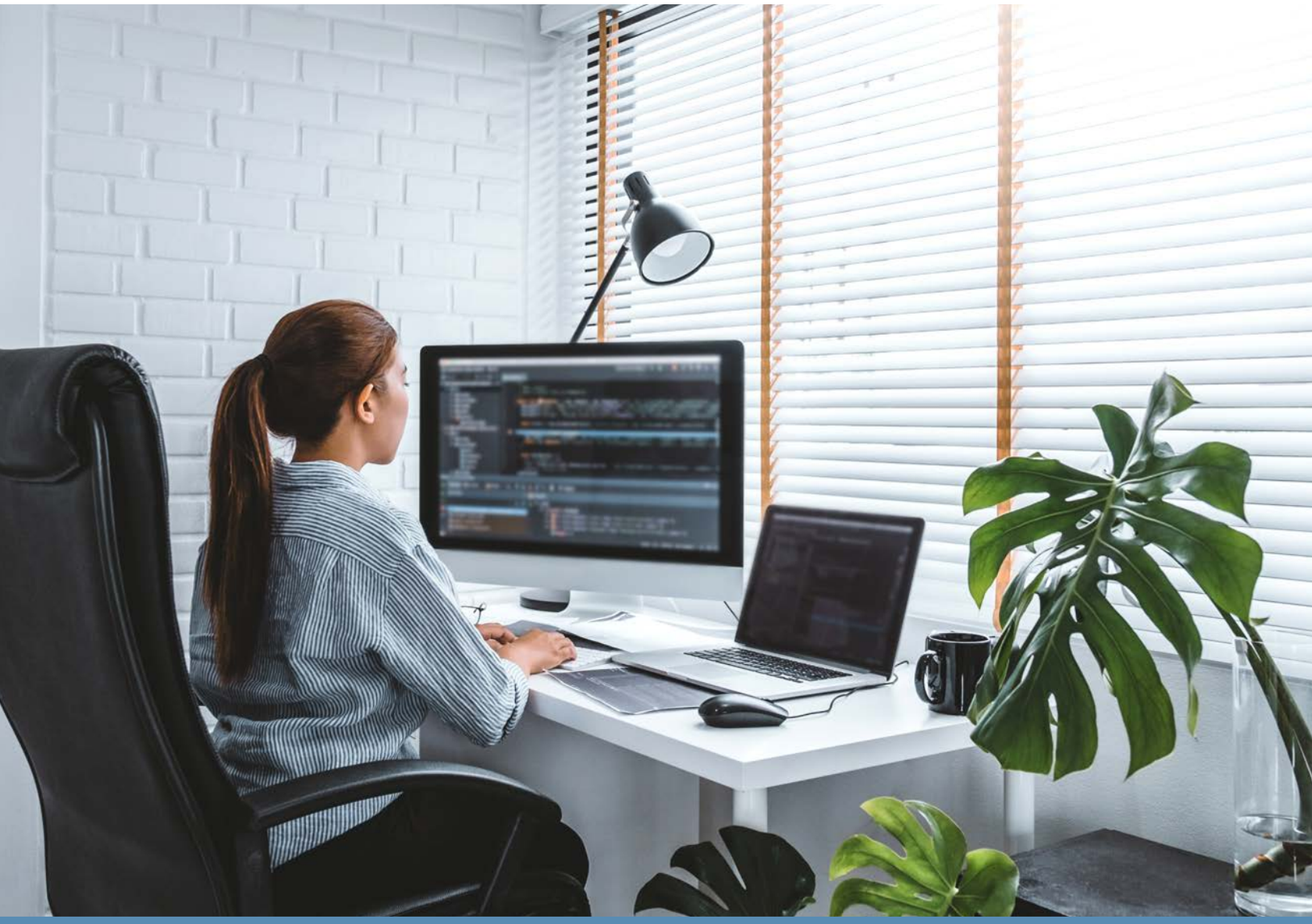
En partenariat avec



| EBOOK

GÉNÉRALISATION DU TÉLÉTRAVAIL : RETOUR SUR LES BASES POUR UN DÉPLOIEMENT EN TOUTE SÉCURITÉ

Découvrez comment Microsoft 365 + Veeam Backup for *Microsoft Office 365* s'associent pour répondre aux exigences du travail à distance

INTRODUCTION

2020 a vu le déploiement massif du télétravail avec le contexte sanitaire, obligeant ainsi les services informatiques à équiper et connecter leurs collègues en un temps record pour maintenir au mieux l'activité. Néanmoins, la généralisation du télétravail perçue au début comme une solution provisoire, est amenée à perdurer, faisant du travail à distance non pas un objectif court-terme mais bien une vision long-terme.

