République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab de Blida

Mémoire de fin d'études

Pour l'obtention du diplôme de master en informatique

Option : Sécurité des Systèmes d'Information

Thème

Mise en place d'un mobile application management (MAM)

Au sein de la société NAFTAL

Organisme d'accueil : NAFTAL

Réalisé par :

BENTOUTA Nassim

ARBANE Abdelhakim

Promotrice :

- Mme. MESKALDJI

Encadrante :

- Mme. MAIZ

Année universitaire 2022/2023

REMERCIEMENTS

Tout d'abord, nous remercions Dieu le Tout-Puissant, de nous avoir donné la volonté et le courage de réaliser ce travail.

Un grand merci à notre promotrice, Mme Kh. MESKALDJI, qui nous a beaucoup aidé dans la correction et la rédaction de ce document, et aussi pour sa patience, sa disponibilité, et pour avoir accepté de mener ce travail.

Nous exprimons notre gratitude à tout le personnel de la société NAFTAL pour leur collaboration, en particulier les personnes qui nous ont fourni les éléments nécessaires à la réalisation de notre projet. Nous sommes particulièrement reconnaissants à Mme Amel MAIZ pour avoir accepté de nous confier cette mission et aussi pour son aide et ses précieux conseils ainsi que leur disponibilité durant le stage.

Nous remercions sincèrement les membres du Jury de nous avoir fait l'honneur d'accepter et d'évaluer notre travail et tout le corps professoral du département d'informatique de l'Université Saad Dahlab Blida1 pour les efforts fournis dans notre formation.

Enfin, nous voudrions exprimer notre profonde gratitude et nos vrais sentiments à nos familles, qui nous ont toujours soutenus.

DEDICACE ABDELHAKIM

Je dédie ce modeste travail :

À Mes parents, pour leur amour infini, leurs sacrifices, leur soutien et Leurs encouragements,

À Ma chère grand-mère paternelle et à la mémoire de mon grand-père, que Dieu l'accueille dans son vaste paradis,

À la mémoire de mes chers Grands-parents maternels, que Dieu les accueille dans son vaste paradis,

À mes chers frères et ma chère sœur,

À tous les membres de ma famille ainsi que mes amis,

À tous ceux qui me sont chers et à toutes les personnes qui m'ont aidé à atteindre ce niveau.

ABDELHAKIM

DEDICACE NASSIM

Je dédie ce modeste travail :

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse,

leur soutien et leurs prières tout au long de mes études,

À toute ma famille pour leur support et leurs encouragements

À ma tante Nassiba pour son encouragement permanent, et son soutien moral,

À mon frère Rachid et ses camarades Nasouf et Ahmed pour leur soutien

tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux, et le fruit de votre

soutien infaillible.

NASSIM

RESUME

Cette étude propose une approche complète de la sécurité et de la gestion des points de terminaison et des applications dans les architectures organisationnelles, en se concentrant sur l'utilisation des technologies couramment utilisées. Elle met en avant l'importance des mesures de sécurité robustes pour protéger les données critiques et garantir l'intégrité des systèmes organisationnels. En utilisant des outils tels qu'Active Directory, AD Connect, Microsoft Intune, Microsoft Defender et Power BI, cette recherche vise à renforcer la sécurité des points de terminaison et des applications et à simplifier leur gestion. Elle met également en évidence l'utilisation de JavaScript pour créer des interfaces intuitives facilitant la gestion des points de terminaison et des applications par les administrateurs annexes.

Mots clés : Points de terminaison, architectures organisationnelles, mesures de sécurité, données critiques, intégrité des systèmes, interfaces intuitives, administrateurs annexes.

ABSTRACT

This study proposes a comprehensive approach to endpoint security and management within organizational architectures, focusing on the use of commonly used technologies. It emphasizes the importance of robust security measures to protect critical data and ensure the integrity of organizational systems. By utilizing tools such as Active Directory, AD Connect, Microsoft Intune, Microsoft Defender, and Power BI, this research aims to enhance endpoint security and streamline their management. It also highlights the use of JavaScript in creating intuitive interfaces to facilitate endpoint management by auxiliary administrators.

Keywords: Endpoint, organizational architectures, robust security measures, critical data, integrity, organizational systems, intuitive interfaces, auxiliary administrators.

ملخص

تقدم هذه الدراسة نهجًا شاملاً لأمن وإدارة نقاط النهاية في الهياكل التنظيمية، مع التركيز على استخدام التقنيات المستخدمة بشكل شائع. تؤكد الدراسة أهمية اتخاذ تدابير أمنية قوية لحماية البيانات الحساسة وضمان سلامة أنظمة المؤسسة. باستخدام أدوات مثل Active Directory و AD Connect و Microsoft Intune و Microsoft Defender و Power BI إنشاء واجهات مستخدم بديهية تسهل إدارة نقاط النهاية من قبل المشرفين المساعدين. في JavaScript، تهدف هذه الدراسة إلى تعزيز أمن نقاط النهاية وتبسيط إدارتها. كما تسلط الضوء على استخدام

الكلمات الرئيسية: نقاط النهاية، الهياكل التنظيمية، تدابير أمنية قوية، البيانات الحساسة، سلامة الأنظمة المؤسسية، واجهات مستخدم بديهية، المشرفين المساعدين.

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES ABREVIATIONS

- **COVID**: Coronavirus Disease
- **NAFTAL**: National Agency for the Development and Control of Fuel Prices
- **DCSI**: Directorate of Communication Systems and Information
- **AD**: Active Directory IAM: Identity and Access Management
- **MFA**: Multi-Factor Authentication
- **RBAC**: Role-Based Access Control
- **ABAC**: Attribute-Based Access Control
- **ZT**: Zero Trust
- **ZTA**: Zero Trust Architecture
- **PDP**: Policy Decision Point
- **PEP**: Policy Enforcement Point
- **EDR**: Endpoint Detection and Response
- **IOC**: Indicators of Compromise
- **BYOD**: Bring Your Own Device
- **MDM**: Mobile Device Management
- **MAM**: Mobile Application Management
- **NIST**: National Institute of Standards and Technology
- **CIS**: Center for Internet Security
- **IBM**: International Business Machines
- **EM+S**: Enterprise Mobility + Security
- **OU**: Organizational Unit
- **AAD**: Azure Active Directory
- **Http(s)**: Hypertext Transfer Protocol (Secure)
- **CSV**: Comma Separated Values
- **SSO**: Single Sign-On
- **VPN**: Virtual Private Network
- **API**: Application Programming Interface
- **OAuth**: Open Authorization
- **VM**: Virtual Machine
- **ADUC**: Active Directory Users and Computers
- **GPMC**: Group Policy Management Console
- **CRUD**: Create, Read, Update, Delete.

INTRODUCTION GÉNÉRALE

La pandémie du COVID-19 a servi d'exemple d'impact qu'une telle crise peut avoir sur les entreprises et sur notre manière de travailler, cette dernière a poussé plusieurs entreprises à adopter des méthodes de travail ''non-traditionnelles'' comme le travail à distance pour assurer leur continuité. Par conséquent, les défis liés à la sécurité et à la gestion des points de terminaison et des applications dans un environnement télétravail se sont intensifiés, Notamment l'utilisation des appareils personnels et des réseaux domestiques peu fiables chez les employés. Il existe alors un risque accru pour l'organisation en termes d'attaques malveillantes ou d'exposition aux violations de données. Afin d'assurer la sécurité de leurs données et systèmes dans ce nouveau contexte professionnel, il est donc primordial pour les entreprises d'établir des mesures robustes.

Le recours aux équipements personnels pour travailler devient alors un défi majeur du télétravail. Le niveau de sécurité inférieur dont disposent ces appareils peut les rendre plus exposés aux cyberattaques qu'un équipement professionnel. Cependant, des mesures de sécurité comme le cryptage des dispositifs et les logiciels antivirus sont mises en place par les organisations afin de préserver leurs informations et leur infrastructure.

De même, assurer la sécurité du cloud est aussi essentiel que la protection des équipements lorsqu'on travaille à distance. Avec une croissance rapide du télétravail entraînant une utilisation accrue des services en ligne par les entreprises, nous devons veiller à ce que toutes nos informations soient protégées sur le Cloud.

Cependant, la problématique que ce rapport de master traite est la sécurisation et la gestion des points de terminaison et des applications dans un contexte télétravail. Pour cela la solution proposée est la mise en place d'une architecture dont le composant central est une solution de gestion des points de terminaison et des applications et qui combine les quatre services clés de Microsoft suivants : Intune qui servira comme un outil de gestion et de sécurisation des points de terminaison et des applications, Power BI dont le rôle est la visualisation des données, Microsoft Defender qui nous permettra d'apporter des

fonctionnalités supplémentaires pour protéger nos ressources ainsi qu'Azure AD qui nous servira comme source d'identité. De plus, une console web a été développée pour simplifier l'administration et faciliter l'accès à nos services principaux.

Pour élaborer sur cette solution vous avons adopté le plan suivant : Nous commencerons d'abord par l'étude de l'existant au premier chapitre où nous allons présenter l'organisme d'accueil du stage, expliquer les concepts clé liés à notre problématique, et mener une étude comparative des différentes solutions disponibles. Puis, nous passerons à la conception de la solution dans le deuxième chapitre où nous allons expliquer comment chacun des éléments contribue à notre approche. Ainsi, l'implémentation de la solution est abordée dans le troisième chapitre. Ensuite, nous allons présenter deux cas d'utilisation exposés dans le quatrième chapitre. Puis, nous allons finir par une conclusion générale.

CHAPITRE 1 : ÉTUDE DE L'EXISTANT

1. INTRODUCTION

La définition des besoins de la structure d'accueil ainsi qu'un aperçu sur les solutions existantes pour répondre à ces besoins sont nécessaires pour atteindre notre objectif. Pour ce faire, ce chapitre sera divisé en deux parties. Dans la première partie, nous présenterons l'organisme d'accueil ainsi que les différents besoins identifiés au sein de cet organisme. Ensuite, nous explorerons les concepts clés liés á notre problématique en abordant une description des principales solutions disponibles sur le marché.

2. PRESENTATION DE L'ORGANISME D'ACCUEIL

2.1 Structure d'accueil DCSI

DCSI (Direction Centrale des Systèmes d'Information) est la nouvelle structure de NAFTAL, créée dans le cadre du processus de restructuration de la société en 2004. Le projet présenté dans ce mémoire a été proposé par la Direction Centrale Des Systèmes d'Information (DCSI) dans le cadre d'un plan d'action visant à la gestion des dispositifs mobiles dans un contexte télétravail.

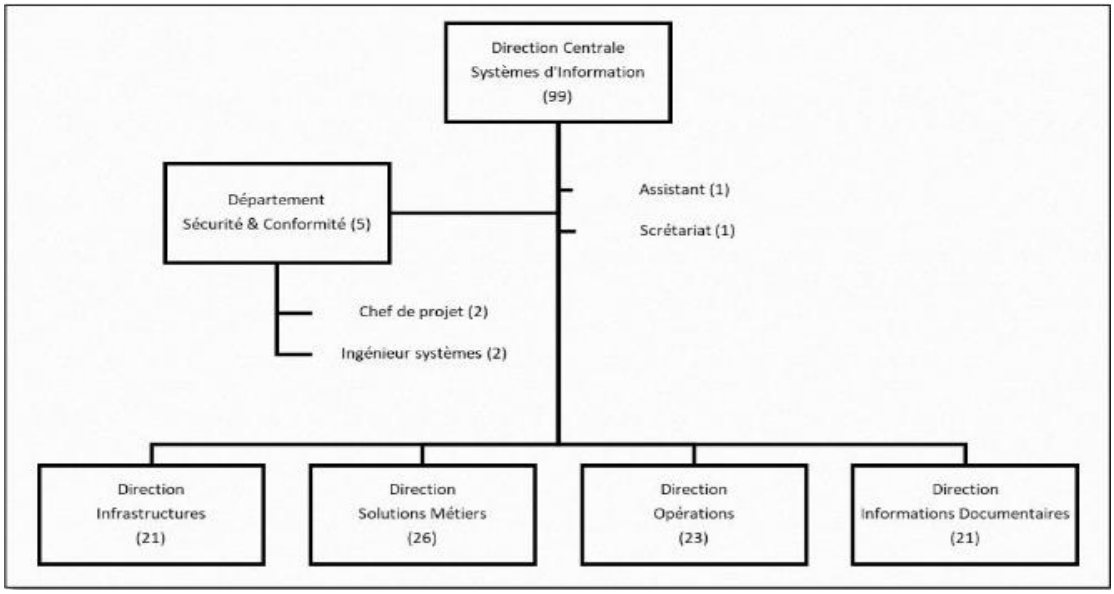

Figure 1 : Organigramme Direction Centrale Systèmes d'Information.

2.2 Missions de la DCSI

Les missions des cinq directions de la DCSI sont les suivantes :

a) Direction infrastructures

- Définir et mettre en œuvre l'architecture des systèmes, des bases de données et réseaux d'infrastructure du Système d'Information.
- Doter l'entreprise d'une infrastructure de communication sous forme de réseau étendu qui intègre toutes les structures de la Société.

b) Direction solutions métiers

- Concevoir et réaliser des solutions informatiques qui répondent aux besoins opérationnels de l'ensemble des Structures de la Société.

c) Direction opérations

- Veiller au bon fonctionnement des plateformes monétiques et décisionnelles.
- Garantir la disponibilité du matériel informatique dédié aux utilisateurs finaux du système d'information de la société.

d) Département sécurité & conformité

- Concevoir et mettre en place un dispositif permettant la sécurité et la pérennité des systèmes d'information mis en place.
- Mettre en place des règles de conformité et de contrôle interne dans l'établissement.

e) Direction informations documentaires

- Construire une banque de données documentaire de l'information règlementaire interne et externe.
- Mettre en couvre les solutions adéquates pour la conservation du patrimoine documentaire et informationnel de la société.

2.3 Définition des besoins clés

De multiples besoins ont été identifiés dans le cadre du projet de thèse et leur traitement a conduit à la création d'une approche adaptée. Il s'agit des besoins suivants :

- Sécurisation avancée des points de terminaison dans l'espace cloud.
- Gestion centralisée et efficace des points de terminaison et des applications.

- Intégration fluide entre l'Active Directory (AD) local et le Cloud.
- Console web conviviale pour les administrateurs.
- Visualisation des données pour une prise de décision éclairée.

Notre objectif principal est d'apporter une solution exhaustive qui garantit à la fois la sécurité et la gestion efficace des points de terminaison et des applications dans le domaine du cloud, afin d'améliorer la sûreté ainsi que le rendement opérationnel de ces derniers tout en fournissant une expérience utilisateur optimale aux responsables de sites annexes.

