

Comment sécuriser votre système d'information avec Microsoft Defender for Business ?

Mardi 16 mai 2023



Sommaire

01. La cybersécurité en quelques mots
02. Microsoft Defender
03. Microsoft Defender for Business
04. L'approche et le déploiement par BS Empower
05. Questions & Réponses



Lucile GRAS

Directrice Marketing



Antoine LOREAU

Consultant Avant-vente



Julien GUELLEC

Cloud Solution Architect Microsoft



01. La cybersécurité en quelques mots

« Il faut rendre la sécurité numérique sexy, c'est-à-dire compréhensible et mettre dans la tête de nos dirigeants que ce n'est pas un mal nécessaire mais absolument indispensable pour le développement de l'entreprise »

Guillaume Poupard, ancien directeur général de l'ANSSI

Définitions

« La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. »

Source Kaspersky

« La cybersécurité est la pratique consistant à protéger les systèmes, les réseaux et les programmes contre les attaques numériques. Ces cyberattaques visent généralement à accéder à des informations sensibles, à les modifier ou à les détruire, à extorquer de l'argent aux utilisateurs, ou à interrompre les processus normaux de l'entreprise. »

Source Cisco

Nouveau paradigme

La sécurisation des systèmes d'information est une guerre incessante qui nécessite de se préparer aux attaques.

La sécurité consiste à comprendre les menaces et à faire le nécessaire pour les atténuer, mais il est impossible de parer toutes les attaques.

C'est pourquoi, il est important d'adopter une stratégie et une approche de défense en profondeur fondées sur le risque.



La sécurité est une priorité pour les clients PME

+300%

d'attaques de ransomwares au cours de l'année écoulée, dont plus de 50 % ont ciblé les petites entreprises¹



1 in 4

Près d'une PME sur quatre déclare avoir subi une faille de sécurité au cours de l'année écoulée³

70%

Plus de 70 % des PME pensent que les cybermenaces deviennent davantage un risque commercial³

90%

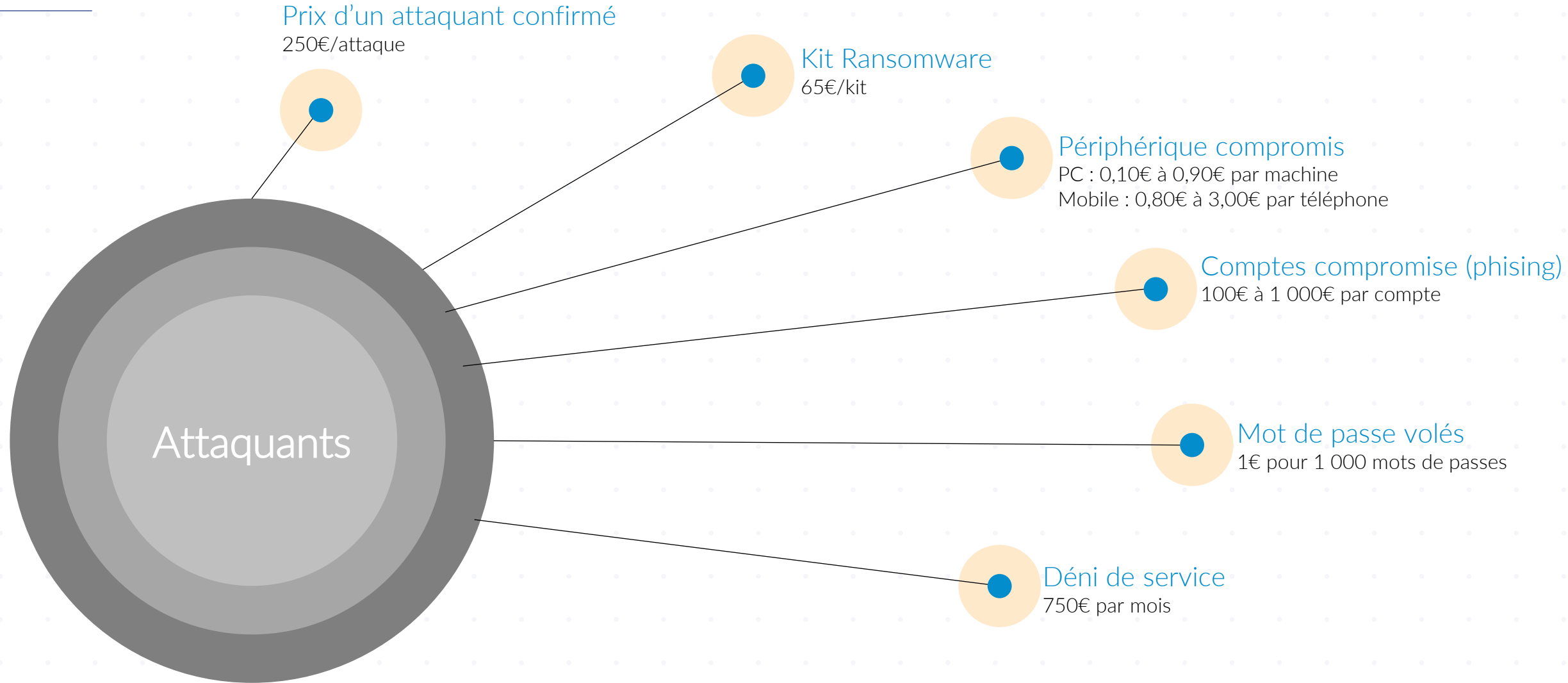
Les PME envisageraient d'embaucher un nouveau MSP s'ils offraient la bonne solution de cybersécurité⁴



