastructure	202
Topologie de déploiement de DirectAccess	203

Topologies à base de Windows Server 2008 R2 versus Windows Server 2012	203
Matrice de compatibilité des topologies de déploiement réseau de DirectAccess	204
Configuration de DirectAccess (Windows Server 2012 et Windows 8) ..	205
Installation de DirectAccess en mode Simplifié	205
Exploration de la configuration simplifiée DirectAccess	208
Surveillance de l'état du serveur DirectAccess	216
Vérification de la configuration sur les postes clients	218
Matrice comparative des fonctionnalités par implémentation DirectAccess	219
Administration d'un poste connecté en DirectAccess	220
 CHAPITRE 11	
Windows To Go – Un environnement de travail vraiment mobile	223
Fonctionnement	223
Différences entre Windows To Go et une installation classique	224
Scénarios d'utilisation de Windows To Go	225
Prestataires	225
Bring Your Own Device	225
Voyager léger/télétravailler	225
PC partagés/libre-service	226
Quelques considérations à prendre en compte	226
Quelles sont les configurations matérielles compatibles ?	226
Quid des données de l'utilisateur ?	227
Comment ces espaces de travail vont-ils être administrés ?	227
Création d'un support Windows To Go	227
Windows To Go et Windows Store	233
 Glossaire	237
Index	241