3. CONCEPTS CLES

3.1 La gestion des identités et des accès (IAM)

La gestion des identités et des accès (IAM) est l'ensemble des outils et des procédures utilisés pour réguler l'utilisation de leur infrastructure informatique et physique. Autrement dit, il s'agit '' *des processus, technologies et politiques qui gèrent l'accès des identités aux ressources numériques et déterminent les autorisations que ces identités ont sur ces ressources* '' [1], cependant, les concepts clés de l'IAM sont les suivants :

a) Permissions, opérations, et objets

Les habilitations en sécurité informatique établissent les opérations autorisées pour chaque utilisateur sur des objets déterminés. Les fonctions incluent aussi bien des opérations primaires comme la lecture et l'écriture que des opérations complexes comme effectuer une transaction monétaire. Divers objets nécessitent l'utilisation de permissions telles que celles qui permettent l'accès aux bases de données ou encore aux applications ainsi qu'aux dossiers et fichiers. [2]

b) Authentification et autorisation

L'identification et la permission jouent un rôle central dans le système IAM, une méthode d'authentification telle que MFA (Multi-Factor Authentication) est une méthode courante utilisée pour authentifier les utilisateurs et les systèmes en plus des mots de passe. Ainsi, Le choix des actions autorisées pour les utilisateurs et systèmes est lié aux modèles de contrôle d'accès telles que RBAC or ABAC qui sont appliqués, ce qui assure que toutes les informations confidentielles ne sont accessibles qu'aux utilisateurs qui y sont habilités. [2]

c) La gestion et l'approvisionnement du cycle de vie de l'utilisateur

La gestion du cycle de vie de l'utilisateur gère l'ensemble de l'identité d'un utilisateur dans une organisation, y compris la création, la maintenance et la désactivation du compte. L'approvisionnement accorde et révoque l'accès aux ressources en fonction du rôle ou des attributs de l'utilisateur. [2]

3.2 Zero Trust

La cybersécurité selon Zero Trust implique une évaluation continue plutôt que de se reposer sur la confiance implicite. De plus, l'intégralité du processus de gestion de l'identité et des accès est pris en compte dans cette architecture globale. L'objectif principal est de garantir que seules les personnes qui ont besoin des ressources y ont accès en ne leur octroyant que le minimum de privilèges requis. Plutôt que d'avoir recours à l'ancienne méthode défensive du périmètre dans l'approche traditionnelle de la sécurité informatique. Zero Trust a choisi de s'attaquer au grand défi que représente le trafic non autorisé. Assurer la sécurité des ressources et données de l'entreprise nécessite une telle approche.

Une définition opérationnelle de Zero Trust et de son architecture est la suivante : Zero Trust (ZT) vise à assurer des décisions d'accès précises et limitées dans les systèmes d'information, malgré un réseau considéré comme compromis. L'architecture Zero Trust (ZTA) est le plan de cybersécurité d'une entreprise qui intègre les concepts du zero trust. Ainsi, cette architecture nécessite l'infrastructure réseau et des politiques opérationnelles mises en place.

Dans le modèle abstrait d'accès illustré dans la Figure 2 ci-après, un sujet a besoin d'accéder à une ressource d'entreprise. L'accès est accordé via un point de décision de politique (PDP) et un point d'application de la politique correspondant (PEP). [3]

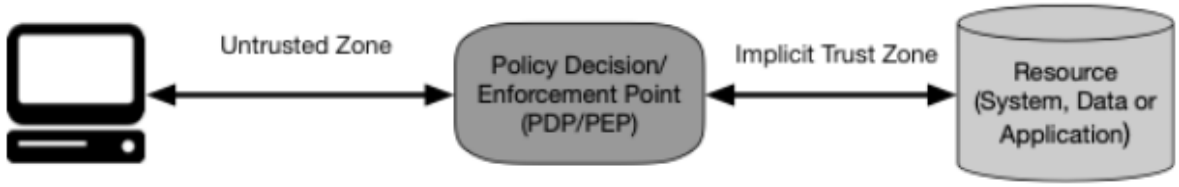

Figure 2: Zero Trust Access. [4]

Principes fondamentaux de la confiance zéro (Zero trust) :

1. Toutes les sources de données et les services informatiques sont considérés comme des ressources.
2. Toutes les communications sont sécurisées, quel que soit l'emplacement du réseau.
3. L'accès aux ressources individuelles de l'entreprise est accordé de manière spécifique à chaque session.
4. L'accès aux ressources est déterminé par des politiques dynamiques, y compris l'état observable de l'identité du client, de l'application/service et de l'actif demandeur, et peut inclure d'autres attributs comportementaux et environnementaux.
5. L'entreprise surveille et mesure l'intégrité et la posture de sécurité de tous les actifs possédés et associés.
6. Toute authentification et autorisation des ressources sont dynamiques et strictement appliquées avant d'accorder l'accès.
7. L'entreprise collecte autant d'informations que possible sur l'état actuel des actifs, de l'infrastructure réseau et des communications, et les utilise pour améliorer sa posture de sécurité. [3]

3.3 **Détection et réponse des points de terminaison (EDR)**

La détection et la réponse des points de terminaison (EDR) est un mécanisme de sécurité conçu pour fournir une protection en temps réel. Ce système collecte des données à partir des points de terminaison, puis les stocke et les traite dans une base de données centralisée. Les événements collectés sont ensuite corrélés en temps réel pour identifier

toute anomalie comportementale dans l'hôte. En conséquence, les systèmes EDR alertent rapidement les utilisateurs et les équipes d'intervention d'urgence de toute menace. [5]

3.4 La chasse aux menaces (Threat hunting)

La chasse aux menaces est une méthode précise et itérative de détection, de reconnaissance et de compréhension des intrus qui ont infiltré les réseaux du défenseur. [6] Il existe deux méthodes pour la chasse aux menaces : la chasse basée sur le réseau et la chasse basée sur l'hôte. La chasse basée sur le réseau consiste à rechercher des indicateurs de compromission (IOC) en examinant le trafic réseau. La chasse basée sur l'hôte nécessite des informations détaillées sur le système analysé, pour identifier les signes de compromission en analysant le comportement du système, les logiciels installés et les processus en cours d'exécution. [7]

3.5 La gestion des vulnérabilités

La gestion des vulnérabilités fait référence au processus continu d'identification, de catégorisation et de résolution des vulnérabilités de sécurité. Ce processus comprend quatre étapes principales, qui incluent l'identification et la découverte des vulnérabilités, leur évaluation, la correction des vulnérabilités et la vérification du processus tout en signalant les vulnérabilités trouvées.

3.6 Politique de sécurité

Une politique de sécurité est un document écrit qui décrit les directives, les attentes et l'approche générale d'une organisation pour protéger la confidentialité, l'intégrité et l'disponibilité de ses données.

3.7 Bring Your Own Device (BYOD)

Le concept de BYOD permet aux employés d'utiliser leur propre appareil (téléphone intelligent/tablette/ordinateur portable) pour accéder aux ressources informatiques de leur entreprise et effectuer des tâches professionnelles hors site, ce qui facilite le travail mobile ainsi que la création d'un lien entre les vies personnelles et professionnelles grâce à la connexion des technologies intelligentes. Le choix du BYOD comme solution pour accéder aux

ressources professionnelles partout a permis une amélioration significative des conditions de travail des employés. [8]

3.8 La gestion des appareils mobiles (MDM)

Les organisations doivent gérer avec efficacité un certain nombre d'appareils comme des machines virtuelles ou des ordinateurs pour garantir leur fonctionnement sûr et fiable. Elles ont pour priorité de maintenir à jour et sécuriser nos équipements conformément aux politiques internes dans le but d'éviter toute atteinte au réseau ou aux données. Avec le travail hybride qui implique souvent un mélange de télétravail ou encore du travail avec des périphériques personnels il devient impératif qu'une stratégie solide pour gérer ces périphériques soit mise en place afin de protéger toutes les informations confidentielles. [9]

3.9 La gestion des applications mobiles (MAM)

Les entreprises peuvent sécuriser et contrôler facilement leurs applications d'entreprise grâce au logiciel MAM conçu pour gérer les applications mobiles, ce qui permet la mise en place d'une politique visant à restreindre le partage de données et à séparer les applications professionnelles grâce à l'aide offerte par cet outil aux administrateurs informatiques. Ses fonctions incluent aussi la possibilité d'utiliser une distribution efficace de logiciels en plus d'une gestion optimale des licences et une bonne maîtrise du cycle d'application. [10]

3.10 La cybersécurité technique et administrative

L'utilisation des technologies appropriées pour contrer les menaces cybernétiques émergentes contre les entreprises et organisations est un objectif clé dans le domaine de la cybersécurité technique. Pour protéger les informations contre le vol ou l'utilisation malveillante par une tierce partie. Il est recommandé d'installer des systèmes techniques sur l'ordinateur ou le système informatique afin d'empêcher toute tentative non-autorisée. De plus, une protection complète est fournie pour les points de terminaison ainsi que pour les identités et données. [11]

Les organisations assurent la sécurité de leur écosystème en mettant en place des politiques et pratiques spéciales pour contrer les attaques cybernétiques. Pour garantir la sécurité de leurs données, il faut gérer les personnes, les procédés et les technologies. Pour ce faire, il est courant pour nous de respecter les normes de conformité prédéfinies par des experts certifiés comme NIST et CIS. [12]

4. ÉTUDE DES SOLUTIONS EXISTANTES

4.1 Microsoft Intune

L'application basée sur le cloud Microsoft Intune MDM / MAM offre une solution complète pour la gestion des appareils et applications, permettant ainsi la protection des données ainsi que la gestion et la sécurisation des périphériques et applications. [13]

- **Avantages :**
  - Intégration avec d'autres services Microsoft : Microsoft Intune peut être combiné avec Azure Active Directory et Microsoft Defender pour offrir des capacités et des fonctionnalités supplémentaires.
  - Prise en charge de Windows Autopilote : Microsoft Intune prend en charge Windows Autopilote, qui simplifie le processus de déploiement de nouveaux périphériques en les préconfigurant pour réduire le temps de productivité.
  - Architecture basée sur le cloud : En tant que service basé sur le cloud, Microsoft Intune peut être accessible de n'importe où et ne nécessite aucune infrastructure sur site.
- **Inconvénients :**
  - Absence d'implémentation sur site : Microsoft Intune est un service basé sur le cloud et ne peut pas être implémenté sur site.
  - Support de fichiers limité : Microsoft Intune ne prend pas en charge les fichiers (.pkg) ou (.exe).
  - Complexité : Microsoft Intune dispose d'un grand nombre de fonctionnalités, ce qui peut rendre difficile la navigation et la personnalisation du portail.

4.2 ManageEngine mobile device manager plus

ManageEngine Mobile Device Manager Plus est une solution complète de gestion de la mobilité d'entreprise conçue pour offrir le personnel d'entreprise possibilité de la mobilité, en améliorant la productivité des employés sans compromettre la sécurité de l'entreprise. [14]

- **Avantages :**
  - Offre un soutien étendu pour la mobilité et la sécurité.
  - Peut être facilement intégré à d'autres solutions cloud.
  - Capable de gérer un grand nombre d'appareils sans interférence externe.
- **Inconvénients :**
  - L'interface utilisateur peut ne pas répondre aux attentes de certains utilisateurs.
  - Ne prend pas en charge les systèmes d'exploitation Linux.

4.3 IBM MaaS360

La plateforme web IBM® MaaS360® permet une gestion totale des appareils mobiles. On peut surveiller et gérer des dispositifs mobiles tels que des smartphones, tablettes, etc. Le portail MaaS360 assure la prise en charge des fonctions d'administration, de gestion des appareils, de distribution de logiciels et du libre-service des politiques. Il assure également la conformité des appareils. [15]

- **Avantages :**
  - Une gestion puissante et sécurisée pour couvrir l'ensemble du cycle de vie de la mobilité.
  - Une intégration facile avec votre infrastructure existante. [16]
- **Inconvénients :**
  - Problème de synchronisation.
  - L'interface utilisateur est plutôt moyenne. [16]

5. CONCLUSION

En conclusion, Après une analyse approfondie des besoins posés pour la gestion et la sécurisation des points de terminaison et des applications dans l'espace cloud, il est clair que Microsoft Intune offre la meilleure solution possible. Ce chapitre a couvert un certain nombre de concepts essentiels comme l'IAM, la confiance zéro, le MAM, le MDM et la chasse des menaces. De plus, nous avons mené une étude comparative. Des solutions disponibles telles qu'IBM MaaS360, ManageEngine MDM Plus, VMware Workspace ONE et Microsoft Intune, chaque solution a ses propres forces et capacités, mais Microsoft Intune est particulièrement remarquable pour son approche complète et efficace de la sécurité des points de terminaison et des applications dans le cloud grâce aux fonctionnalités avancées qu'il offre comme l'accès conditionnel, les politiques régissant la conformité des appareils et la protection des applications. Les organisations peuvent également sécuriser leurs points de terminaison grâce à sa capacité d’intégration avec d'autres services Microsoft tels qu’Azure AD ou encore Office 360.

CHAPITRE 2 : LA CONCEPTION DE LA SOLUTION

1. INTRODUCTION

La solution que nous avons choisie nécessite l'intégration d'autres services pour répondre au problème de la sécurisation des points de terminaison et des applications dans le cloud. Cependant, l'architecture de notre solution illustrée par la figure 3 nécessite une source d'identité, un outil de gestion, un outil de sécurité et un outil de visualisation des données. Pour répondre à ces exigences, nous utiliserons Azure AD comme source d'identité, Microsoft Intune comme outil de gestion, Microsoft Defender pour les points de terminaisons comme outil de sécurité et Power BI comme outil de visualisation des données. De plus, nous avons développé une console web pour les administrateurs au niveau des branches pour accéder à ces services, car les portails principaux des services Microsoft ne sont accessibles qu'au niveau de la direction centrale.

