Monitoring Sécurité
Pack Premium Be-Cloud

20% des entreprises ont déjà subis un **préjudice supérieur à 50K €**

6 entreprises sur 10 **n'ont pas de budget** spécifique **pour lutter** contre la fraude et la menace cyber

53% des entreprises ont connu en moyenne **5 tentatives de fraudes** en 2020

Plus que jamais, la sécurité, la protection de vos données, de vos identités, doit être au cœur de votre système d'information.

Le Pack Be-Cloud Premium prend en compte le traitement des alertes standard configurées par Microsoft dans le centre de Sécurité et Conformité de votre tenant Microsoft Office 365.

Ces dernières sont redirigées vers notre support sécurité via un compte mail de votre tenant dédié et sécurisé*.

Nous gérons pour vous l'ensemble de ces alertes en vous les signalant, en vous les expliquant et en les traitant.

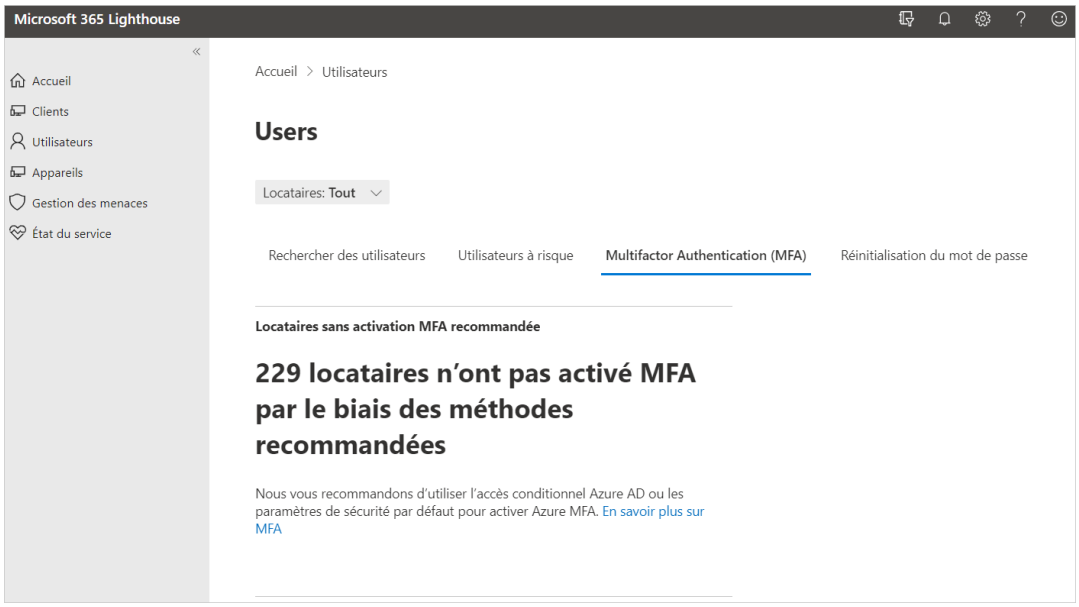
Be-Cloud assure également votre sécurité, au quotidien, sur les potentielles menaces visant votre parc informatique (virus, malware, etc.) ainsi que les accès utilisateurs à votre système d'information (Authentification multi-facteur – MFA) depuis un portail dédié Microsoft.

*nécessite une licence Exchange

Contrôle sécurité

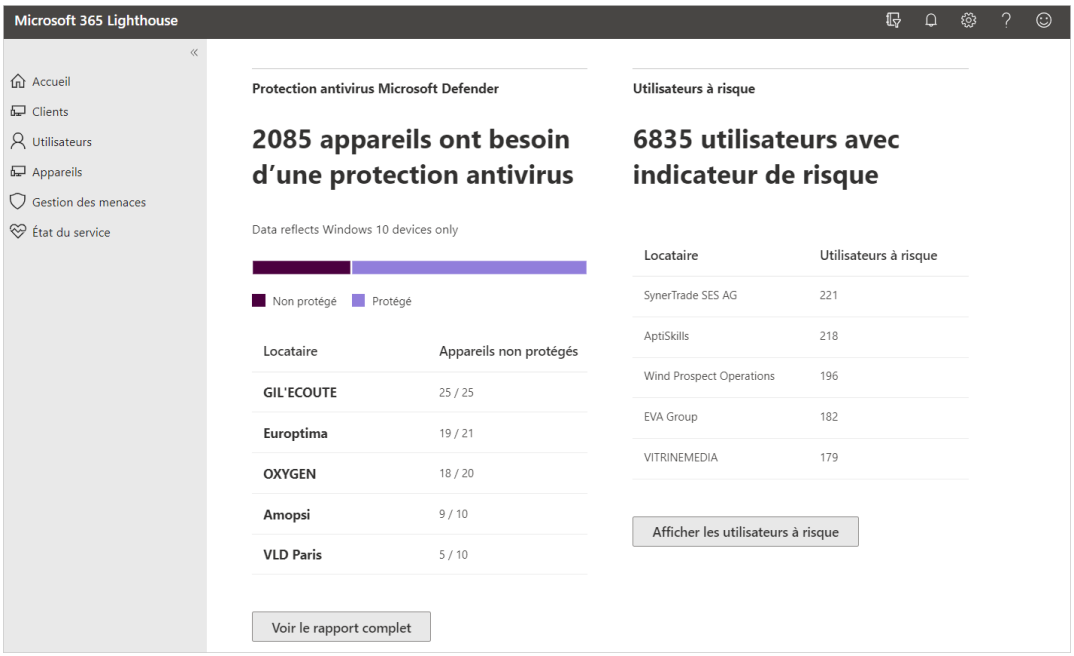
Contrôle de l'authentification multi-facteur