\$108K

coût moyen d'une violation de données dans une PME.⁵

Produits d'attaque en vente sur Internet



Les actes de cyber-malveillance en 2021*

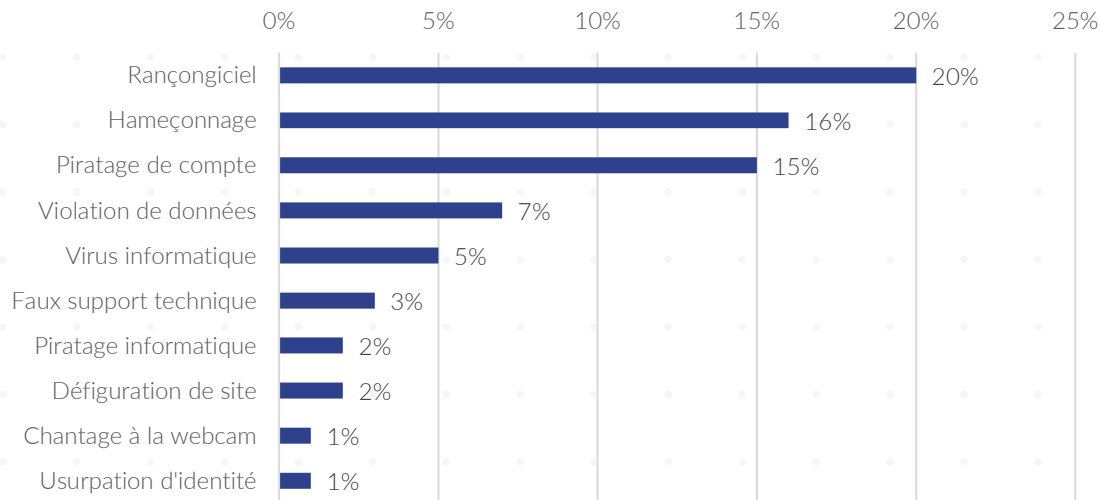
Les rançongiciels :
première menace
pour les entreprises et les collectivités

+95%
de hausse
en 2021

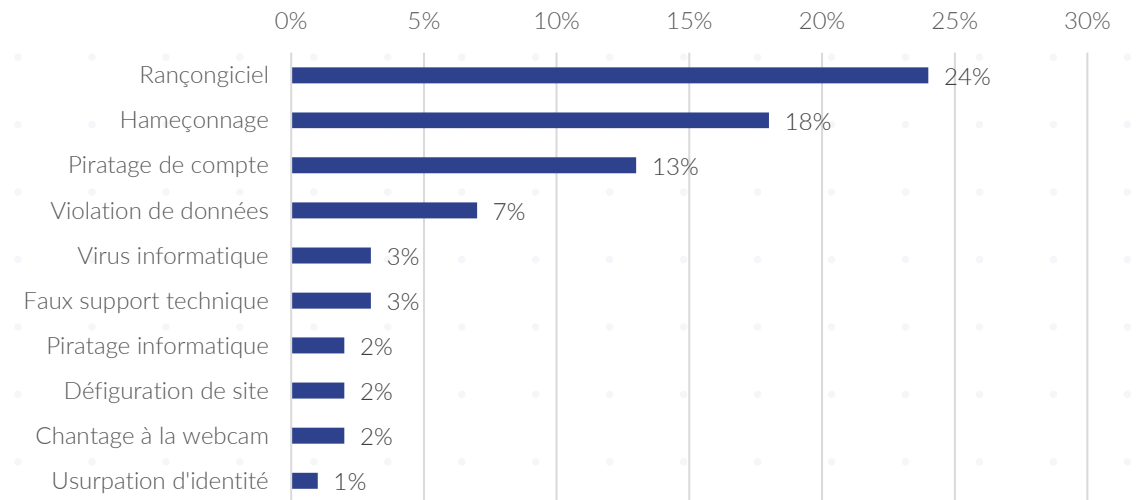
Le piratage de compte :
les messageries
de plus en plus ciblées