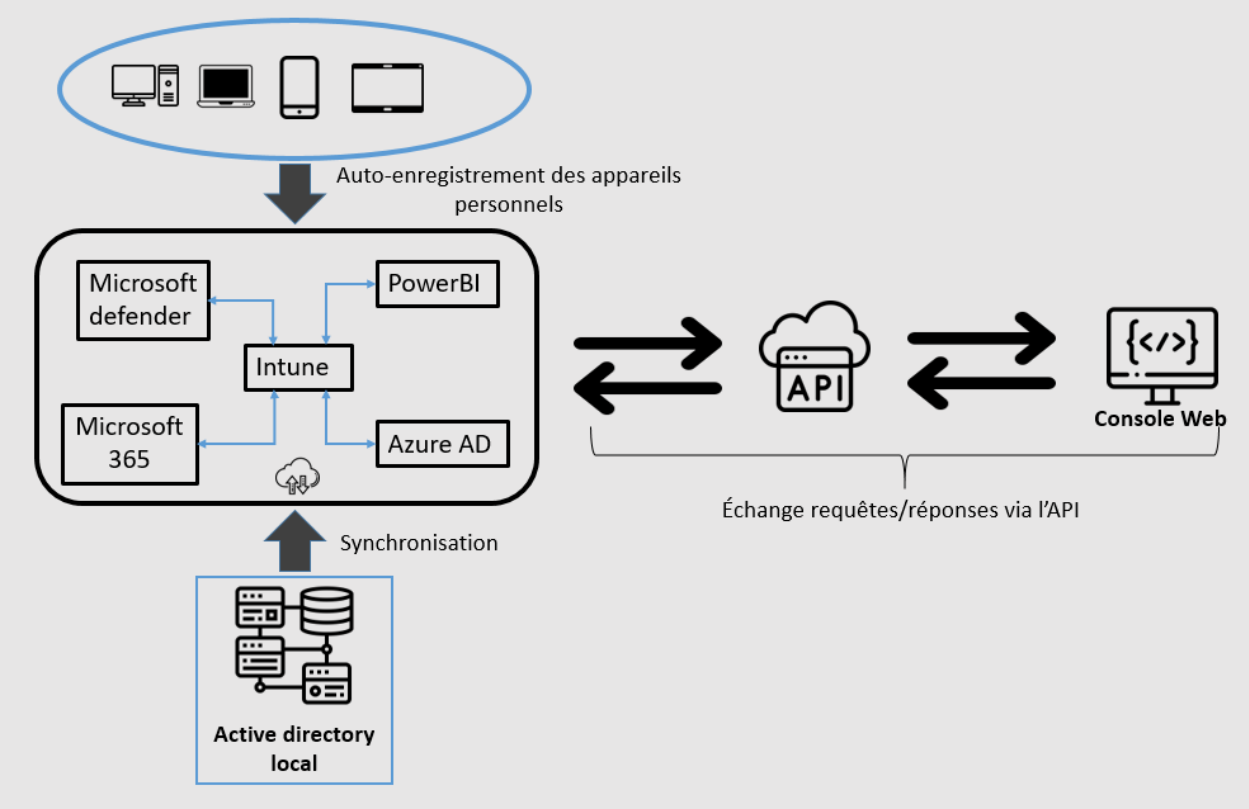

Figure 3 : Illustration globale de l'architecture de la solution.

2. LICENCES REQUISES POUR LES PRODUITS CLES

Pour une solution qui intègre Azure AD, Intune, Power BI et Microsoft Defender pour les points de terminaison, les licences appropriées pour chaque produit doivent être obtenues.

Azure AD est inclus dans l'offre Microsoft Enterprise Mobility + Security (EM+S), qui fournit des solutions de gestion des identités et des accès. [17]

Intune fait également partie de l'offre EM+S et fournit la gestion des appareils mobiles et des applications. [18]

Power BI offre à la fois des options de licence gratuites et payantes, y compris Power BI Pro et Power BI Premium par utilisateur (PPU). Le type de licence requis est déterminé par l'endroit où le contenu est stocké, comment l'utilisateur interagit avec lui et si le contenu utilise des fonctionnalités Premium. [19]

Microsoft Defender pour les points de terminaison est disponible sous plusieurs options de licence, y compris Microsoft Defender pour les points de terminaison Plan 1 et Plan 2. Ces plans fournissent une protection avancée contre les menaces avec une protection antivirus et antimalware, une atténuation des rançongiciels et plus encore, ainsi qu'une gestion et un rapport centralisés. [20]

Les objectifs principaux de ces produits sont de fournir un accès sécurisé aux ressources, de gérer les appareils mobiles et les applications, de fournir des informations commerciales grâce à la visualisation des données et de se protéger contre les menaces avancées.

3. SOURCE DE DONNEES

3.1 **Active Directory (AD) local :**

Pour une gestion optimale des utilisateurs et des groupes sur un réseau local, il est nécessaire d'utiliser un composant comme l'AD Local. Les administrateurs peuvent bénéficier d'une solution complète pour gérer les politiques de sécurité ainsi que le contrôle d'accès aux

ressources ce qui assure également une bonne gestion d'authentification et autorisation des utilisateurs. La suite d'applications qu'il propose facilite le travail administratif tout en permettant une bonne gestion aussi bien pour les comptes utilisateurs que pour les groupes de sécurité ou encore les unités organisationnelles (OU)[1]. [21]

En effet, nous avons mis en place une source de données qui utilise un AD local sur un serveur Windows, et nous avons utilisé Azure AD (AAD) Connect pour la synchronisation des utilisateurs depuis l'AD local vers Azure AD. (Voir figure 4)

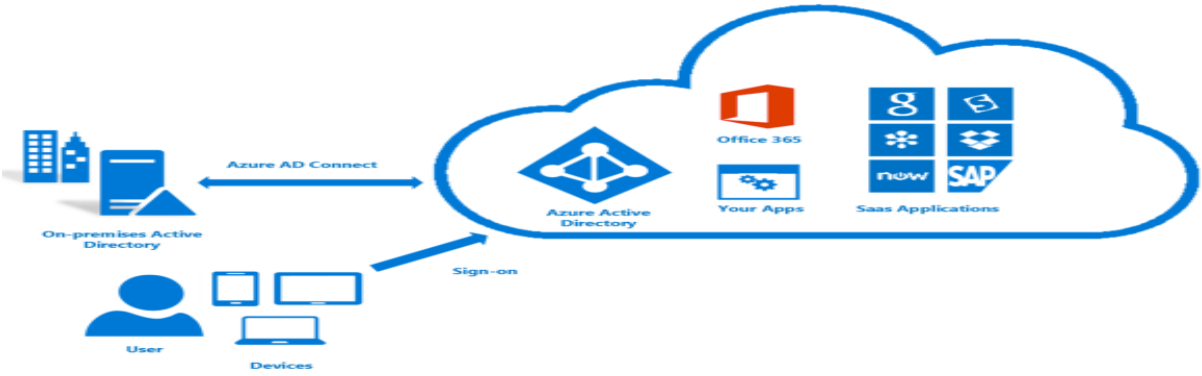

Figure 4 : Le rôle de AAD Connect dans l'architecture du cloud hybride. [22]

Azure Ad Connect présente un avantage clé - La configuration SSO permet aux utilisateurs d'utiliser les identifiants de l'AD local pour accéder aux services basés sur le cloud afin que les utilisateurs n'aient pas besoin de se rappeler de plusieurs combinaisons nom d'utilisateur/mot de passe différentes. D'ailleurs, la SSO peut être obtenue en synchronisant le hachage des mots de passe ou en utilisant l'accès fédéré.

Lors du processus de synchronisation, Azure AD Connect analyse les objets contenus dans l'AD sur site et compare ces derniers avec ceux présents dans Azure AD afin d'établir une liste des modifications qui devront être intégrées. Dès qu'une modification aux informations d'un utilisateur telles qu'un nouvel ajout ou une mise à jour sur le site de l'entreprise est effectuée, Azure AD Connect identifie rapidement cet évènement et met automatiquement en application les mises à jour nécessaires pour maintenir la cohérence dans les données stockées. [22]

[1] Unité organisationnelle (OU) : Un conteneur utilisé pour organiser et gérer des objets au sein d'un domaine.

3.2 **Azure AD**

La plate-forme Azure AD fournit également un ensemble solide de fonctionnalités pour assurer la sécurité des utilisateurs tout en respectant les principes fondamentaux liés à la gestion d'identification et d'accès (IAM) Azure AD est un service servant à gérer les identités et les accès tout en fournissant une plateforme centralisée permettant de contrôler l'accès ainsi que les permissions attribuées aux utilisateurs.

Grâce à ses mécanismes d'authentification solides, Azure AD assure la protection de l'identité des utilisateurs, et la prise en charge de l'authentification multi-facteurs est assurée afin de préserver la confidentialité des données stockées dans le cloud. L'emplacement et le risque de connexion sont pris en compte dans les politiques d'accès conditionnelles proposées par Azure AD pour sécuriser les accès aux ressources.

L'utilisation d'Azure AD pour une architecture cloud hybride (illustré par la figure 5) propose un modèle d'autorisation souple et précis qui se conforme aux principes de l'IAM, on peut limiter l'accès aux ressources en définissant avec précision les rôles et les autorisations accordés aux utilisateurs ou groupes.

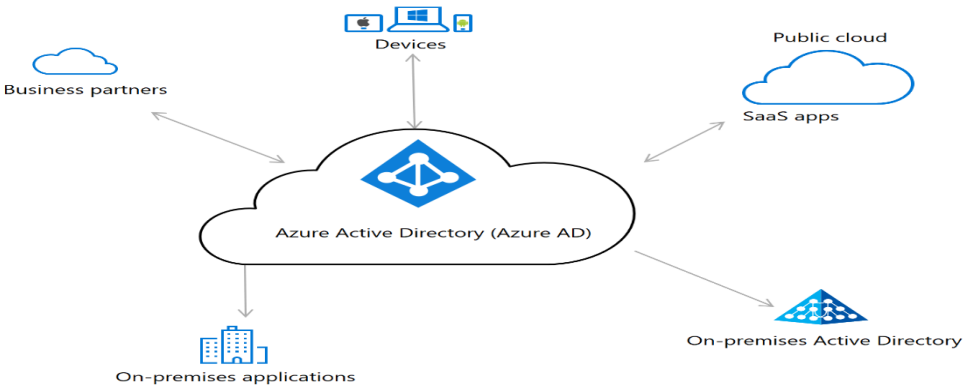

Figure 5 : Architecture basique du cloud hybride. [23]

Des garanties élevées en termes de sécurité et conformité sont offertes aux organismes par Azure AD afin qu'ils puissent protéger avec assurance leurs identités ainsi que leurs informations confidentielles, grâce aux algorithmes d'apprentissage automatique intégrés dans sa bibliothèque fonctionnelle cette application assure une totale sécurité en matière d'identification. Elle détecte et alerte sur toutes tentatives frauduleuses suite à une éventuelle utilisation contraire aux normes usuelles, avec cette fonctionnalité, les entreprises

sont plus réactives vis-à-vis d'éventuelles menaces tout en appliquant les mesures idoines pour protéger efficacement leurs utilisateurs ainsi que leur information. [24]

La surveillance de l'accès aux ressources et le contrôle des accès peuvent être réalisés efficacement avec la gestion d'identité privilégiée qui est une fonctionnalité de sécurité très importante. On peut citer comme exemple de ces fonctionnalités : L'accès juste à temps ainsi que les workflows d'approbation afin de garantir la mise en œuvre appropriée pour une surveillance efficace des accédants. [25]

En supplément à ses caractéristiques sécuritaires, Azure AD a également une technologie pointue pour la gestion des rapports ainsi que la supervision. Les journaux d'audit détaillés ainsi que les rapports relatifs aux connexions fournissent aux entreprises une occasion idéale pour suivre attentivement l'activité liée à leurs comptes utilisateur tout en veillant à réduire leur exposition aux problèmes potentiels au niveau sécuritaire. Dans le but d'offrir une vue complète sur la poste sécuritaire des entreprises, Azure AD s'intègre avec plusieurs autres outils telles qu'Azure Security Center ou bien encore Microsoft Cloud App Security.

4. OUTIL DE GESTION

4.1 Microsoft Intune

Microsoft Intune offre une gestion unifiée en se synchronisant avec Azure AD, permettant une inscription immédiate des utilisateurs et des dispositifs, tout en offrant une gestion efficace des systèmes multiplateformes. [26]

Intune simplifie la gestion des applications grâce à ses fonctions de déploiement et de suppression, ainsi que la possibilité de se connecter à un magasin privé pour distribuer des applications personnalisées. Il prend en charge une variété d'applications, y compris celles provenant du magasin d'applications et celles créées sur mesure. L'intégration avec Azure AD, Microsoft Defender et Microsoft 365 offre des avantages significatifs, comme illustré dans la figure 6, avec une gestion automatique des applications incluses dans Microsoft 365. [27]

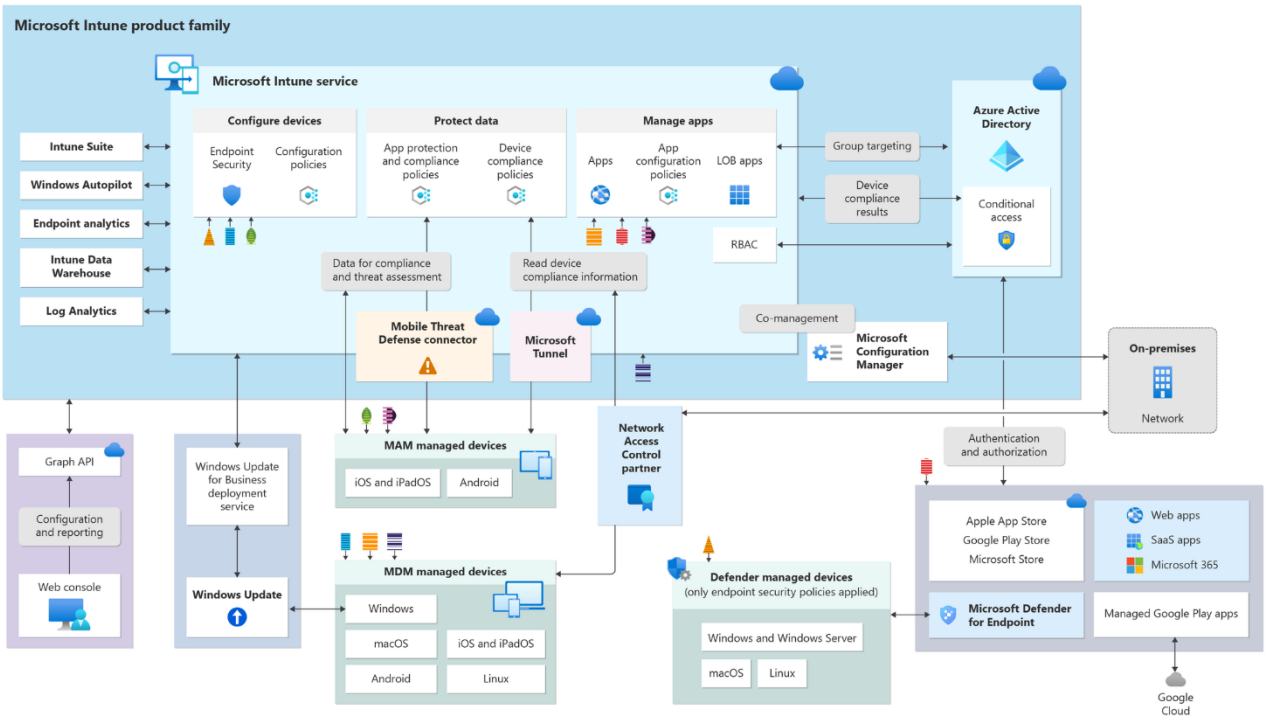

Figure 6 : Illustration de l'architecture et fonctionnalités de Microsoft Intune. [28]

L'ensemble complet des politiques disponibles avec Intune simplifie considérablement la tâche liée à la gestion des paramètres de sécurité sur les appareils. Ainsi, les fonctionnalités disponibles incluent une variété de politiques comme celles liées à la conformité ou l'accès conditionnel. Le tout étant accompagné par un certain nombre d'options supplémentaires qui comprennent notamment différents profils et bases de sécurité avec également un système d'anneaux pour les mises à jour.