Une étude du Gartner publiée en Juillet 2020 montre ainsi que 48% des employés vont continuer à travailler à distance au moins partiellement dans un monde post-COVID, contre 30% avant la pandémie.*

Il s'agit donc pour les responsables informatiques de pérenniser une pratique souvent mise en place de façon réactive. Notre objectif chez Bechtle en tant que conseiller IT est donc d'accompagner dans la durée les entreprises dans leur réflexion autour de cette nouvelle organisation du travail.

La première étape consiste à déployer une solution qui combine mobilité et sécurité afin de permettre aux employés de continuer leur activité en alternant entre présence sur site et télétravail, sans compromettre la sécurité de l'entreprise et de ses données.

Il s'agit là d'un besoin crucial auquel répond Microsoft en positionnant ses solutions cloud Microsoft 365 pour les PME mais aussi pour les grandes entreprises. L'élément clé dans le déploiement sécurisé du télétravail est le module Enterprise Mobility + Security (EMS) inclus dans les plans Microsoft 365 E3 et Microsoft 365 E5, ou disponible en add-on. Ce module permet de déployer le télétravail de façon sécurisée pour l'ensemble des collaborateurs en permettant à la fois la gestion des terminaux et la protection contre les menaces et risques cyber.

Néanmoins s'il est une chose sur laquelle Microsoft n'agit pas, c'est la responsabilité des données à proprement parler (Microsoft, de par son SLA - Service Level Agreement - garantit l'accès aux données mais pas l'intégrité de celles-ci). En effet, il revient aux organisations de protéger et sauvegarder leurs données en cas de perte accidentelle ou malveillante. C'est là qu'intervient Veeam avec sa solution Veeam Backup for *Microsoft Office 365* permettant le backup et la restauration des données Office 365 (incluant les données Teams).

En combinant Microsoft 365 + Veeam Backup for *Microsoft Office 365*, les organisations assurent ainsi la continuité de leurs activités en cas de recours durable au télétravail, sans pour autant compromettre la sécurité de leurs données.

Ce livre blanc présente donc les avantages à associer ces deux solutions et retrace les principales étapes à suivre pour les mettre en place de façon simple et efficace.

** Etude Gartner « How the Remote Work Revolution Will Change the Employer-Employee Relationship », 9 Juillet 2020.*

Sommaire

1.
MICROSOFT 365 + VEEAM BACKUP FOR *MICROSOFT OFFICE 365*. LA SOLUTION OPTIMALE

Présentation de Microsoft 365

Il existe de nombreux plans Microsoft, mais seulement trois incluent le module EMS nécessaire au déploiement sécurisé du télétravail :

< 300 utilisateurs	> 300 utilisateurs	
Microsoft 365 Business Premium	**Microsoft 365 E3**	**Microsoft 365 E5**
Microsoft 365 Business Standard Windows 10 Pro **Fonctionnalités Enterprise Mobility + Security (EMS) :** Azure Active Directory Premium P1 Information Protection Microsoft Intune : gestion des appareils et applications	Office 365 E3 Windows 10 Enterprise E3 Enterprise Mobility + Security (EMS) E3	Office 365 E5 Windows 10 Enterprise E5 Enterprise Mobility + Security (EMS) E5

> Les licences M365 E3 et E5 vous permettent de couvrir les licences d'accès client ainsi que les serveurs « On Prem » pour Exchange et SharePoint.
>
> Franck Pelloux
> Spécialiste Cloud Microsoft

Le module EMS peut également être acheté en add-on aux plans Office 365. Le module EMS se décline en deux versions : EMS E3 et EMS E5.

EMS E3	EMS E5
Azure Active Directory Premium P1 **Microsoft Intune : gestion des appareils et applications** Information Protection Microsoft Advanced Threat Analytics (ATA) **Windows Server CAL rights**	EMS E3 + Azure Active Directory Premium P2 Rule-based Classification Microsoft Cloud App Security Azure Advanced Threat Protection (ATP)

Un élément-clé du module EMS est la fonctionnalité Azure Active Directory (Azure AD) Premium, qui existe là encore en 2 versions : P1 et P2. Il est également possible d'acheter les modules Azure AD Premium en add-on.

Azure Active Directory est un service de gestion des identités et accès permettant aux employés d'accéder aux ressources Microsoft 365, Azure, et autres applications SaaS, mais également aux ressources internes hébergées sur le réseau d'entreprise, intranet et autres applications cloud de votre organisation.