99% des comptes utilisateurs piratés ne disposaient pas de l'authentification multi-facteur. Be-Cloud et Microsoft conseillent fortement à l'ensemble de leurs clients d'utiliser cette méthode de protection de d'identité.
Dans ce cadre, nous vérifions, très régulièrement que nos clients et leurs utilisateurs sont bien protégés par cette méthode.



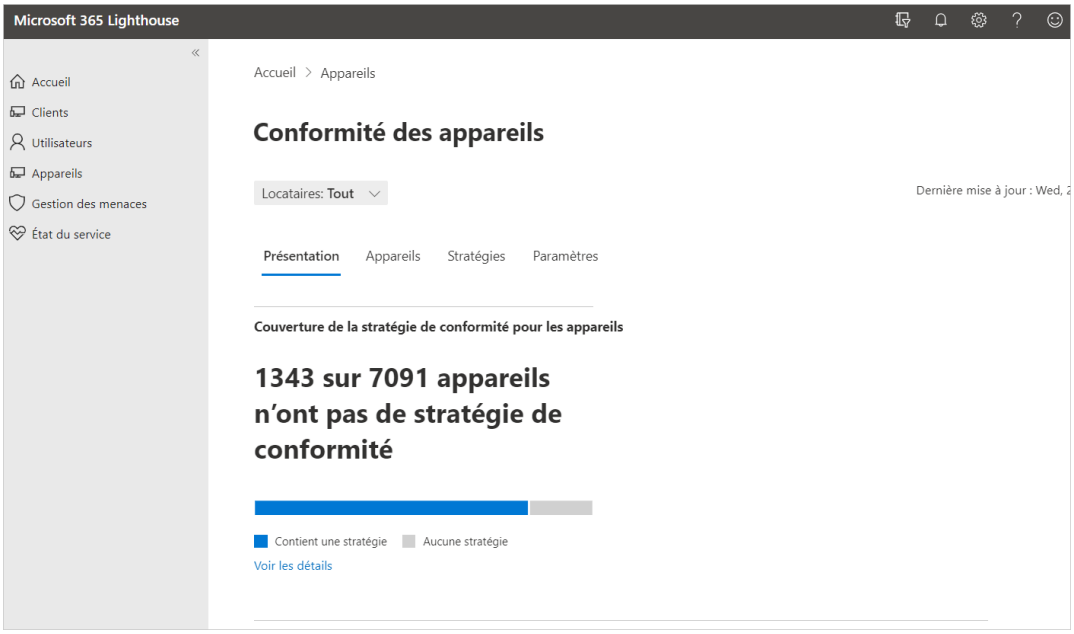
Contrôle de la protection des menaces dans l'antivirus Microsoft Defender et de la mise à jour de Microsoft Defender

Les tentatives de piratages via des virus, des ransomware, des chevaux de Troie, etc, concernent également les terminaux (PC, smartphones) utilisés pour accéder aux systèmes d'informations des organisations. Windows 10 intègre un antivirus complet et performant Microsoft Defender qui permet entre autres de protéger l'utilisateur contre les menaces actives (virus, des ransomware, des chevaux de Troie, etc.). Be-Cloud contrôle régulièrement que Microsoft Defender est à fonctionnel et à jour.