Pour être considéré comme conforme en tant qu'utilisateur ou appareil, il est important de suivre scrupuleusement les règles et paramètres de conformité établis. Les politiques peuvent inclure des mesures s'appliquant aux appareils non conformes comme l'alerte aux utilisateurs sur leur état et la sécurisation de leurs informations. [29]

Gérer les paramètres et fonctionnalités des appareils peut être simplifié grâce à l'utilisation d'un profil de configuration ou une base de sécurité, ces modèles sont utiles pour personnaliser différents aspects tels que les connexions internet et VPN ainsi que pour obtenir des certificats. [30]

Avec l'utilisation des politiques de protection des applications vous avez le pouvoir d'administrer et sécuriser les données utilisées par votre entreprise dans une application. De plus, avec l'utilisation d'Intune MAM, il est facile de gérer des applications destinées à augmenter la productivité telles que les différentes suites bureautiques dont celle de Microsoft. [31]

Ces politiques aident à garantir un accès sécurisé aux ressources de l'entreprise, à protéger les données de l'entreprise sur les appareils et à fournir une conteneurisation des données pour éviter les fuites de données.

5. OUTIL DE SECURITE

5.1 Microsoft Defender

La protection des points de terminaison avec la puissante solution de sécurité de Microsoft nommée autrefois Windows Defender - aujourd'hui connue sous le nom de Microsoft defender [32]. Tous les outils nécessaires sont disponibles avec ce dernier pour améliorer considérablement l'intégration avec Microsoft Intune permettant ainsi une meilleure gestion cloud des points de terminaison. [33].

Il est essentiel d'avoir accès aux outils de sécurité que propose Microsoft Defender pour se défendre efficacement contre les menaces en perpétuel changement (Voir figure 7), les fichiers étant continuellement analysés par cette fonctionnalité de protection simultanée permettent de détecter toute activité malveillante potentielle. [32].

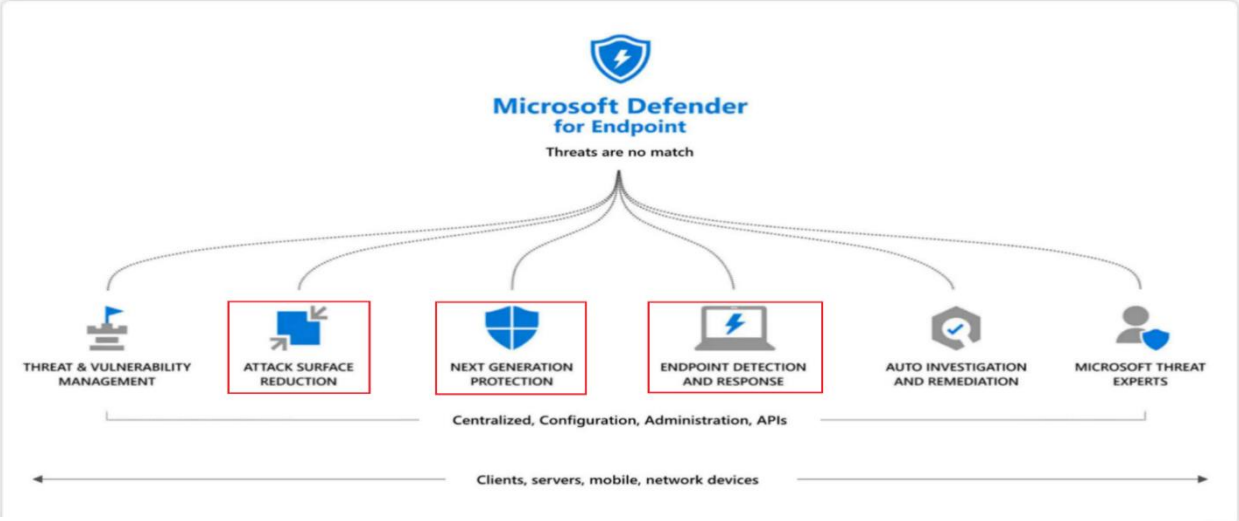

Figure 7 : Fonctionnalités de Microsoft Defender. [34]

La détection et la réponse sur les points d'accès (EDR) est intégrée dans Microsoft Defender pour fournir une protection accrue contre les menaces, ainsi que pour surveiller au mieux les éventuels incidents liés à la sécurité. Grâce à l'utilisation conjointe de techniques d'apprentissage automatique et d'analyse comportementale, ainsi que la collecte intelligente des données sur les menaces, le système permet une détection rapide des éventuelles tentatives malveillantes. [33].

Microsoft Defender assure un haut niveau de sécurité des points de terminaison grâce à l'approche Zero Trust, avec des contrôles d'accès rigoureux et une authentification constante. Les politiques Zero Trust permettent de surveiller le comportement des appareils et d'offrir une approche granulaire pour l'autorisation d'accès, réduisant ainsi efficacement le risque de violation de sécurité. [35].

De plus, Microsoft Defender offre des options personnalisables dans les paramètres avancés, permettant une adaptation sur mesure, notamment avec un planning personnalisable pour l'analyse antivirus et la possibilité de gérer facilement les opérations de mise en quarantaine ou de remédiation en cas de détection de fichiers suspects. [36].

6. OUTIL DE VISUALISATION DES DONNEES

L’outil Power BI facilite la visualisation et l'analyse de données dans les organisations en offrant la facilité de création de tableaux de bord grâce à une interface graphique intuitive ainsi que la disponibilité d'options complètes pour la visualisation. De plus, cette solution offre plusieurs options permettant la connexion aux sources de données principales telles que Microsoft Intune.

Power BI Desktop est largement reconnu comme étant le choix optimal en tant qu'environnement primaire pour le développement offrant ainsi un large éventail d'outils ainsi que différentes caractéristiques qui vous permettront la conception conviviale aussi bien les rapports que les indicateurs clés. En utilisant Power BI, une entreprise peut facilement transformer ses données brutes en visualisations claires et exploitables. [37] (Voir la figure 8)

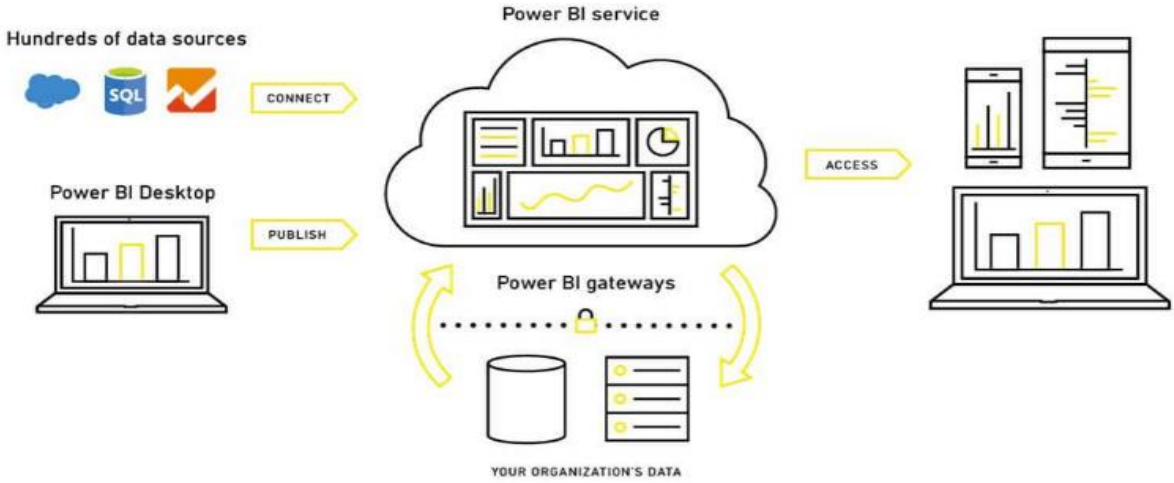

Figure 8 : Power BI Architecture [38].

7. OUTILS DE DEVELOPPEMENT

Notre console web a été conçue en utilisant une combinaison performante impliquant Vue.js, Vuetify et AXIOS pour une meilleure interaction avec l'API Microsoft Graph. En utilisant cette console intuitive et simple d'utilisation basée sur le diagramme ci-dessous (Figure 9), il devient plus facile pour les administrateurs locaux d'accéder aux différents services dont ils ont besoin ainsi que de gérer leur administration.

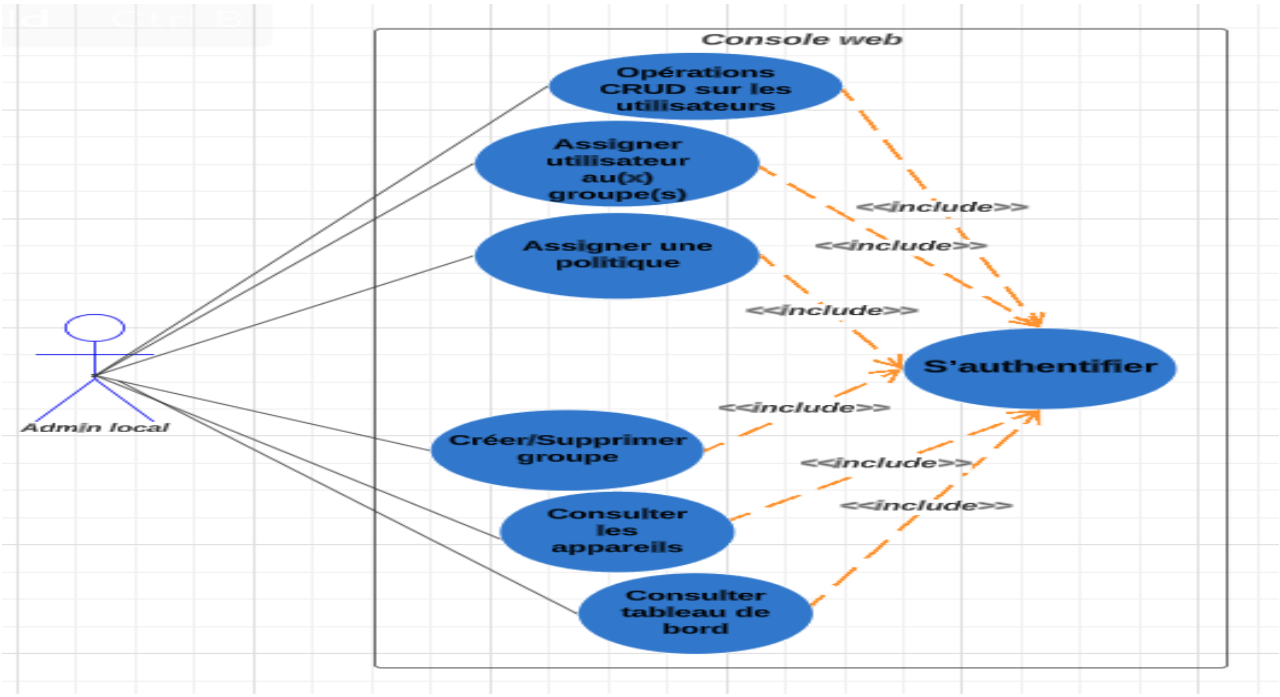

Figure 9 : Diagramme de cas d'utilisation pour la console WEB.

7.1 Microsoft graph API

Microsoft Graph API est l'une des interfaces de programmation les plus robustes sur le marché pour accéder un ensemble de services disponibles sur Microsoft 365. En utilisant cette solution logicielle, il est possible d'intégrer facilement différents services Microsoft dans des applications [39]. L'utilisation d'OAuth 2 nous permet de recevoir un jeton d'accès pour l'application, il est alors essentiel que les développeurs l'enregistrent dans Azure AD et définissent les autorisations nécessaires [40]. De plus, afin d'exercer un contrôle précis sur les données ou les opérations accessibles à une application spécifique il est possible de définir différents niveaux d'autorisations ou de privilèges [41]. Cependant, la figure 10 ci-dessous expose clairement comment les développeurs peuvent accéder à un large éventail des fonctions grâce à l'utilisation de l'API Microsoft Graph pour la prise en charge flexible and personnalisée. [39]

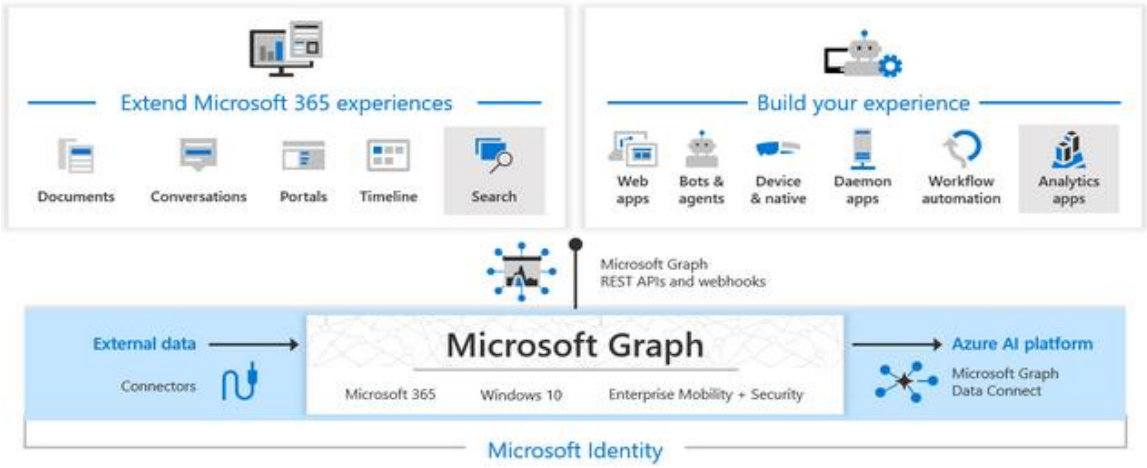

Figure 10 : Les capacités de l'API Microsoft Graph. [42]

En tant que Framework progressif pour les interfaces utilisateur en JavaScript, VueJS permet aux développeurs de créer des projets flexibles avec une grande facilité [43]. Les nombreux composants disponibles dans Vuetify basés sur Material Design de Google assurent une expérience utilisateur cohérente et belle dans les applications Vue.js [44]. De plus, en utilisant une bibliothèque axée sur javascript comme AXIOS, la communication fluide avec Microsoft Graph API devient un jeu d'enfant, simplifiant les appels d'API ainsi que la gestion complète de l'authentification et du traitement des réponses [45]. La combinaison de VueJS, Vuetify et AXIOS offre un puissant ensemble d'outils pour construire des applications Web riches en fonctionnalités et esthétiquement agréables.

8. CONCLUSION

En conclusion, ce chapitre traite de l'élaboration d'une solution visant à protéger les points de terminaison et les applications des grandes entreprises dans le cloud. Notre architecture propose l'utilisation d'Azure AD comme source d'identité, intégré avec un outil de gestion tel que le service Microsoft Intune. Parallèlement, l'intégration de Microsoft Defender permet de protéger contre les intrusions, tandis que Power BI offre des capacités de visualisation efficaces pour les données. De plus, nous avons développé une console web pour les administrateurs locaux afin d'accéder à ces services. La mise en place de cette solution nécessite l'obtention des licences appropriées pour chaque produit, assurant ainsi la sécurité des ressources et une gestion optimale des appareils et des applications.