+139%
de piratage de
compte en 2021

Principales recherches d'assistance pour les collectivités et administrations



Principales recherches d'assistance pour les entreprises





02.
Microsoft Defender (XDR)

Microsoft Entra



Sécurisation des accès

Gestion des identités et des accès dans votre environnement

- Politiques adaptatives fondées sur les risques
- Expérience transparente pour tout utilisateur
- Gestion unifiée des identités et accès
- Simplification du cycle de vie



Visibilité et contrôle

Gouvernance des identités, des accès et des permissions en environnement multi-cloud

- Visibilité des identités et accès aux ressources
- Détecter les autorisations inutilisées ou excessives
- Automatisation du principe de moindre privilège



Vérification d'identité

Vérifier les informations d'identification en fonction des standards d'identité décentralisées

- Créer une confiance avec des informations d'identification vérifiables
- Intégrez et récupérez les comptes plus rapidement
- Accès sécurisé aux applications
- Donner aux individus le contrôle sur leurs données



Comprendre et gouverner les données

Gérer la visibilité et la gouvernance des données dans votre environnement

- Cartographier vos données
- Rendre les données facilement détectables
- Gérer le partage et l'accès aux données



Protégez les données, où qu'elles se trouvent

Protégez les données sensibles dans les clouds, les applications et les périphériques

- Protégez les données sensibles où qu'elles se trouvent
- Empêcher le partage accidentel de données
- Classer et gouverner à l'échelle de l'entreprise



Améliorer la posture de risque et de conformité

Identifier les risques liés aux données et gérer les exigences de conformité réglementaire

- Gérer les risques internes et la conformité
- Enquêter sur les violations de stratégie
- Réduisez les risques grâce à l'automatisation

Microsoft Priva



Gestion de la confidentialité

Protégez les données personnelles et créez un environnement de travail résilient en matière de protection de la vie privée

- Identifier les risques et les conflits critiques en matière de protection de la vie privée
- Automatisez les opérations de confidentialité et les réponses aux demandes de droits des objets
- Permettre aux utilisateurs de gérer efficacement les données et de prendre des mesures pour se conformer à l'évolution des réglementations en matière de confidentialité

Microsoft Defender



Protection contre les menaces

Stoppez les menaces dans l'ensemble de votre organisation

- Sécurisez tous les clouds, toutes les plateformes
- Bénéficiez d'une protection intégrée
- Réponse rapide et intelligente



Sécurité des clouds

Bénéficiez d'une protection intégrée pour vos ressources, applications et données multi-cloud

- Renforcez votre posture de sécurité
- Protégez-vous contre l'évolution des menaces
- Contrôler l'accès aux applications et aux ressources critiques
- Créez des applications nativement sécurisées

Microsoft Intune



Gestion des périphériques

Propulsez l'avenir du travail avec un patrimoine numérique moderne et sécurisé

- Gérez les périphériques de manière unifiée (bureau, mobiles et virtuels)
- Protéger les applications et périphériques
- Simplifiez les charges de travail informatiques et mettez à l'échelle les déploiements avec le cloud



