Préparer le déploiement de Microsoft Defender ATP

03/04/2020 • 5 minutes de lecture •

Dans cet article

Parties prenantes et déconnexion
Environnement
Contrôle d'accès basé sur les rôles
Ordre d'adoption
Étape suivante

S'applique à:

- Microsoft Defender– Protection avancée contre les menaces (MicrosoftDefender ATP)

Le déploiement de Microsoft Defender ATP est un processus en trois étapes:

Phase 1: préparation

Phase 2: configuration

Étape 3: intégration

Vous êtes actuellement dans la phase de préparation.

La préparation est la clé du déploiement réussi. Dans cet article, vous serez guidé sur les points que vous devez prendre en considération lorsque vous préparez le déploiement de Microsoft Defender ATP.

Parties prenantes et déconnexion

La section suivante permet d'identifier toutes les parties prenantes impliquées dans le projet et dont vous devez vous déconnecter, revoir ou rester informé.

Ajoutez des parties prenantes dans le tableau ci-dessous en fonction de votre organisation.

- DONC = connexion à ce projet
- R = revoir ce projet et entrer une information
- J'ai connaissance du projet

Nom	Rôle	Action
Entrez le nom et l'adresse de courrier	**Chief Information Security officier (CISO)** est *un représentant exécutif qui sert de sponsor au sein de l'Organisation pour le déploiement de la nouvelle technologie.*	AFIN
Entrez le nom et l'adresse de courrier	Le **Centre d'opérations de cyber Defense (Cdoc)** est *un représentant de l'équipe Cdoc chargé de définir la façon dont cette modification est alignée avec les processus de l'équipe opérations de sécurité du client.*	AFIN
Entrez le nom et l'adresse de courrier	**Architecte** de la sécurité responsable de *l'équipe de sécurité chargée de définir le mode d'alignement de ce changement avec l'architecture de sécurité principale de l'organisation.*	R
Entrez le nom et l'adresse de courrier	**Architecte** de lieu de travail , *un représentant de l'équipe informatique chargée de définir le mode d'alignement de ce changement avec l'architecture de l'espace de travail principal au sein de l'organisation.*	R
Entrez le nom et l'adresse de courrier	**Analyste** *de la sécurité un représentant de l'équipe Cdoc qui peut fournir des informations sur les fonctionnalités de détection, l'utilisation de l'utilisateur et l'utilité globale du changement du point de vue des opérations de sécurité.*	Ma

Environnement

Cette section est utilisée pour s'assurer que votre environnement est compris par les parties prenantes qui vous aideront à identifier les dépendances

potentielles et/ou les modifications requises dans les technologies ou les processus.

Quoi?	Description
Nombre de points de terminaison	
Nombre de serveurs	
Moteur de gestion	
Distribution CDOC	
Événements et informations de sécurité (SIEM)	

Contrôle d'accès basé sur les rôles

Microsoft recommande l'utilisation du concept de privilèges minimum. Microsoft Defender ATP tire parti des rôles intégrés d'Azure Active Directory. Microsoft recommande de passer en revue les différents rôles disponibles et d'en choisir un en fonction de votre besoin pour chaque personnage. Il est possible que certains rôles doivent être appliqués temporairement et supprimés une fois le déploiement terminé.

Personnages	Rôles	Rôle Azure AD (si nécessaire)	Affecter à
Administrateur de la sécurité			
Analyste de sécurité			
Administrateur de point de terminaison			
Administrateur d'infrastructure			
Propriétaire de l'entreprise/partie prenante			

Microsoft recommande l'utilisation de la gestion des identités privilégiées pour gérer vos rôles et fournir des contrôles d'audit, de contrôle et d'accès supplémentaires pour les utilisateurs disposant d'autorisations d'annuaire.

Microsoft Defender ATP prend en charge deux méthodes de gestion des autorisations:

- **Gestion des autorisations de base**: définir les autorisations sur accès complet ou lecture seule. Dans le cas des utilisateurs de gestion des autorisations de base ayant le rôle d'administrateur général ou d'administrateur de sécurité dans Azure Active Directory, ils disposent d'un accès total lorsque le rôle du lecteur de sécurité a accès en lecture seule.

- **Contrôle d'accès basé sur les rôles (RBAC)**: définir des autorisations granulaires en définissant des rôles, en attribuant des groupes d'utilisateurs Azure ad aux rôles et en accordant aux groupes d'utilisateurs l'accès à des groupes d'ordinateurs. Pour plus d'informations. Pour plus d' aide sur le contrôle d'accès basé sur les rôles, voir gérer l'accès au portail.