CHAPITRE 3 : DEPLOIEMENT ET TESTS DE LA SOLUTION

1. INTRODUCTION

Dans le chapitre précédent, nous avons effectué des études conceptuelles. Nous passerons maintenant à la mise en place concrète de notre solution dans cette partie. Nous débuterons en définissant les outils et les différentes technologies que nous avons utilisé. Par la suite, nous détaillerons davantage la mise en œuvre de la solution. Enfin, nous présenterons deux cas d'utilisation pour valoriser et valider l'efficacité de notre solution.

2. ENVIRONNEMENT DE TRAVAIL

Dans cette section, nous procéderons à la description de l'environnement matériel et logiciel, ainsi que de l'architecture de la solution qui a été mise en place.

2.1 Environnement Matériel

Pour mener à bien le projet, nous avons utilisé un ordinateur portable qui présentait les spécifications techniques suivantes :

- Processeur Intel(R) Core (TM) i7-5500U CPU @ 2.40GHz
- Carte graphique Intel(R) HD Graphics 5500 4GB / NVIDIA GeForce 930m 2GB
- Mémoire vive 8 GO
- Système d'exploitation Windows 10 Entreprise LTSC 64-bit
- Disque dur 512 HDD

2.2 Environnement Logiciel

L'environnement virtuel comprenait l'utilisation de machines virtuelles (VM) déployées à l'aide de VirtualBox, une VM Windows Server 2019 pour simuler un serveur dans

notre infrastructure de test ainsi qu'une VM Windows 10 était utilisée comme client pour effectuer des tests et des analyses. Pour le développement de la console web, nous avons utilisé Visual Studio.

2.3 Technologies et Outils

- **Active Directory Users and Computers (ADUC)** : ADUC est un outil de gestion Microsoft pour administrer les comptes d'utilisateurs, les groupes et les objets dans un domaine Active Directory.
- **Group Policy Management Console (GPMC)** : GPMC est un outil Microsoft pour gérer les Objets de Stratégie de Groupe (GPO) dans un environnement Active Directory.
- **Windows PowerShell** : PowerShell est une interface en ligne de commande et un langage de script de Microsoft pour automatiser les tâches administratives et gérer les configurations système.

3. IMPLEMENTATION DE LA SOLUTION

3.1 Installation de l'Active Directory local

L'installation de l'Active Directory (AD) local est une étape clé pour mettre en place une infrastructure de gestion des identités et des ressources au sein d'une organisation. Ce qui nous a permis la création et la gestion des domaines, utilisateurs, groupes et objets de l'annuaire.

3.2 Importation en masse d'utilisateurs, groupes et unités organisationnelles

Nous avons réussi à importer en masse les utilisateurs, les groupes et les unités organisationnelles (OUs) en utilisant des scripts PowerShell. Ces scripts permettent de charger et de synchroniser rapidement un grand nombre d'utilisateurs, de groupes et d'OUs à partir de sources de fichiers CSV. Cela permet de gagner du temps, d'éviter les erreurs manuelles et de simplifier la gestion de l'annuaire. Ils assurent une cohérence et une précision des informations importées, comme le montre le résultat de l'importation présenté à la figure 11.

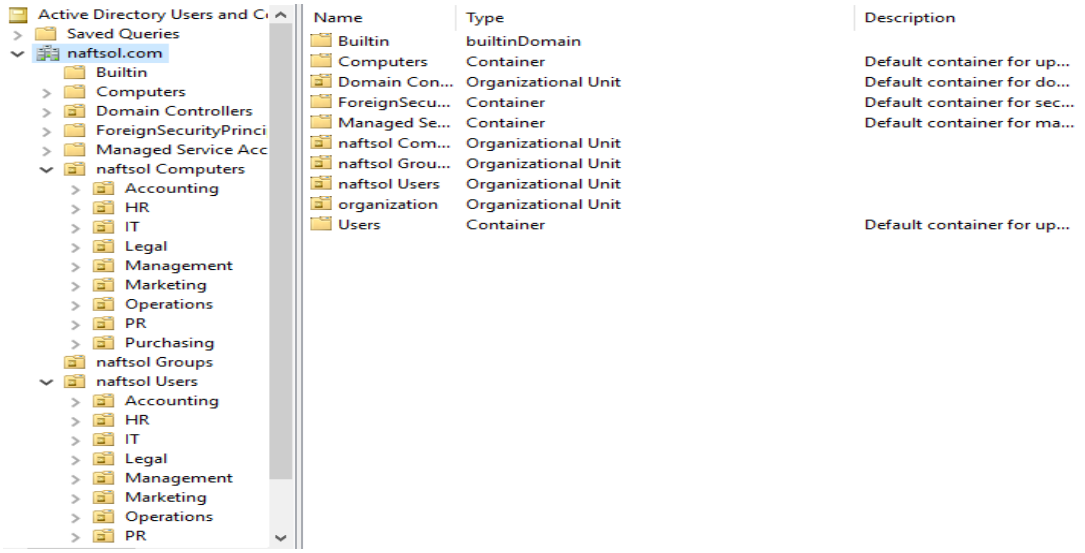

Figure 11: Illustre l'AD local.

3.3 Synchronisation de l'AD local vers l'Azure AD

Grâce à l'utilisation d'Azure AD Connect installée sur Windows Server nous avons pu établir simplement une connexion fluide entre l'Active Directory (AD) local et Azure AD. Comme on le voit sur la figure 12, Azure AD Connect nous a permis la synchronisation automatique des objets tels que les utilisateurs, les groupes et les attributs entre les deux environnements. Afin d'assurer une synchronisation sûre et efficace qui permet une authentification optimale, cette opération utilise les paramètres recommandés comme la synchronisation des haches de mots de passe. La mise en place du concept de gestion des identités et des accès (IAM) peut être réalisée grâce à la synchronisation que nous avons obtenue.

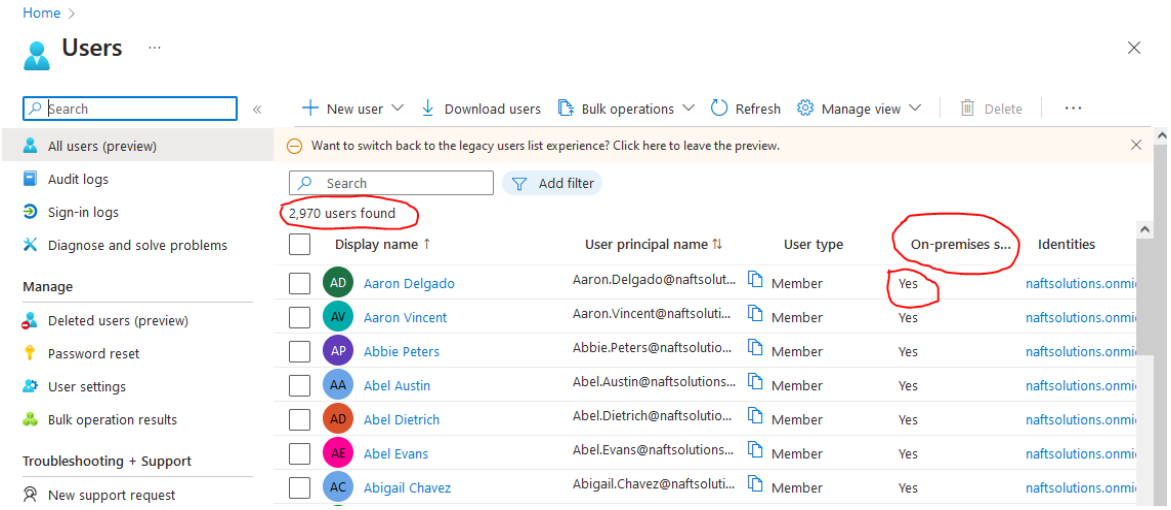

Figure 12 : Les données synchronisés sur Azure AD.

3.4 Création de politiques d'accès conditionnel conformes aux principes de Zero Trust

Microsoft Intune fournit un ensemble de fonctionnalités de gestion d'identité et d'accès conditionnel grâce à son intégration avec Azure AD. De plus, nous avons réussi à mettre en place une architecture de zéro trust grâce aux politiques d'accès conditionnel présentées sur la figure 13 :

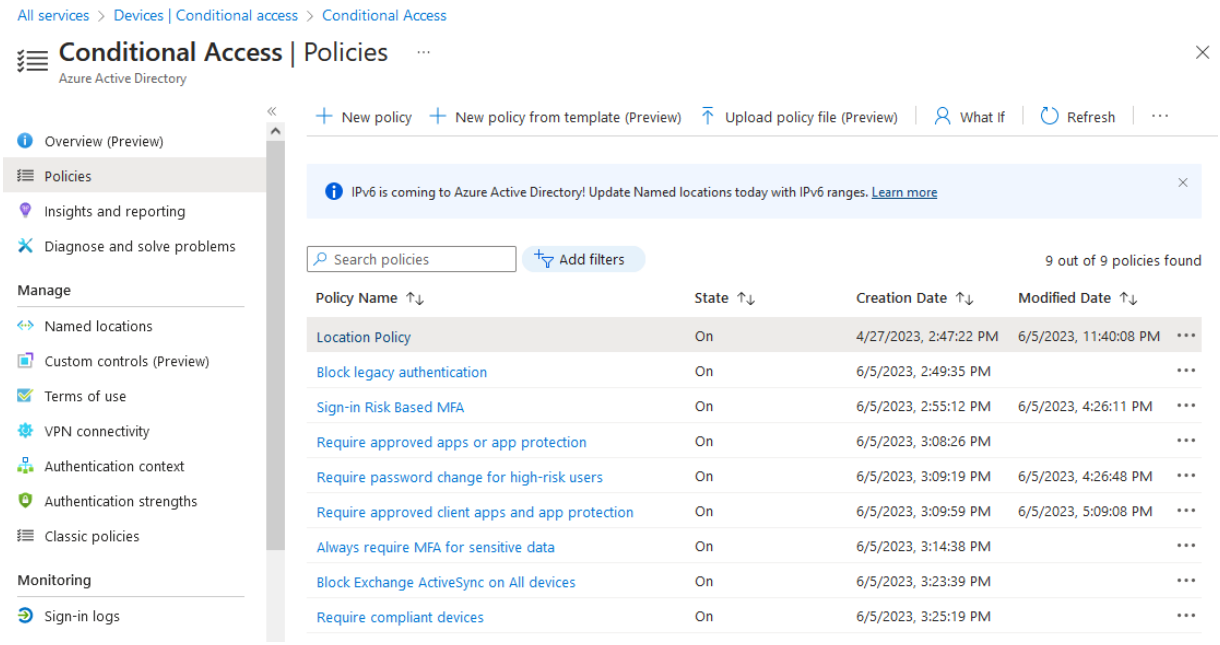

Figure 13 : Les politiques d'accès conditionnel alignées sur le modèle Zero Trust.

Ces politiques garantissent un niveau élevé de contrôle et de sécurité dans le cadre d'une approche Zero Trust où l'accès est accordé en fonction du contexte de l'utilisateur, de l'appareil et de l'activité, plutôt que de faire confiance implicitement à un réseau ou à une identité.

3.5 Élaboration de stratégie de conformité et automatisation avec les scripts personnalisés

L'un des éléments clés de notre stratégie de gestion des appareils est l'utilisation de politiques de conformité, Ces politiques nous permettent de définir et d'appliquer des normes de sécurité générales sur les appareils des utilisateurs. (Voir figure 14)

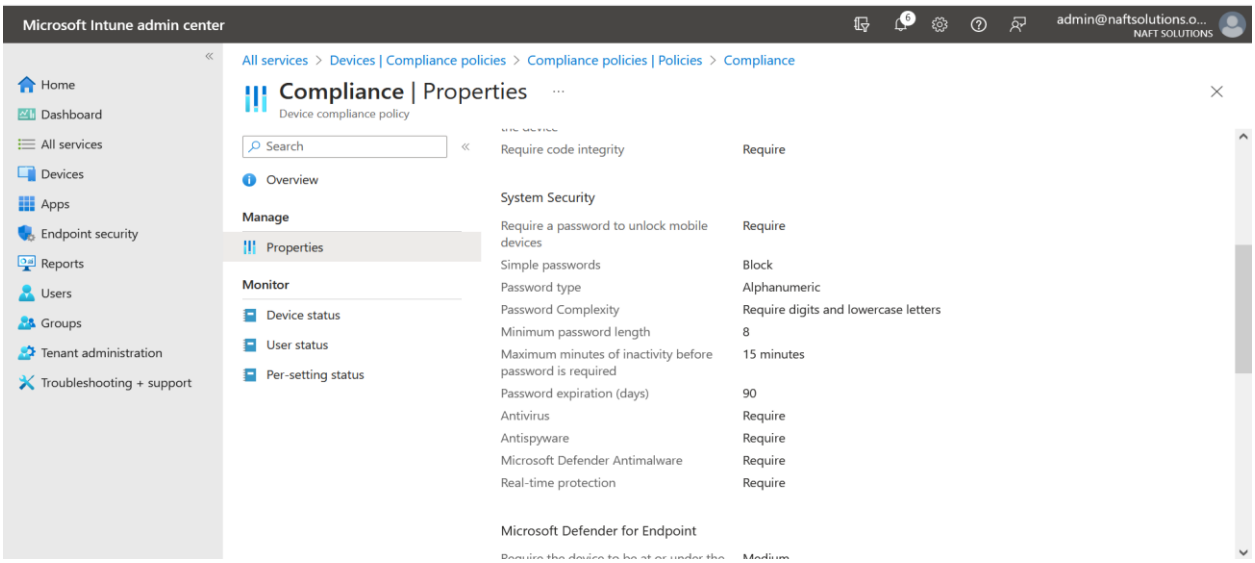

Figure 14 : Capture d'écran de la politique de conformité.

Nous avons utilisé la fonctionnalité "scripts" de Microsoft Intune pour avoir un contrôle plus granulaire sur les paramètres de conformité. Une utilisation pertinente de cette fonctionnalité est d'assurer la conformité des appareils des utilisateurs aux normes CIS Microsoft Intune pour Windows 10, qui sont des référentiels de bonnes pratiques en matière de sécurité. Grâce aux scripts, nous avons automatisé le processus de configuration des appareils pour les aligner sur ces normes.

Figure 15 : Script PowerShell.

Cette fonctionnalité nécessite la création d'un script PowerShell (voir figure 15) et un fichier JSON, comme on le voit sur la figure 16, ce dernier est le fichier de référence qui contient toutes les valeurs des paramètres de conformité nécessaires. Ainsi, le script PowerShell est un script de découverte qui est exécuté sur les appareils afin de récupérer les informations de paramètres que nous recherchons. La sortie du script de découverte est ensuite comparée au fichier de référence (fichier JSON).