Azure AD Premium P1	Azure AD Premium P2
• Changement des mots de passe en libre-service (SSPR) • SSO illimité (SSO pour applications tierces) • Accès aux ressources hybrides et cloud • Microsoft Identity Manager : définition de règles d'accès pour les utilisateurs • Authentification multifacteur (MFA) avancée : vérification de l'identité par SMS ou appel téléphonique • Accès conditionnel classique	Azure AD Premium P1 + **Azure AD Identity Protection :** • Accès conditionnel incluant détection automatique et correction des risques liés à l'identité (ex : connexion depuis une adresse IP anonyme ou à partir d'un emplacement inhabituel, fuite d'identifiants sur le darkweb) • Génération de rapports d'analyse approfondie des risques **Azure AD Privileged Identity Management:** • Limitation des accès administrateurs aux ressources de l'entreprise grâce à la définition de rôles, durées d'accès et politiques de MFA poussées

> Pour se sécuriser au niveau des liens, pièces jointes et le phishing vous pouvez souscrire à l'offre Microsoft Defender for Office 365 Plan 1. Cette offre est incluse dans Microsoft 365 Business Premium et Microsoft E5 mais doit être souscrite en add-on pour le plan Microsoft E3.
>
> Franck Pelloux
> Spécialiste Cloud Microsoft

Les plans Microsoft 365 E3 et E5 incluant EMS offrent donc aux utilisateurs à la fois une grande mobilité grâce à la gestion de vos périphériques via Intune, mais également une sécurité renforcée contre les menaces et comportements suspects.

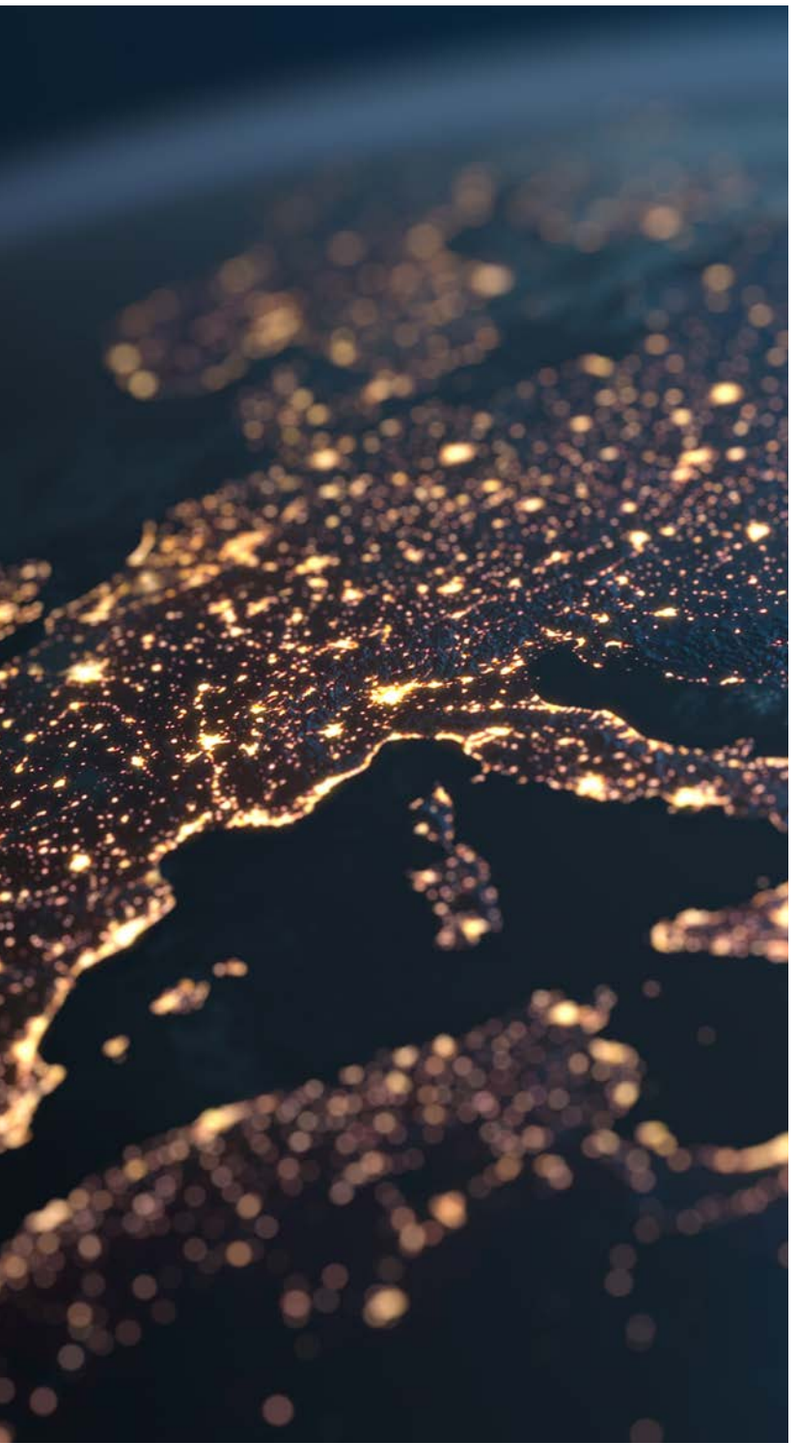
Malgré la sécurité renforcée proposée dans les différents plans et modules Microsoft, les entreprises restent responsables de leurs données. Il est donc de leur ressort de se prémunir contre les risques de perte de données accidentelles ou malveillantes.