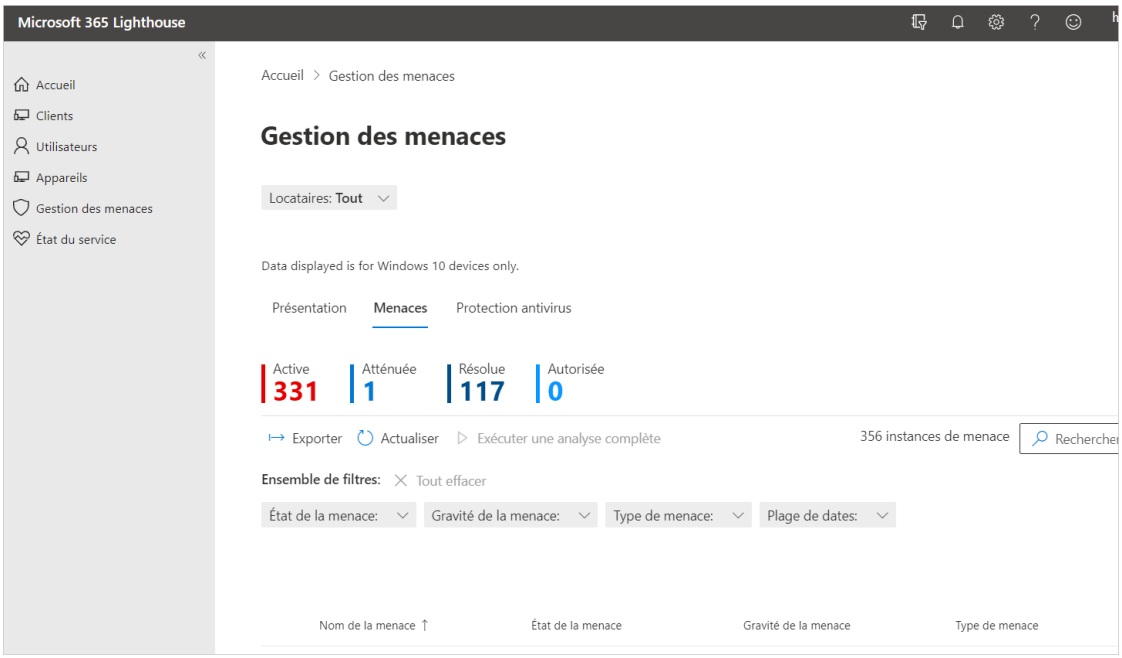
Contrôle de la conformité de votre parc informatique.

Pour éviter les intrusions et les vols de données, les matériels ayant accès à votre système d'information doivent, en fonction de stratégies de sécurité, être reconnus comme conformes. Be-Cloud contrôle régulièrement que l'ensemble de vos matériels sont conformes à vos stratégies de sécurité et peuvent ainsi accéder à vos données en toute sécurité.



Gestion et traitement des alertes de sécurité

Le traitement de certaines alertes pourra nécessiter un accès à votre tenant avec des droits d'administration. Nous notifions par mail le signataire du contrat de toutes les alertes reçues et de l'ensemble des actions menées afin d'en assurer le traitement. Ces alertes couvrent une partie de la sécurité de votre système d'information. Afin de garantir l'intégrité et la pérennité de votre système d'information, nous vous conseillons de suivre le parcours de sécurité* dans son intégralité. Vous trouverez à la suite une liste non exhausive des alertes en standard que nous traiterons.



Liste des alertes de sécurité

Stratégies d'alertes en standard :

Suspicious email sending patterns detected
Détection de modèles suspects d'envoi de courriels

Elevation of Exchange admin privilege
Elévation du privilège d'administration d'Exchange

Email messages containing malware removed after delivery
Messages électroniques contenant des logiciels malveillants supprimés après la livraison

Malware campaign detected and blocked
Campagne de logiciels malveillants détectée et bloquée

Email reported by user as malware or phish
Courriel signalisé par l'utilisateur comme étant un logiciel malveillant ou un phish

Unusual volume of file deletion
Volume inhabituel de suppression de fichiers

Unusual external user file activity
Activité inhabituelle dans les fichiers d'utilisateurs externes

Liste des alertes de sécurité

Stratégies d'alertes en standard :

eDiscovery search started or exported
Recherche eDiscovery lancée ou exportée

Malware campaign detected in SharePoint and OneDrive
Campagne de logiciels malveillants détectée dans SharePoint et OneDrive

Creation of forwarding/redirect rule
Création d'une règle de réexpédition/réacheminement

User restricted form sending email
Utilisateur restreint dans l'envoi de courriels

Unusual increase in email reported as phish
Augmentation inhabituelle du nombre de courriels signalés comme étant du hameçonnage

Unusual volume of external file sharing
Volome inhabituelle de partage de fichiers externes

Email messages containing phish URLs removed after delivery
Messages électroniques contenant des URL de phish supprimés après la livraison

Messages have been delayed
Les messages ont été retardés

Tenant restricted from sending email
Interdiction d'envoyer des courriels aux locataires

Malware campaign detected after delivery
Campagne de logiciels malveillants détectée après la livraison

A potentially malicious URL click was detected
Un clic d'URL potentiellement malveillant a été détecté