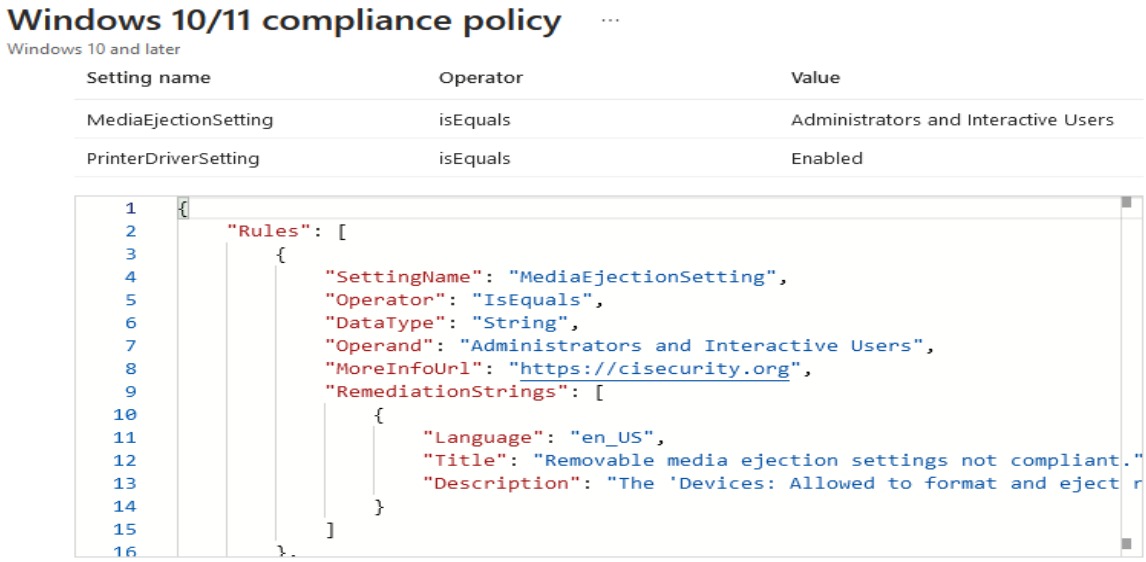

Figure 16 : Fichier de référence JSON.

3.6 **Profils de configuration**

En plus des politiques de conformité, nous avons également utilisé des profils de configuration. Ces profils nous permettent de configurer les paramètres et fonctionnalités des appareils de manière cohérente sur tous les appareils. Cela aide alors à garantir que tous les appareils sont correctement configurés et répondent aux normes de sécurité. Par exemple, les configurations figurées ci-dessous (figure 17), nous permettent de garantir une installation sécurisée des applications.

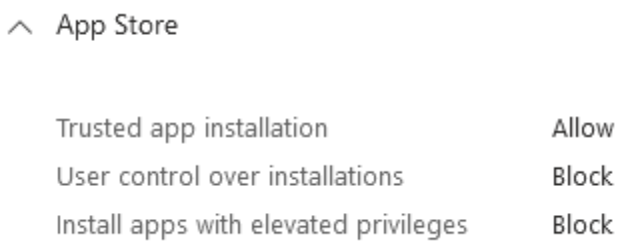

Figure 17 : Capture d'écran d'un exemple de profile de configuration.

3.7 Détection et réponse aux points de terminaison (EDR)

Enfin, nous avons mis en place des politiques de détection et de réponse aux points de terminaison (EDR). Ces politiques nous permettent de déployer Microsoft Defender sur les appareils des utilisateurs. Cela fournit une couche supplémentaire de protection contre les logiciels malveillants et autres menaces.

3.8 Gestion des applications

Un autre élément clé de notre stratégie est la gestion des applications dont l'une de ses fonctionnalités est la capacité de déployer des applications sur les appareils des utilisateurs. Comme on le voit sur la figure 18, nous pouvons gérer et distribuer des applications de manière centralisée sur les appareils des utilisateurs. Cela garantit que tous les utilisateurs ont accès aux applications dont ils ont besoin pour être productifs.

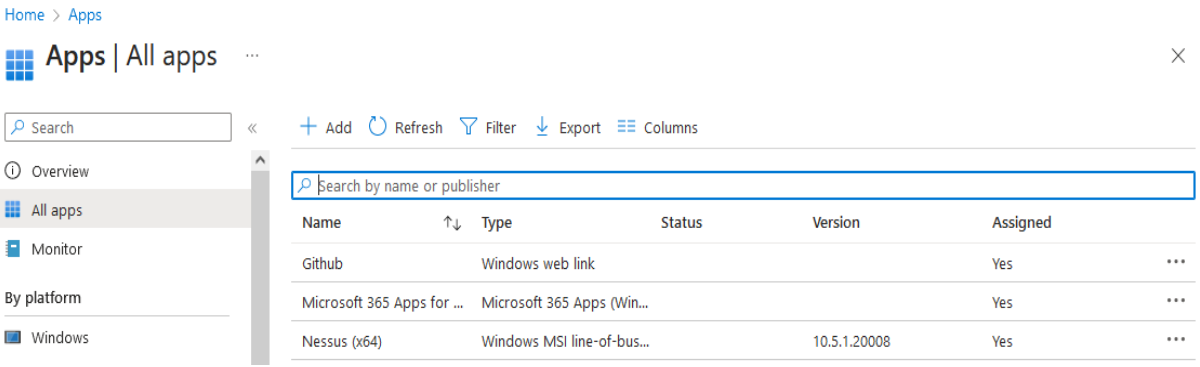

Figure 18 : Catalogue d'applications.

En plus du déploiement d'applications, nous avons également mis en place une suppression sélective d'applications. Cette fonctionnalité nous permet de supprimer à distance les données d'entreprise d'un appareil utilisateur tout en laissant les données

personnelles intactes. Cela est utile dans les situations où un appareil est perdu ou volé, ou lorsqu'un employé quitte l'entreprise.

3.9 Politiques d'anneaux de mise à jour

Nous avons également mis en place une politique d'anneau de mise à jour (illustrée par la figure 19). Cette politique nous permet de contrôler quand et comment les mises à jour sont installées sur les appareils des utilisateurs. En utilisant des anneaux de mise à jour, nous pouvons garantir que tous les appareils sont à jour avec les derniers correctifs de sécurité et fonctionnalités.

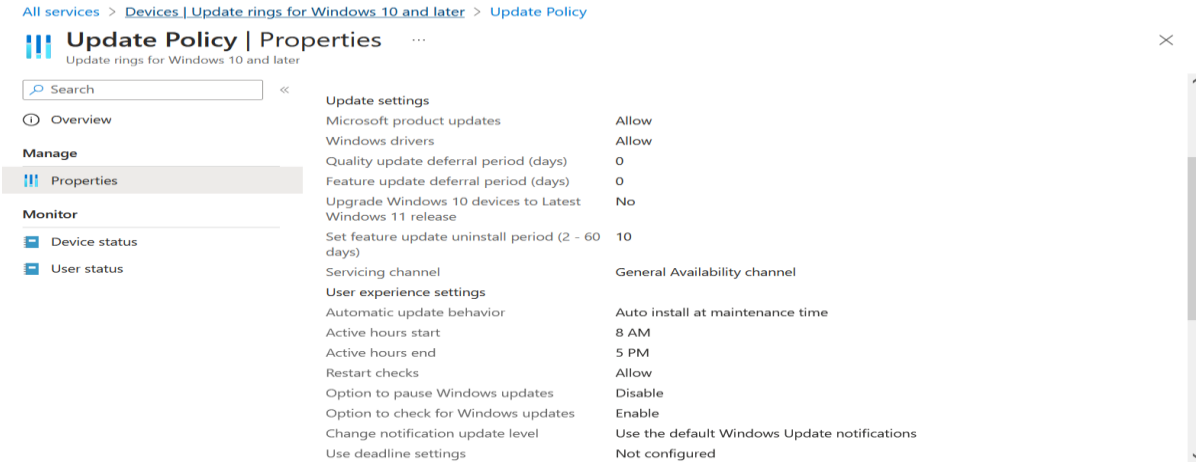

Figure 19 : Capture d'écran d'anneau de mise à jour.

Enfin, nous avons mis en place des politiques d'applications pour Office 365. Ces politiques nous permettent de contrôler comment les utilisateurs interagissent avec les applications Office 365 sur leurs appareils.

3.10 Auto-enrôlement des appareils

Pour l'enrôlement des appareils, les utilisateurs peuvent s'auto- enrôler en installant l'application 'Portail d'entreprise' et en enregistrant l'appareil à l'aide d'un compte Microsoft 365. Si l'enrôlement automatique a été configuré dans Azure AD et Intune, les utilisateurs n'auront besoin de saisir leurs informations d'identification qu'une seule fois lors du processus d'enrôlement. Après avoir saisi leurs informations d'identification, les utilisateurs doivent suivre les tâches requises par l'application pour terminer le processus d'enrôlement.

3.11 Intégration de Power BI et Microsoft defender

Pour faciliter l'intégration de Power BI avec Microsoft Intune, la première étape a consisté à se connecter au site Web de Power BI en utilisant les identifiants d'administrateur global. Par la suite, Power BI Desktop a été téléchargé et le connecteur Intune présenté sur la figure 20 a été configuré. Cela a permis l'importation de données d'Intune dans Power BI, permettant l'utilisation des données d'Intune pour gérer la sécurité. Le processus de synchronisation entre Power BI et Intune facilite la génération de rapports interactifs pour le service Intune.

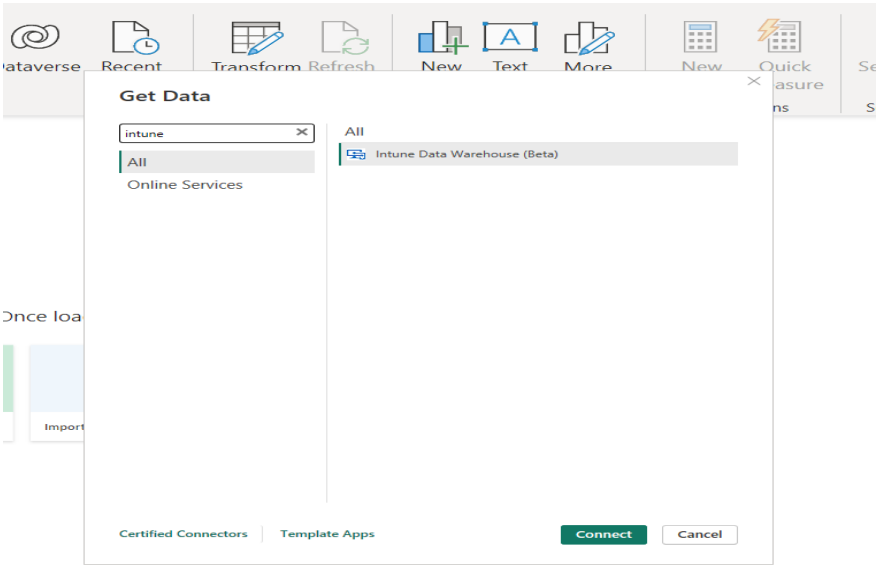

Figure 20 : Connecteur Intune sur Power BI. Desktop

En plus des étapes mentionnées ci-dessus, une politique de collecte de données d'Intune pour les données de points de terminaison a également été créée. Cette politique spécifie les types de données de points de terminaison qui sont collectées à partir d'Intune et importées dans Power BI. La création de cette politique est une étape importante pour garantir que les données de points de terminaison utilisées dans les rapports Power BI sont précises et pertinentes.

Ainsi, afin d'intégrer Microsoft Defender avec Intune, une connexion a été faite au niveau des portails Intune et Microsoft Defender. Par la suite, les connecteurs Microsoft Defender et Intune illustrés par les figures 21 et 22 (respectivement) ont été activés, respectivement. Cela a permis la synchronisation des données entre les deux services et l'intégration des appareils à Microsoft Defender.

Figure 21 : Connecteur Microsoft Defender.

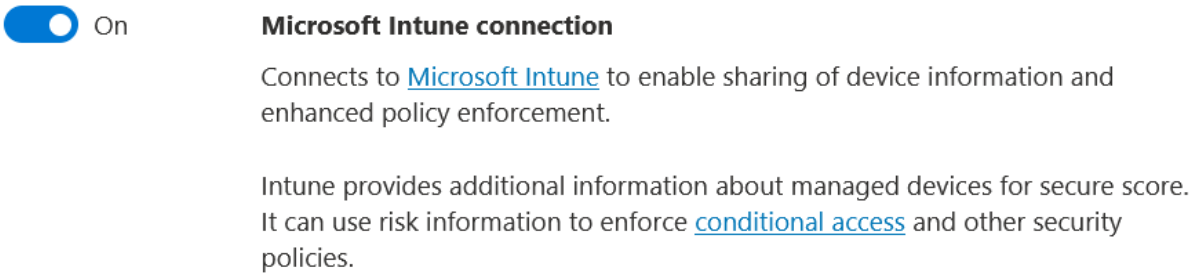

Figure 22 : Connecteur Intune.

De plus, une politique de détection et de réponse aux points de terminaison (EDR) a été créée. Cette politique joue un rôle crucial dans le déploiement de Microsoft Defender sur les points de terminaison en spécifiant la manière dont les données des points de terminaison sont collectées et analysées par Microsoft Defender. La politique EDR est un élément important du processus d'intégration car elle contribue à garantir que les données des points de terminaison sont surveillées avec précision et efficacité par Microsoft Defender.

3.12 Les fonctionnalités de sécurité supplémentaires apportées par Microsoft defender

Les multiples fonctionnalités intégrées dans Microsoft Defender assurent une protection optimale pour la solution. De plus, des fonctions telles que l'Antivirus ou encore la détection de menaces sont intégrées dans le logiciel avec une gestion efficace de toutes les vulnérabilités.

La fonctionnalité Antivirus est une barrière efficace pour empêcher l'infiltration de programmes nuisibles comme les rançongiciels ou logiciels espions et elle analyse sans cesse vos appareils pour repérer tout programme dangereux et vous alerte dès qu'elle le découvre.

La pratique régulière de la chasse aux menaces permet à notre entreprise d'être proactive en traquant et éliminant les dangers potentiels qui pourraient peser sur elle, les menaces potentielles peuvent être identifiées avec cette fonctionnalité afin de pouvoir être atténuées avant même qu'elles n'affectent notre système. Un exemple est fourni dans cette image capturée (Figure 23), en illustrant comment une requête a été exécutée sur la base des événements afin de valider que les points de terminaison ont été bien configurés pour l'installation du logiciel Antivirus Microsoft Defender.