C'est ici que Veeam Backup for *Microsoft Office 365* prend tout son sens.

Présentation de Veeam Backup for *Microsoft Office 365*

Contrairement aux idées reçues, Microsoft n'est pas responsable de vos données et prend seulement en charge l'architecture. En effet, même s'il est possible de mettre en place une stratégie de rétention des données, les options proposées par Microsoft ne constituent pas une solution de sauvegarde complète dans la durée. Par conséquent, il revient aux entreprises d'assurer la protection de leurs données en cas d'attaque de ransomware ou de suppression accidentelle ou malveillante. Cette protection des données est cruciale, faisant ainsi du backup la couche ultime en matière de sécurité pour les entreprises.

Les 7 raisons pour lesquelles sauvegarder Office 365 est essentiel :



- Suppression accidentelle
- Lacunes et imprécision dans la stratégie de rétention
- Menaces de sécurité internes
- Menaces de sécurité externes
- Obligations légales et exigences de conformité
- Gestion des déploiements de messagerie hybride et des migrations vers Office 365
- Structure des données Teams

Leader sur le marché du back up depuis plusieurs années, Veeam propose une solution simple et efficace permettant de sauvegarder et restaurer les données Office 365. Il est ainsi possible de protéger les données Exchange (on-prem et online), SharePoint (on-prem et online), OneDrive for Business et Teams.

Ces différentes données peuvent ensuite être stockées soit dans le cloud (stockage objet), soit on-prem.

La restauration des données se fait elle de façon granulaire grâce aux différentes applications permettant de retrouver et restaurer uniquement les données souhaitées. Ces applications incluent :

- Veeam Explorer pour Microsoft Exchange pour les boîtes mails ;
- Veeam Explorer pour Microsoft SharePoint pour les fichiers et dossiers personnels ;
- Veeam Explorer pour Microsoft OneDrive pour les fichiers d'entreprise ; et
- Veeam Explorer pour Microsoft Teams pour les données Teams incluant canaux et équipes.

> Au-delà de la couche sécuritaire supplémentaire, Veeam Backup for *Microsoft Office 365* remplit également un rôle primordial au niveau des exigences de conformité. En effet, en offrant la possibilité de définir des règles de rétention des données sur le long terme, vous répondez ainsi aux obligations légales qui sont imposées par les différentes législations.
>
> Abdelkader Ait Ali
> Spécialiste Backup et Virtualisation

En combinant Microsoft 365 + Veeam Backup for Microsoft Office 365, vous maximisez donc la protection de vos données et réduisez ainsi drastiquement vos risques en matière de sécurité et conformité.

Mais concrètement, une fois la décision prise d'opter pour ces deux solutions, comment tirer au mieux parti des fonctionnalités de chacune pour obtenir un environnement de travail à la fois sécurisé et simple à gérer pour les administrateurs ?

2.
LES ETAPES DU DEPLOIEMENT DE LA SOLUTION MICROSOFT 365 + VEEAM BACKUP FOR *MICROSOFT OFFICE 365*

Etape 1 : Sécuriser la connexion à distance

Il s'agit ici de mettre en place l'authentification multifacteur (MFA) via Azure Active Directory, fonctionnalité incluse dans le module EMS.

L'authentification multifacteur consiste à vérifier l'identité de l'utilisateur lors d'une connexion en faisant appel à une seconde vérification d'identité. Ainsi le mot de passe n'est plus suffisant pour se connecter, il faut également entrer un code SMS envoyé sur son portable ou répondre à un appel sur son téléphone.