Microsoft recommande l'utilisation de RBAC pour s'assurer que seuls les utilisateurs qui ont une justification d'entreprise peuvent accéder à l'ATP de Microsoft.

Des informations supplémentaires sont disponibles sur les instructionsd'autorisation.

L'exemple de tableau suivant permet d'identifier la structure du Centre des opérations de cyber Defense dans votre environnement pour vous aider à déterminer la structure RBAC requise pour votre environnement.

Niveau	Description	Autorisation requise
Niveau1	**Équipe d'opérations de sécurité locale/équipe informatique** En règle générale, cette équipe effectue un examen et examine les alertes contenues dans leur emplacement géographique, puis passe au niveau 2 dans les cas où une correction active est requise.	

Niveau	Description	Autorisation requise
Niveau2	**Équipe d'opérations de sécurité régionale** Cette équipe peut voir tous les ordinateurs de sa région et effectuer des actions de correction.	Afficher des données
Niveau3	**Équipe d'opérations de sécurité globale** Cette équipe est composée d'experts en sécurité et est habilité à afficher et à effectuer toutes les actions du portail.	Afficher des données Alertes activités de recherche active Alertes activités de recherche active Gérer les paramètres du système de portail Gérer les paramètres de sécurité

Ordre d'adoption

Dans de nombreux cas, les organisations auront des produits de sécurité des points de terminaison existants. Tout le minimum que doit avoir chaque organisation est une solution antivirus. Toutefois, dans certains cas, une entreprise peut également avoir implanté une solution EDR déjà.

Historiqueement, le remplacement d'une solution de sécurité utilisée comme nécessitant un temps important et difficile à accomplir en raison des raccordements serrés dans les dépendances de couche et d'infrastructure de l'application. Toutefois, étant donné que le système d'exploitation Microsoft Defender ATP est intégré au système d'exploitation, il est désormais facile d'obtenir des solutions tierces.

Choisissez le composant de Microsoft Defender ATP à utiliser et supprimez ceux qui ne s'appliquent pas. Le tableau ci-dessous indique l'ordre dans lequel Microsoft recommande la façon dont la suite de sécurité du point de terminaison doit être activée.

Composant	Description	Classement de l'ordre d'adoption
Réponse de point de terminaison & réponse (EDR)	Les fonctionnalités de détection de point de terminaison et de réponse de Microsoft Defender - PACM permettent de détecter des attaques avancées qui sont en temps réel et exploitables. Les analystes de la sécurité peuvent hiérarchiser efficacement les alertes, obtenir une visibilité sur l'ensemble des violations et prendre des mesures pour remédier aux menaces. En savoir plus.	1
Protection de nouvelle génération (NGP)	L'antivirus Microsoft Defender est une solution anti-programme malveillant prédéfinie qui fournit une nouvelle génération de protection pour les postes de travail, les ordinateurs portables et les serveurs. L'antivirus Windows Defender inclut les éléments suivants:	deuxième
Réduction de surface d'attaque (ASR)	Les fonctionnalités de réduction de surface d'attaque dans Microsoft Defender ATP permettent de protéger les appareils et applications de l'organisation contre les nouvelles menaces émergentes. En savoir plus.	3D
Threat & Management Vulnerability (TVM)	Le Threat & Management Vulnerability est un composant de Microsoft Defender ATP, et fournit aux administrateurs de la sécurité et aux équipes des opérations de sécurité une valeur unique, notamment:	n°4
Recherche automatique & de correction (AIR)	Microsoft Defender ATP utilise des enquêtes automatisées pour réduire considérablement le volume des alertes qui doivent être examinées individuellement. La fonctionnalité d'analyse automatisée exploite divers algorithmes de contrôle et les processus utilisés par les analystes (tels que les règles) pour examiner les alertes et prendre des mesures de correction immédiate pour résoudre les violations. Cela réduit	Non applicable

Composant	Description	Classement de l'ordre d'adoption
	considérablement le volume des alertes, ce qui permet aux experts en sécurité d'effectuer des tâches plus sophistiquées et d'autres initiatives à forte valeur ajoutée. En savoir plus.	
Microsoft Threat experts (MTE)	Microsoft Threat experts est un service de chasse géré qui fournit aux centres d'opérations de sécurité (SOCs) une analyse et une analyse de niveau expert pour vous aider à garantir que les menaces critiques dans leurs environnements uniques ne sont pas manquées. En savoir plus.	Non applicable

Étape suivante

Configurer le déploiement de Microsoft Defender ATP

Étape 2: installation