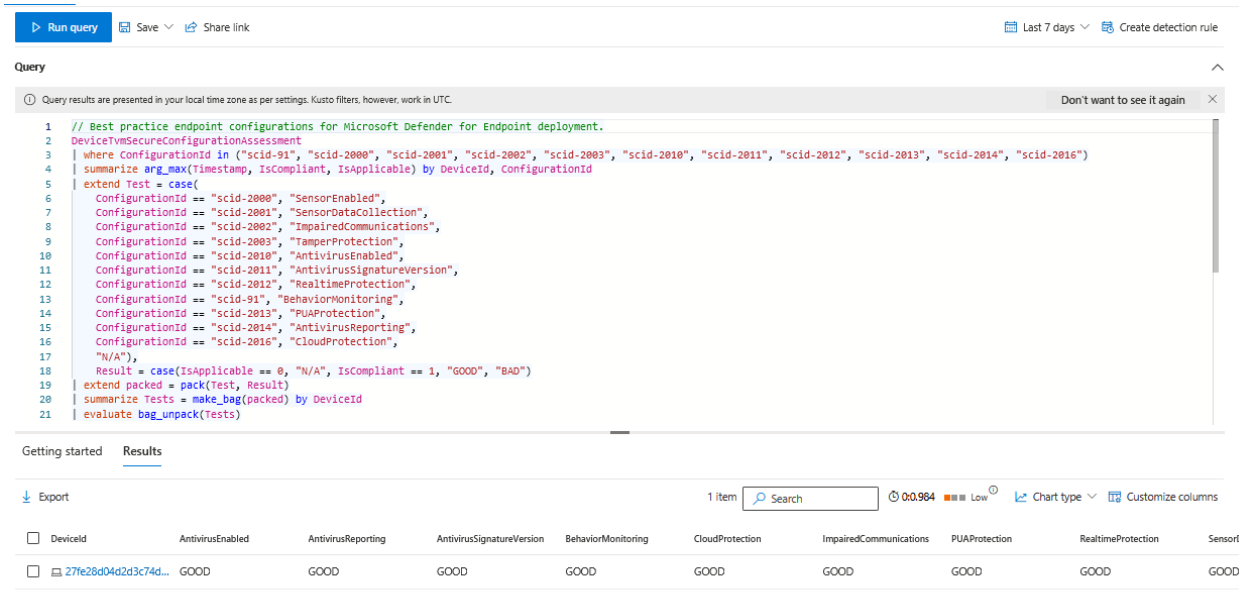

Figure 23 : Requête de chasse aux menaces.

De plus, la gestion des menaces et des vulnérabilités est une approche basée sur les risques pour gérer les vulnérabilités dans notre environnement. Comme on le voit sur la figure 24, elle nous aide à identifier et à prioriser les vulnérabilités en fonction de leur impact potentiel, nous permettant ainsi de nous concentrer d'abord sur les problèmes les plus critiques.

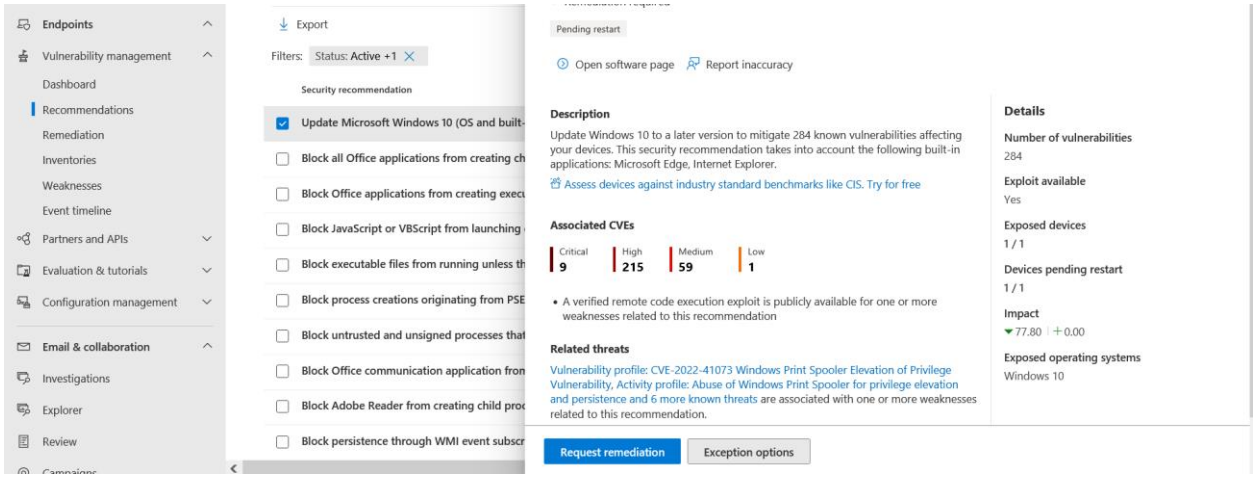

Figure 24 : La gestion des menaces et des vulnérabilités

En plus de ces fonctionnalités, Microsoft Defender nous permet également de prendre des mesures telles que l'initiation de scan Antivirus et l'isolement des appareils. Cela nous donne un plus grand contrôle sur la sécurité de votre environnement.

3.13 Préparation de l'API Microsoft Graph pour une gestion simplifiée et sécurisée

L'API Microsoft Graph fournit une interface solide pour communiquer avec les services de Microsoft tout en extrayant des informations importantes pour une meilleure gestion des points de terminaison. Cela accroît l'efficacité et la productivité des utilisateurs. Pour sa configuration et sa mise en œuvre, nous avons effectué des opérations cruciales telles que l'enregistrement d'applications et la définition précise des autorisations de ressources. Nous avons aussi mis en place des politiques de sécurité et des flux d'authentification avancés. En implémentant les flux d'authentications tels qu'Authentification OAuth 2.0 avec les systèmes dédiés au renouvellement régulier du jeton, nous sommes en mesure de fournir un haut niveau d'autorisation ainsi qu'une grande sécurité comme montrée sur la Figure 25. Ceci arrive quand on interagit avec l'API Microsoft Graph. Grâce à ses fonctionnalités avancées, telles que la pagination, la recherche, les filtres et les liaisons entre les entités, nous sommes en mesure de récupérer, manipuler et analyser de manière efficace les données liées aux points de terminaison.

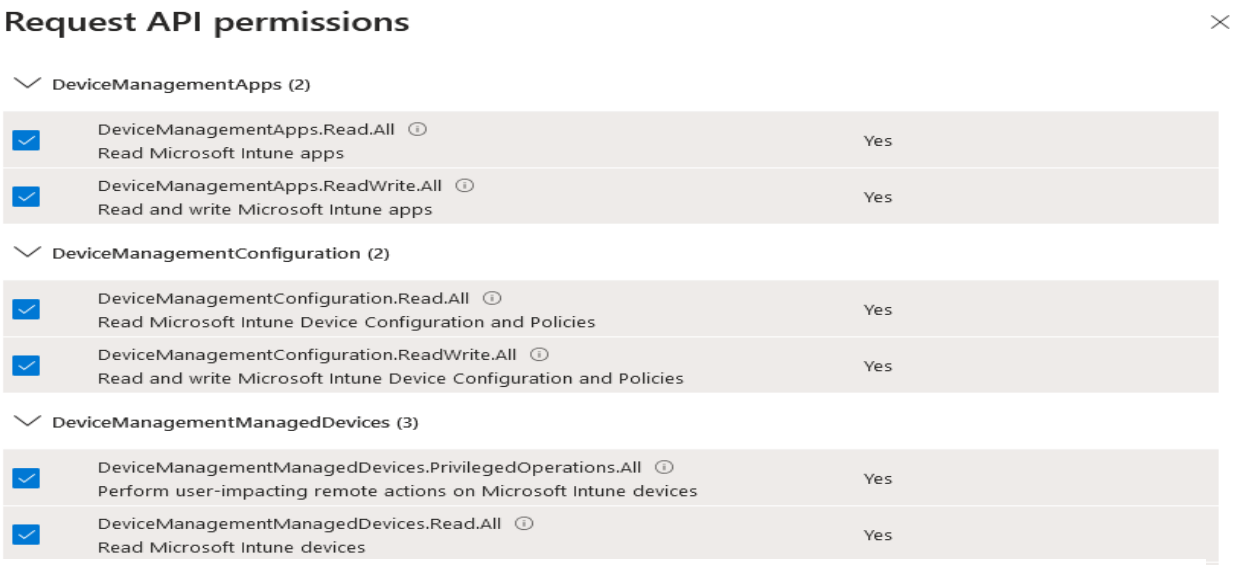

Figure 25 : Capture d'écran des permissions d'API

3.14 **Postman**

Nous avons utilisé l'outil Postman pour effectuer des tests approfondis des requêtes API avant de commencer la conception de notre application. Nous avons pu valider la communication avec l'API Microsoft Graph et vérifier les résultats pour leur conformité. Ces tests nous ont permis de simuler différentes demandes. Cette étape cruciale en amont a permis d'établir des échanges fiables et cohérents avec l'API. Elle a construit les fondements solides pour notre application sécurisée de gestion des points de terminaison.

3.15 **Une console web personnalisée** pour **une gestion sécurisée**

En utilisant JavaScript, nous avons développé une console web, offrant aux administrateurs des annexes ou des branches un contrôle centralisé, intuitif et performant pour la gestion et la sécurisation de leurs points de terminaison et applications. L'objectif de cette console web est de prouver la possibilité de développer une interface personnalisée selon les besoins d'un type d'utilisateur afin de simplifier l'utilisation des services Microsoft utilisés et de séparer les responsabilités et les tâches.

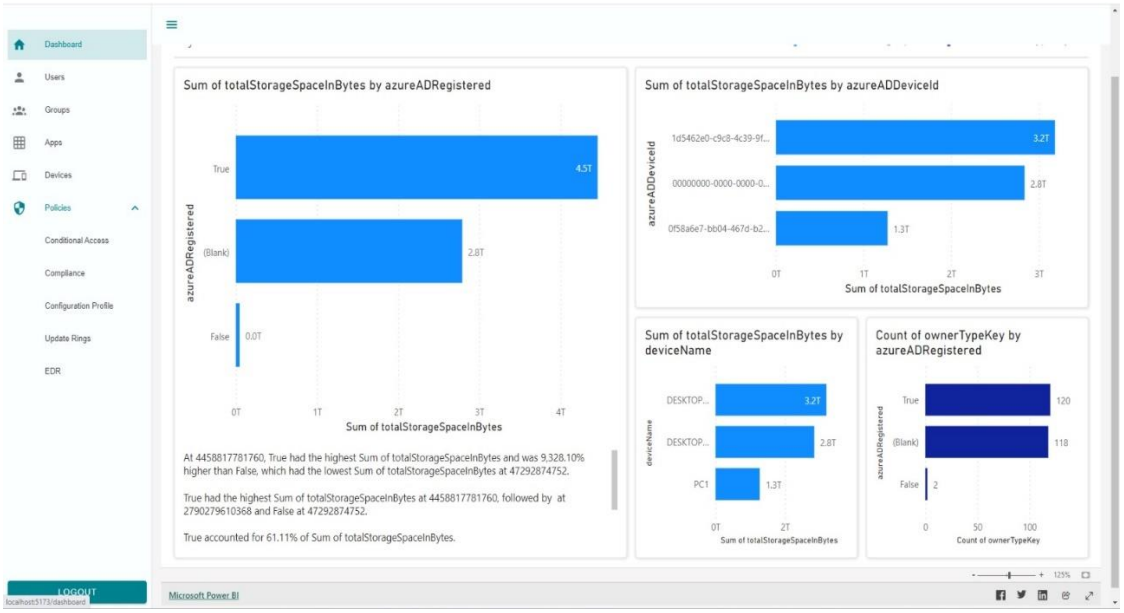

Figure 26 : Capture d'écran de la console web.

Comme on le voit sur la figure 26 ci-dessus, La console développée nous permet d'effectuer des opérations basiques telles que les opérations CRUD sur les utilisateurs, la consultation des tableaux de bord, l'affectation de différents types de politiques aux groupes d'utilisateurs.

4. TESTS ET ÉVALUATIONS

4.1 Attaque brute force ou informations d'identification divulguées

Lors d'une connexion normale à partir de l'ordinateur d'Alma, l'utilisateur désigné peut accéder facilement au site web https://portal.azure.com car elle utilise des appareils de confiance, sans augmentation du risque d'authentification ou de l'utilisateur, et sans demande de MFA. Cependant, si les informations d'identification de l'utilisateur sont utilisées depuis un autre emplacement, il est possible de se connecter en entrant le nom d'utilisateur et, dans ce cas, le mot de passe volé. Dans cette situation, une authentification multi-facteur (MFA) peut être nécessaire en raison du risque accru d'authentification, comme illustré dans la figure 27.

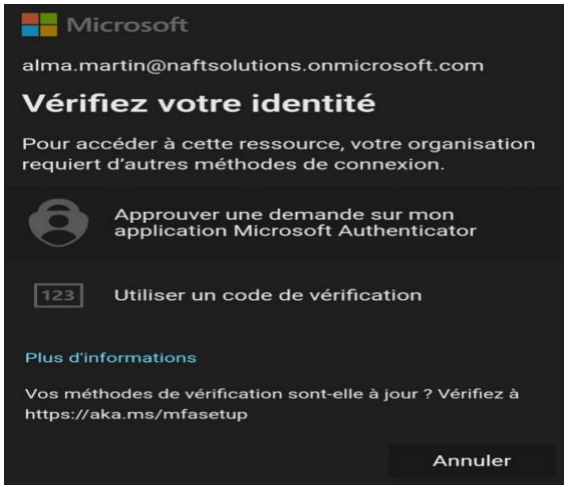

Figure 27 : Demande MFA.

La situation illustrée dans la Figure 28 serait atteinte si nous arrivions à passer outre cette demande de MFA.

Figure 28 : Échec de connexion.

La connexion est impossible, car notre équipement ne respecte pas les exigences de conformité requises. On peut observer dans la Figure 29 les politiques d'accès conditionnel qui ont été appliquées à cette connexion.

Figure 29 : Politiques d'accès conditionnel appliquées.

La politique de MFA basée sur le risque d'authentification est mise en œuvre, mais les deux politiques échouent car elles requièrent un appareil conforme. En outre, lors d'une tentative malveillante d'accéder au compte Alma depuis un lieu inhabituel (Somerville, Massachusetts, États-Unis via un VPN dans ce cas), plusieurs actions sont observées au Centre de sécurité Microsoft 365. Tout d'abord, le centre de sécurité génère une alerte en réponse à cette activité de connexion suspecte, comme le montrent les figures 30 et 31.