> Microsoft va plus loin en proposant l'authentification passwordless (sans mot de passe) via les méthodes suivantes :
>
> - Reconnaissance faciale avec Windows Hello
> - Empreinte digitale avec l'utilisation de la clé de sécurité FIDO2
> - Génération de codes temporaires via l'application Microsoft Authentificator
>
> Chrisross Abouo
> Spécialiste Cybersécurité

Il revient aux administrateurs IT de déterminer les règles de MFA qu'ils souhaitent mettre en place selon les possibilités offertes par Azure AD Premium :

Azure AD Premium P1	Azure AD Premium P2
Instaurer l'authentification MFA pour les administrateurs uniquement Instaurer l'authentification MFA pour tous les utilisateurs	Azure AD Premium P1 + Déclencher l'authentification MFA en cas de risque de connexion moyen ou élevé Bloquer les clients sans MFA moderne Exiger le changement des mots de passe à risque

> Quelques fonctionnalités de base MFA (ex: application mobile comme 2e facteur de vérification) sont disponibles par défaut dans les plans suivants : Office 365 E1, Office 365 E3, Office 365 E5, Office 365 F3.
>
> Néanmoins nous recommandons de mettre en place une politique MFA plus poussée permise par la fonctionnalité Azure AD Premium P1 ou P2.
>
> Franck Pelloux
> Spécialiste Cloud Microsoft

Etape 2 : garantir l'accès à distance des applications on-prem

Même si la tendance est de plus en plus aux applications hébergées dans le cloud (Saas), de nombreuses organisations continuent d'héberger des applications sur des serveurs on-prem.

Il s'agit donc ici de continuer à accéder à ces applications même en dehors de l'entreprise.

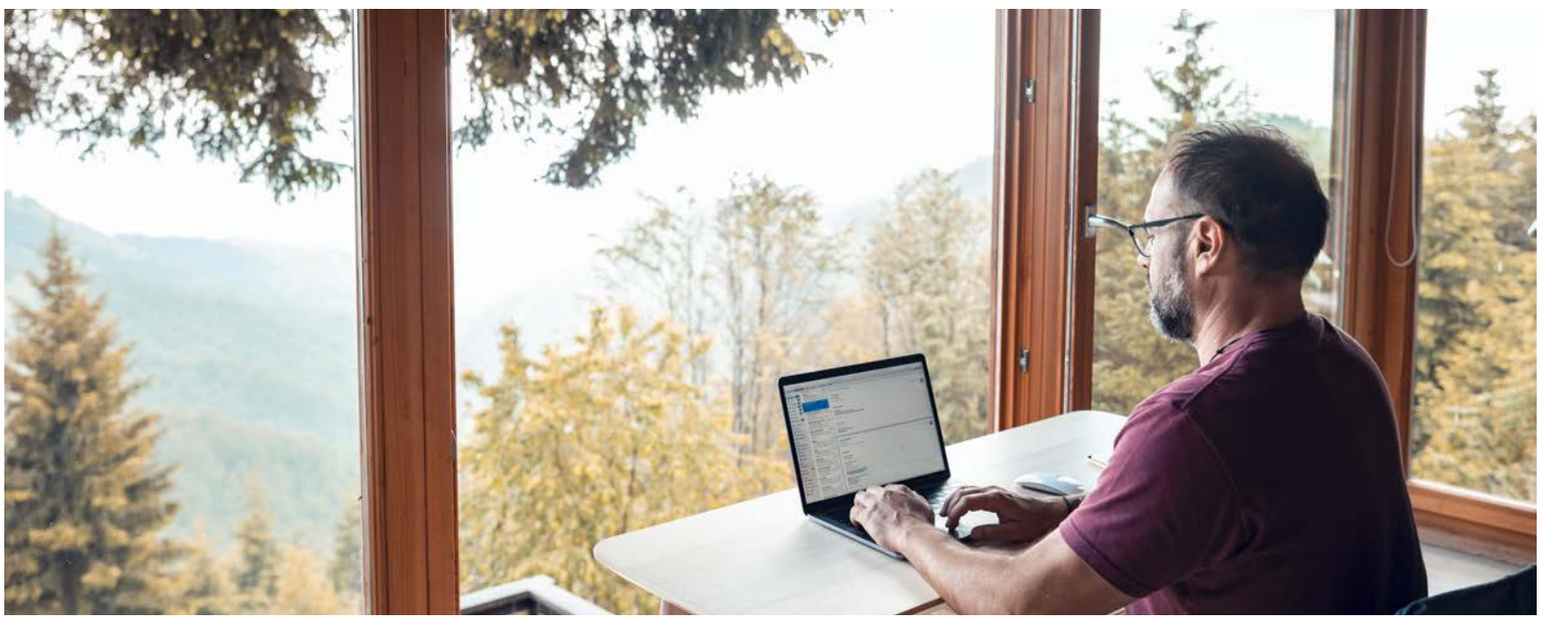
Plusieurs configurations sont possibles selon votre cas de figure :