Identities



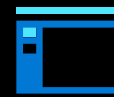
Périphériques



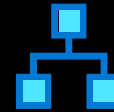
Données



Infrastructure



Apps



Réseau

Microsoft Defender

XDR

Microsoft 365 : Meilleurs outils de sécurité du marché



Identités

Microsoft Defender
for Identity



Anciennement Azure Advanced
Threat Protection



Périphériques

Microsoft Defender
for Endpoint



Anciennement Microsoft Defender
Advanced Threat Protection



Applications Cloud

Microsoft Cloud
App Security



Données utilisateurs

Microsoft Defender
for Office 365



Anciennement Microsoft Office 365
Advanced Threat Protection

Passer de silos individuels à une sécurité cross-domain

03. Microsoft Defender for Business

Assurer la sécurité des terminaux sur toutes les plateformes



 Windows



macOS

Terminaux et serveurs



Azure
Virtual Desktop



Windows 365

Bureaux virtuels



iOS

Périphériques mobiles

Cisco

Juniper Networks

HP Enterprise

Palo Alto Networks

Périphériques réseau



Microsoft Defender for Business

→ Améliorez votre sécurité ←



Gestion des menaces
et des vulnérabilités



Réduction de la
Surface d'Attaque



Protection Next
Generation



Endpoint Detection
& Response



Auto Investigation &
Remédiation






Intégration et
administration simplifiées

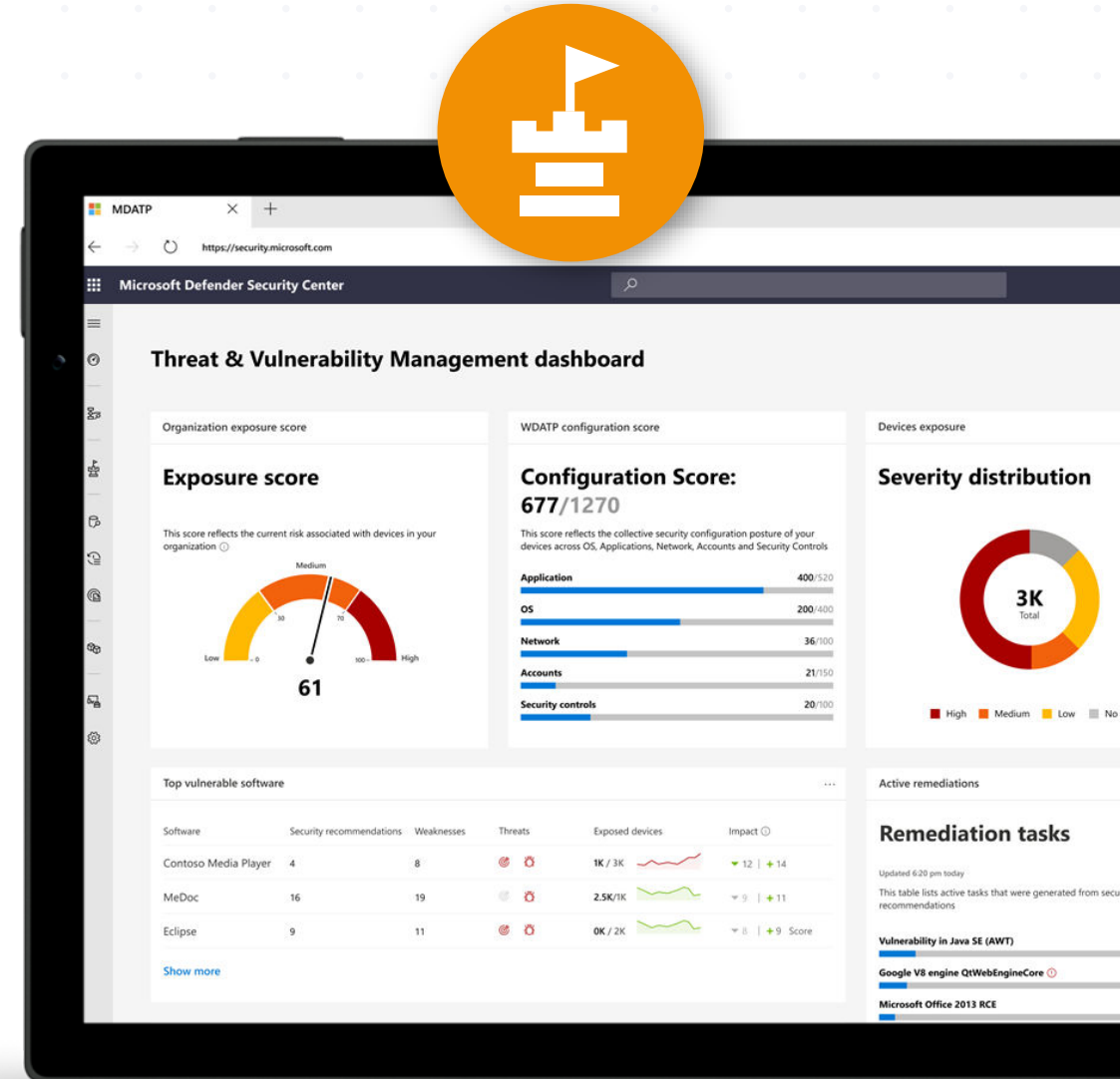


APIs et Intégration

Gestion des menaces et des vulnérabilités

Une approche basée sur le risque pour évaluer le niveau de gestion

- 1  Découverte en temps réel
- 2  Priorisation en fonction du contexte
- 3  Process de remediation construit de bout en bout