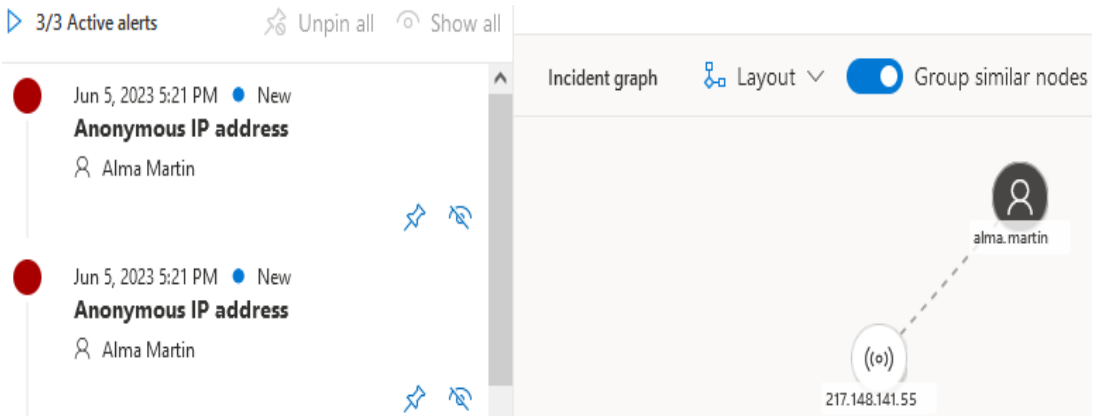

Figure 30 : Alerte d'activité de connexion risquée.

User name	alma.martin
User account	naftsol
IP address	217.148.141.55
Sign-in location	Somerville, Massachusetts, US
User Agent	Mozilla/5.0 (Linux; Android 12; SAMSUNG SM-M315F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/21.0 Chrome/110.0.5481.154 Mobile Safari/537.36
Sign-in request Id	72e7f19e-67b1-41d2-9947-717161ff1600

Figure 31 : Details d'alerte d'activité de connexion risquée.

Le deuxième constat révèle une élévation du niveau de risque de l'utilisateur Alma. La prochaine fois qu'Alma se connectera elle/il devra changer son mot passe comme indiqué dans la figure 32 suite aux exigences relatives aux politiques d'utilisation car il y a un risque utilisateur important.

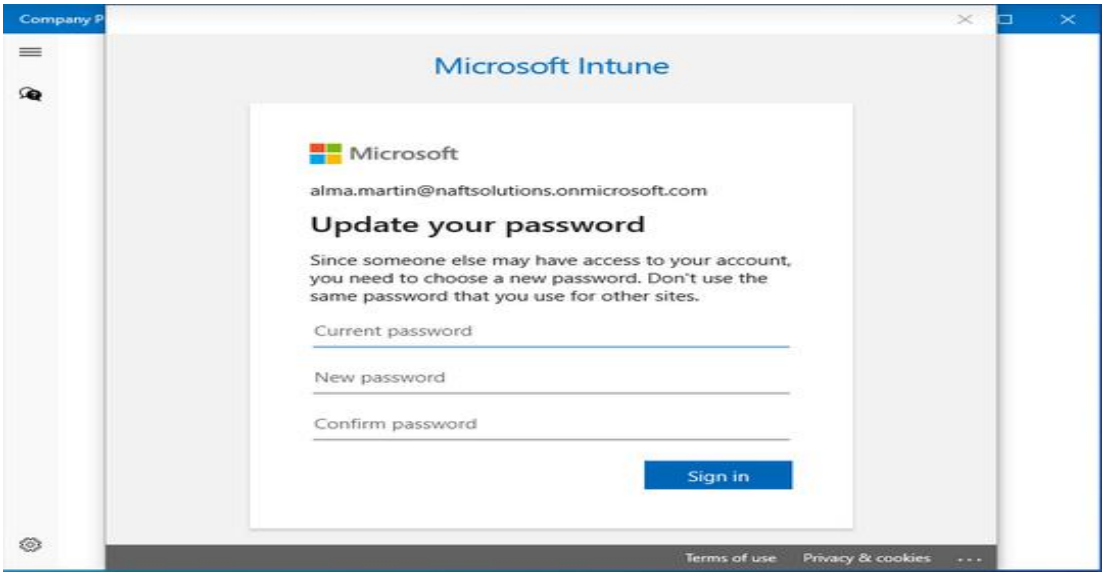

Figure 32 : Changement de mot de passe obligatoire.

4.2 Accès au portail d'entreprise via un appareil non conforme

En utilisant son appareil personnel, Alma souhaite se connecter au portail de l'entreprise en tant qu'employée. Cependant, son dispositif ne respecte pas les normes de sécurité du CIS (Center for Internet Security) ni les normes internes de l'entreprise définies sur Microsoft Intune. Si l'appareil non conforme de Alma essaie de se connecter, Intune prévient Alma par notification comme le montre la figure 33.

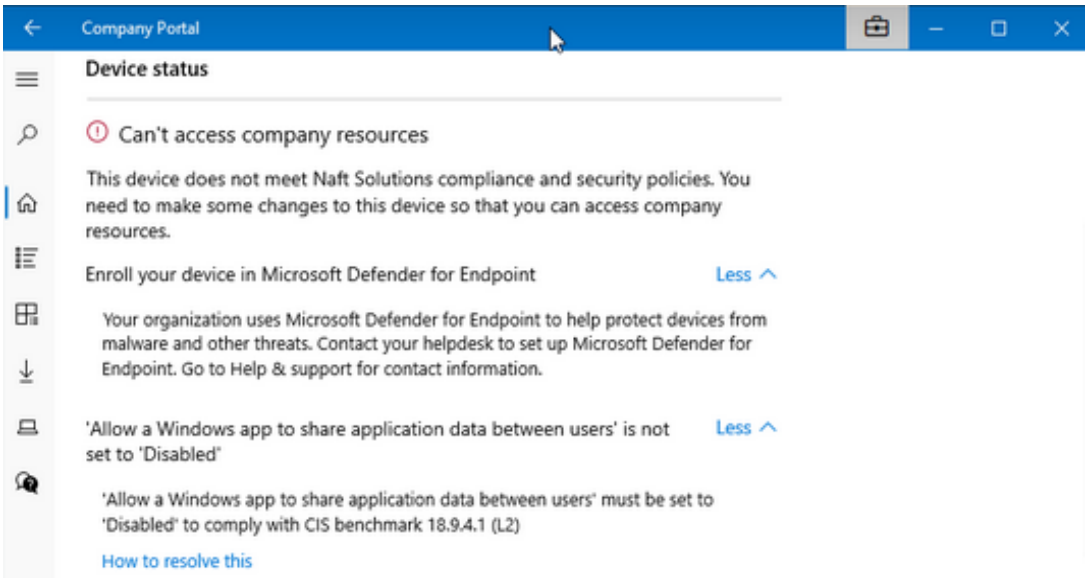

Figure 33 : Notifications de non-conformité.

Alma sollicite le service d'assistance technique en appelant le support informatique de son entreprise, et il est guidé par le service d'assistance informatique quant aux exigences spécifiques de conformité et reçoit des instructions sur la façon dont elle peut rendre son appareil conforme. Après avoir apporté les corrections nécessaires, Alma tente encore une fois d'accéder au portail. Intune a constaté que toutes les exigences étaient désormais satisfaites pour l'appareil appartenant à Alma, ce qui lui permet de connecter avec succès sur le portail de l'entreprise et d'avoir un accès complet aux ressources dont il a besoin pour travailler. (Voir figure 34)

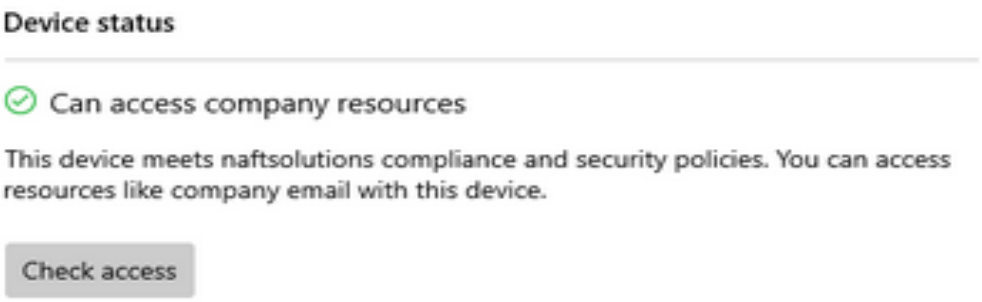

Figure 34 : Possibilité d'accéder aux ressources de l'organisation.

5. CONCLUSION

En conclusion, nous avons démontré dans ce chapitre comment mettre en place une solution qui permet de sécuriser et gérer les points de terminaison dans un environnement télétravail. La première étape du processus impliquait la création d'un active directory local qui est ensuite synchronisé avec Azure Active Directory. Ensuite, nous avons utilisé différents types de politiques de sécurité implémentées sur Microsoft Intune pour assurer la conformité avec les normes CIS en mettant en place une architecture de zero trust. Ainsi, nous avons expliqué l'enrôlement automatique des appareils, les fonctionnalités de gestion des applications, et le rôle de l'intégration de Power BI et Microsoft Defender. Par la suite, nous avons présenté la console Web que nous avons développé et nous avons fini par la mise en scène de deux cas d'utilisation pour tester notre solution.

CONCLUSION GENERALE

Ce projet de fin d'études a porté sur la sécurité et la gestion des points de terminaison et des applications, un aspect critique de la protection des systèmes d'information. Notre objectif principal était de mettre en place une solution efficace pour garantir la sécurité et la gestion des points de terminaison et des applications au sein de NAFTAL.

Nous avons réussi à atteindre nos objectifs en concevant et en implémentant une architecture de sécurité solide pour les points de terminaison et les applications. Nous avons mis en place des mesures de protection avancées. Les avantages offerts par cette solution incluent une gestion centralisée simplifiée des points de terminaison et des applications et des applications, surveillance continue en temps réel ainsi que l'application de politiques de sécurité strictes.

En testant notre solution, nous avons pu confirmer son efficacité dans la détection et le blocage des attaques sur les points de terminaison. De plus, nous avons mis en place des mécanismes de réponse appropriés pour minimiser les risques pour l'ensemble du réseau.

La solution peut être améliorée en renforçant les fonctionnalités de la console web et en intégrant l'intelligence artificiel et l'apprentissage automatique pour renforcer l'aptitude à identifier les comportements anormaux, ce qui permet de mieux détecter les anomalies et de prendre des mesures préventives. De plus, en améliorant la convivialité et les fonctionnalités de la console web, les administrateurs peuvent accéder et gérer plus facilement les services clés.

En conclusion, ce stage a été une très bonne expérience pour nous en tant qu'étudiants en sécurité des systèmes d'information car il nous a permis d'appliquer nos connaissances théoriques, d'acquérir de nouvelles connaissances et d'améliorer notre capacité à communiquer, à collaborer et à nous adapter au milieu professionnel en travaillant sur un projet dans une grande entreprise nationale.

REFERENCES

[1] K. H. H. A. &. Y. M. Mohammed, «Identity and Access Management System: A Web-Based Approach for an Enterprise,» 2018.

[2] A. &. L. R. O'Connor, «Economic analysis of role-based access,» RTI International Report Number: RTI, 2010.

[3] National Institute of Standards and Technology, «Zero Trust Architecture,» National Institute of Standards and Technology, 2020.

[4] H. &. T. R. Kaur, «Endpoint detection and response using machine learning,» IOP, 2021.

[5] R. M. &. L. R. T. Lee, «Sans 2018 threat hunting survey results,» SANS Institute Reading Room, 2018.

[6] T. &. L. P. Liliengren, «Threat hunting, definition and framework,» 2018.

[7] A. P. &. P. R. E. Sari, «The impact of cloud computing technology implementation on information security in higher education institutions,» IOP, 2020.

[8] Microsoft, «Qu'est-ce que la gestion des appareils?,» Microsoft Learn, n.d..

[9] TechTarget, «What is Mobile Application Management (MAM)?,» SearchMobileComputing, n.d..

[10] J. Kujo, «Enhancing security of cloud services with Microsoft Enterprise Mobility + Security,» Theseus Digital Repository, 2015.

[11] F. Times, «Administrative Security Controls,» Firewall Times, n.d..

[12] Microsoft, «Qu'est-ce que Microsoft Intune?,» Microsoft, n.d..

[13] ManageEngine, «Logiciel de gestion des appareils mobiles (MDM),» ManageEngine, n.d..

[14] IBM, «Getting started with the MaaS360 portal,» IBM Knowledge Center, n.d..

[15] TrustRadius, «IBM MaaS360 Reviews: Pros and Cons,» TrustRadius, n.d..

[16] Microsoft, «Azure Active Directory,» Microsoft, n.d..

[17] Microsoft, «Microsoft Intune,» Microsoft, n.d..

[18] Microsoft Power BI Consulting, «Types of Licensing in Power BI,» Microsoft Power BI Consulting, n.d..

[19] Microsoft Defender for Endpoint documentation, «Microsoft Defender for Endpoint licensing,» Microsoft, n.d..

[20] Microsoft, «Active Directory Domain Services Overview,» Microsoft, n.d..

[21] Microsoft Learn, «What is Azure AD Connect?,» Microsoft Learn, n.d..

[22] Microsoft Security, «Privileged identity management (PIM),» Microsoft Security, n.d..

[23] K. Järvemets, «Azure Active Directory Privileged Identity Management and Authentication Context,» Kaido Järvemets Blog, 2020.

[24] M. Learn, «What is Microsoft Intune,» Microsoft Learn, n.d..

[25] TechTarget, «Top 4 unified endpoint management software vendors in 2023,» TechTarget, n.d..

[26] Microsoft Learn, «Device compliance policies in Microsoft Intune,» Microsoft Learn, n.d..

[27] Nerdio Help Center, «Overview of Intune Policies and Configurations,» Nerdio Help Center, n.d..

[28] Microsoft Learn, «App protection policies overview,» Microsoft Learn, n.d..

[29] Microsoft, «Microsoft Defender Antivirus in Windows 10,» Microsoft, n.d..

[30] Microsoft, «What is Microsoft Defender for Endpoint?,» Microsoft, n.d..

[31] Microsoft, «Zero Trust security model,» Microsoft, n.d..

[32] Microsoft, «Microsoft Defender for Endpoint security configuration,» Microsoft, n.d..

[33] Microsoft, «Power BI documentation,» Microsoft, n.d..

[34] Microsoft, «Documentation de Microsoft Graph,» Microsoft, n.d..

[35] Microsoft, «Plateforme d'identité Microsoft et flux d'autorisation par code OAuth 2.0,» Microsoft, n.d..

[36] Microsoft, «Référence des autorisations de Microsoft Graph,» Microsoft, n.d..

[37] Vue.js, «Introduction,» Vue.js, n.d..

[38] Vuetify, «À propos,» Vuetify, n.d..

[39] AX OS, «Introduction,» AX OS, n.d..

[40] OASIS, «eXtensible Access Control Markup Language (XACML),» 2005.

[41] Microsoft Learn, «Identity and access management,» Microsoft Learn, n.d..

[42] Microsoft Learn, «High-level architecture of Microsoft Intune,» Microsoft Learn, n.d..

[43] Microsoft, «Defender for Endpoint demonstrations,» Microsoft Learn, n.d..

[44] Guru99, «Power BI Tutorial,» Guru99, n.d..

[45] Microsoft Learn, «Microsoft Graph overview,» Microsoft Learn, n.d..