VOUS AVEZ UNE SOLUTION VPN EXISTANTE

Utilisation du VPN existant et segmentation de tunnel pour optimiser le trafic cloud Microsoft 365 et réduire la latence

VOUS N'AVEZ PAS DE SOLUTION VPN EXISTANTE

Toutes vos applications sont des applications web et vos comptes d'utilisateurs et groupes locaux sont synchronisés avec Azure AD	Vous avez des applications qui ne sont pas des applications web	Vos collaborateurs utilisent leurs ordinateurs personnels
Utilisation du proxy d'application Azure AD pour accéder aux applications web hébergées sur des serveurs intranet locaux *Note : le proxy d'application Azure AD n'est pas inclus dans Microsoft 365 et doit être acheté séparément avec un abonnement Azure distinct*	Utilisation d'un réseau privé virtuel (P2S) Azure qui crée une connexion sécurisée entre un appareil de travail distant et le réseau de votre organisation *Note : Azure P2S VPN n'est pas inclus dans Microsoft 365 et doit être acheté séparément avec un abonnement Azure distinct*	Utilisation de l'application Windows Virtual Desktop *Note : Windows Virtual Desktop n'est pas inclus dans Microsoft 365 et doit être acheté séparément avec un abonnement Azure distinct*



Etape 3 : Configurer les modules de sécurité et conformité

Il s'agit là d'une étape-clé qui consiste dans un premier temps à configurer les modules de sécurité inclus dans vos licences Microsoft 365, puis de définir des règles en matière de conformité propres à vos enjeux métiers et obligations légales.

Configuration des modules de sécurité Microsoft inclus dans vos plans Microsoft 365

Un fois vos licences déployées il vous faut configurer les différents modules de sécurité disponibles pour garantir une sécurité maximale de votre environnement de travail.

	ACTION	LICENCES REQUISES
Protection contre les menaces Protection contre les URL et les fichiers malveillants dans les e-mails et les documents Microsoft Office 365	Configuration de Microsoft Defender pour Office 365	*Plans :* • Microsoft 365 E5 • Microsoft 365 Business Premium *Add-ons :* • Microsoft 365 E5 Security • Microsoft Defender pour Office 365 P1
Protection contre les menaces Protection contre les cyberattaques et programmes malveillants sur les terminaux	Configuration de Microsoft Defender for Endpoint (incluant Microsoft Defender Antivirus)	*Plan :* • Microsoft 365 E5 *Add-ons:* • Microsoft 365 E5 Security • Microsoft Defender for Endpoint
Protection des identités Identification et détection des comportements suspects	Configuration de Microsoft Defender for Identity	*Plan :* • Microsoft 365 E5 *Add-on :* • Microsoft 365 E5 Security
Protection des terminaux et gestion des accès Gestion des PCs et terminaux mobiles avec mise en place de politiques d'accès conditionnels	Configuration d'Intune pour les PCs et Intune Mobile App pour les téléphones portables et tablettes	*Plans :* • Microsoft 365 E5 • Microsoft 365 E3 • Microsoft 365 Business Premium

Configuration des modules de conformité Microsoft inclus dans vos plans Microsoft 365

Qu'il s'agisse de règlementations externes ou internes, Microsoft 365 vous permet de définir et mettre en application votre politique de conformité selon les objectifs fixés.

	ACTION	LICENCES REQUISES
Classification et protection des données Mise en place d'étiquettes de confidentialité pour les messages, documents et sites alertant les utilisateurs du caractère sensible des données manipulées	Configuration de l'ensemble de la politique de conformité dans le centre de conformité Microsoft 365	*Plans :* • Microsoft 365 E5 • Microsoft 365 E3
Protection contre la perte de données Détection et prévention des partages de données à risque		
Contrôle d'application d'accès conditionnel Blocage des téléchargements de données sensibles sur les appareils personnels des utilisateurs		
Stratégie de rétention des données Définition des modalités de stockage et durée de rétention de certaines données clients		
Chiffrement des messages contenant des données sensibles Chiffrement de messages internes et externes contenant des données réglementées (ex : données clients)		

La liste des fonctionnalités présentées ici n'est pas exhaustive – n'hésitez pas à contacter nos experts Microsoft pour toute question supplémentaire.

Etape 4 : Protéger les données

Comme expliqué précédemment, Microsoft n'est pas responsable des données en tant que telles. Il revient donc aux entreprises de mettre en place elles-mêmes des solutions de sauvegarde de leurs données pour pallier les risques de sécurité et répondre aux exigences en matière de conformité.

En déployant Veeam Backup for *Microsoft Office 365* pour vos collaborateurs équipés de Microsoft 365, vous obtenez un environnement de télétravail sécurisé optimal.

Il vous faudra pour cela déployer une licence Veeam Backup for *Microsoft Office 365* par utilisateur Microsoft 365, puis installer les modules Veeam Explorer qui vous permettront ensuite de définir les politiques de rétention incluant durée, emplacement et fréquence des données sauvegardées. C'est également à partir de Veeam Explorer que vous pourrez en quelques minutes seulement restaurer les éléments supprimés d'un collaborateur, qu'il s'agisse par exemple d'emails, de fichiers Office 365 ou encore de dossiers Microsoft Teams.

Une fois vos données Office 365 protégées il vous faut gérer les terminaux utilisés dans le cadre du télétravail, qu'il s'agisse de PCs personnels ou fournis par l'entreprise.

Etape 5 : Gérer les périphériques (PCs, tablettes et mobiles)

Les terminaux utilisateurs (ordinateurs et tablettes personnels, téléphones portables) constituent un point d'entrée fréquent pour les attaques et doivent donc être intégrés dans une gestion globale des terminaux par les équipes IT.

Avec Microsoft 365, c'est le module Microsoft Endpoint Manager qui remplit ce rôle. Les 2 principaux éléments nécessaires au déploiement sécurisé du télétravail sont :

Windows Autopilot

Pour les nouveaux PCs, Autopilot permet le déploiement et la configuration de Windows de façon simple et rapide.

Microsoft Intune

- Pour les appareils existants fournis par l'entreprise, Intune permet aux équipes IT de définir et déployer des règles et paramètres de sécurité ;

- Pour les appareils personnels, les équipes IT peuvent définir des règles d'accès à certaines applications reposant sur l'authentification multifacteur. Il s'agit là d'une alternative pour les utilisateurs ne souhaitant pas inscrire leur appareil personnel dans Intune.

Microsoft Intune constitue donc un pilier majeur dans la sécurisation du travail à distance puisqu'une fois les configurations faites au niveau sécurité et conformité (voir étape 3), Intune permet le déploiement de ces paramètres à l'ensemble des terminaux actifs au sein d'une entreprise.

Etape 6 : Quelle application pour quel usage ?

Une fois l'environnement sécurisé, vos utilisateurs n'ont plus qu'à continuer à utiliser les applications Office 365 avec lesquels ils sont déjà peut être familiers :

- Microsoft Teams pour la collaboration et les réunions internes ou externes ;
- Outlook pour la messagerie électronique ;
- SharePoint et OneDrive pour le stockage et partage de fichiers ;
- Applications Office 365 : Word, Excel, PowerPoint.

Cependant force est de constater que l'environnement utilisateur Microsoft 365 est riche de possibilités. Par conséquent il est souvent recommandé de définir en amont une politique de gouvernance adaptée à vos enjeux métiers, et d'en décliner ensuite un plan d'adoption, l'objectif étant d'assurer une transition efficace entre travail sur site et travail à distance.

Chez Bechtle Comsoft nos consultants proposent des missions sur-mesure pour évaluer vos besoins en matière de gouvernance et d'adoption, afin de vous accompagner au mieux dans le déploiement de vos outils Microsoft.

Mission Immersion 365

Atelier online ou en présentiel d'une demi-journée destiné à mettre en pratique les fonctionnalités d'Office 365 et les nouveautés à partir de cas d'usage métiers et incluant des mises en situation en environnement de démo.

Mission Gouvernance 365

Atelier online ou en présentiel permettant d'identifier les forces et faiblesses de la gouvernance des outils Microsoft 365 pour développer un meilleur contrôle sur ces outils à l'aide de bonnes pratiques.

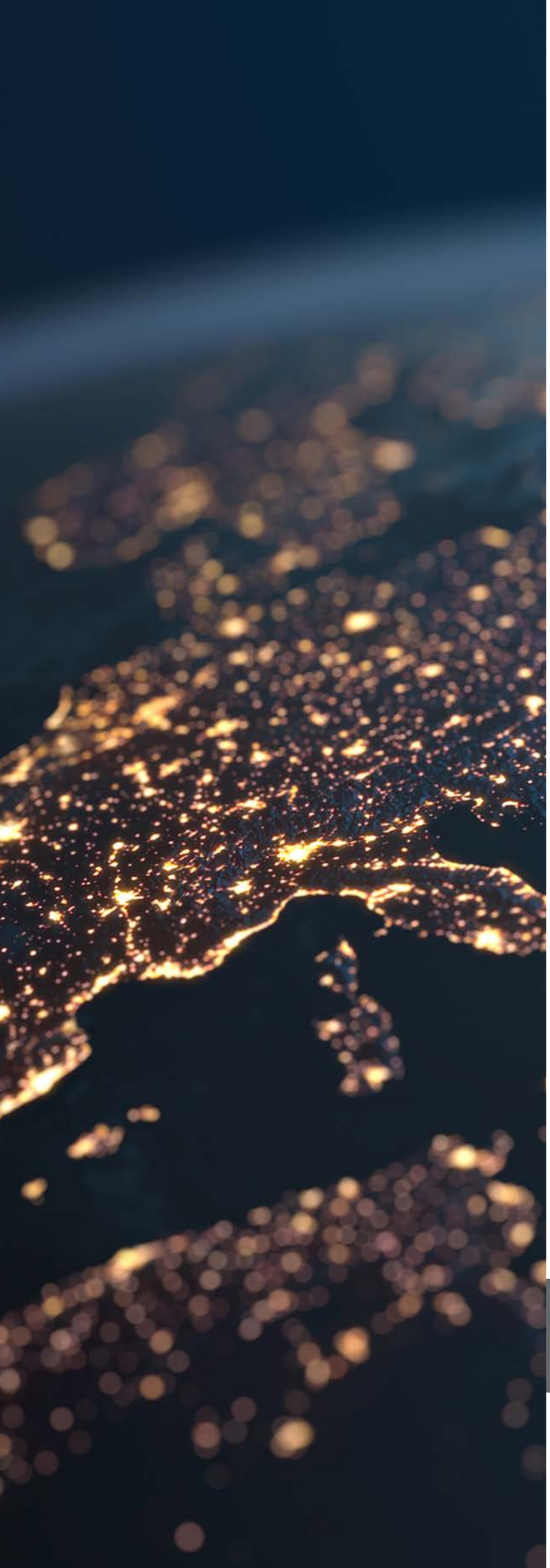
Nos experts vous accompagnement également dans l'analyse de vos besoins en matière de sécurité et protection des données :

Mission Cybersecurity Infrastructure

Evaluation des risques de cybersécurité pour vos actifs Microsoft (terminaux, Microsoft Active Directory, Azure AD et Office 365) et proposition de correctifs pour sécuriser votre environnement Microsoft.

Mission Data Protection Assessment

Atelier online ou en présentiel d'une demi-journée permettant de comprendre les besoins en matière de protection des données dans Office 365 et de définir une stratégie de protection des données Office 365 dans le Cloud.



A l'heure où le télétravail est largement répandu, il convient de valider l'approche mise en place au sein de votre entreprise.

En combinant Microsoft 365 + Veeam Backup for *Microsoft Office 365*, les entreprises bénéficient d'une solution optimale qui leur permet d'offrir un environnement de travail sécurisé à leurs collaborateurs.

Pour en savoir plus, n'hésitez pas à contacter nos experts :

Franck PELLOUX
Spécialiste Cloud Microsoft
+33 4 97 21 58 54
franck.pelloux@comsoft.fr

Chrisross ABOUO
Spécialiste Cybersécurité
+33 1 53 38 19 86
chrisross.abouo@comsoft.fr

AbdelKader AIT ALI
Spécialiste Backup et Virtualisation
+33 1 53 38 16 57
abdelkader.aitali@comsoft.fr

Alexia MAMBOUCKA
Spécialiste Teams et adoption Microsoft 365
+33 1 53 38 20 77
alexia.mamboucka@comsoft.fr

Gold Microsoft Partner
Microsoft

veeam GOLD propartner

216 avenue Jean Jaurès, 75019 Paris
+33 1 53 38 20 50
www.bechtle-comsoft.fr

BECHTLE COMSOFT