THREAT &
VULNERABILITY
MANAGEMENT



ATTACK SURFACE
REDUCTION



NEXT GENERATION
PROTECTION



ENDPOINT DETECTION
& RESPONSE



AUTO INVESTIGATION
& REMEDIATION

Réduction de la Surface d'Attaque

Éliminer les risques en réduisant la surface d'attaque



Durcissement du système, sans interruption



Personnalisation adaptée à votre organisation



Visualisez l'impact et activez-le simplement



THREAT & VULNERABILITY MANAGEMENT



ATTACK SURFACE REDUCTION



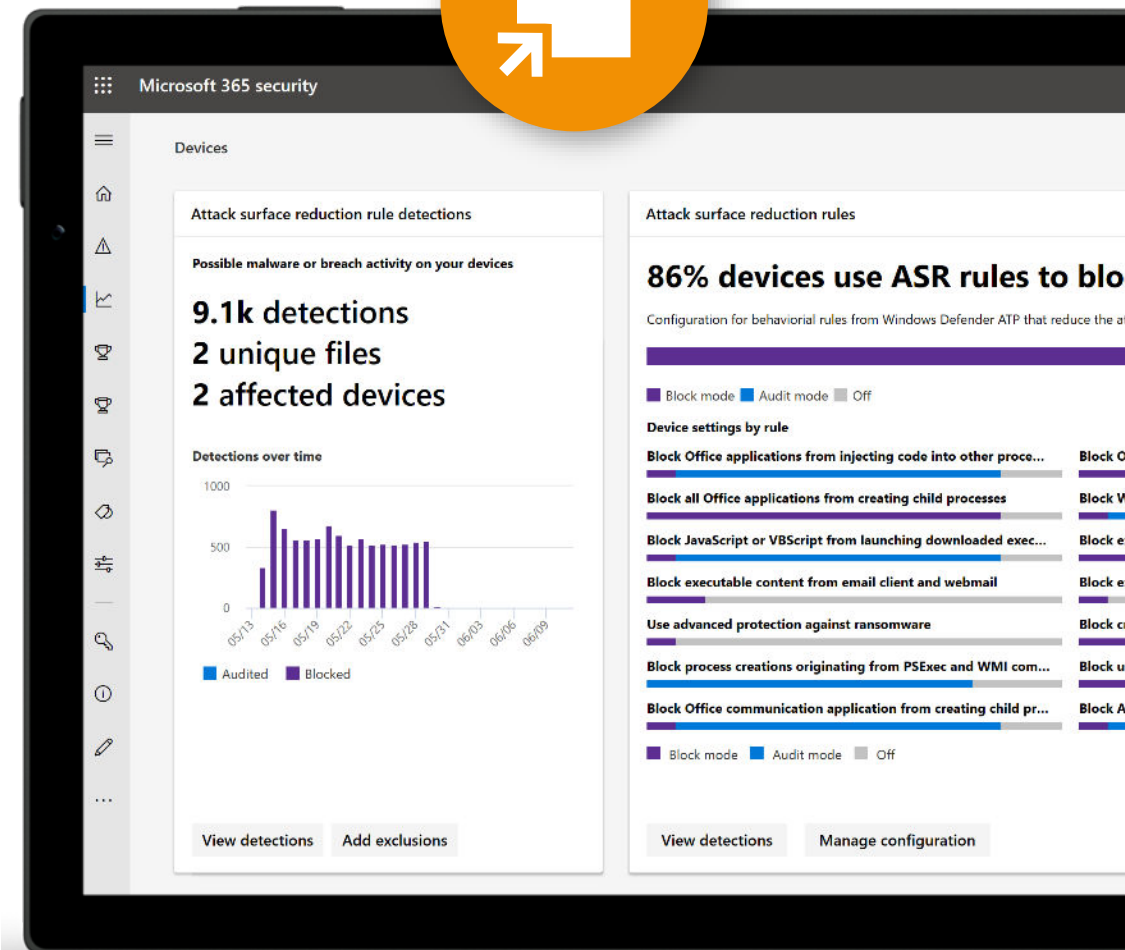
NEXT GENERATION PROTECTION



ENDPOINT DETECTION & RESPONSE



AUTO INVESTIGATION & REMEDIATION



Protection Next Generation

Bloque et s'attaque aux menaces sophistiquées et aux logiciels malveillants



Protection comportementale en temps réel



Bloque les logiciels malveillants



Arrête les activités malveillantes provenant d'applications fiables et non fiables



THREAT &
VULNERABILITY
MANAGEMENT



ATTACK SURFACE
REDUCTION



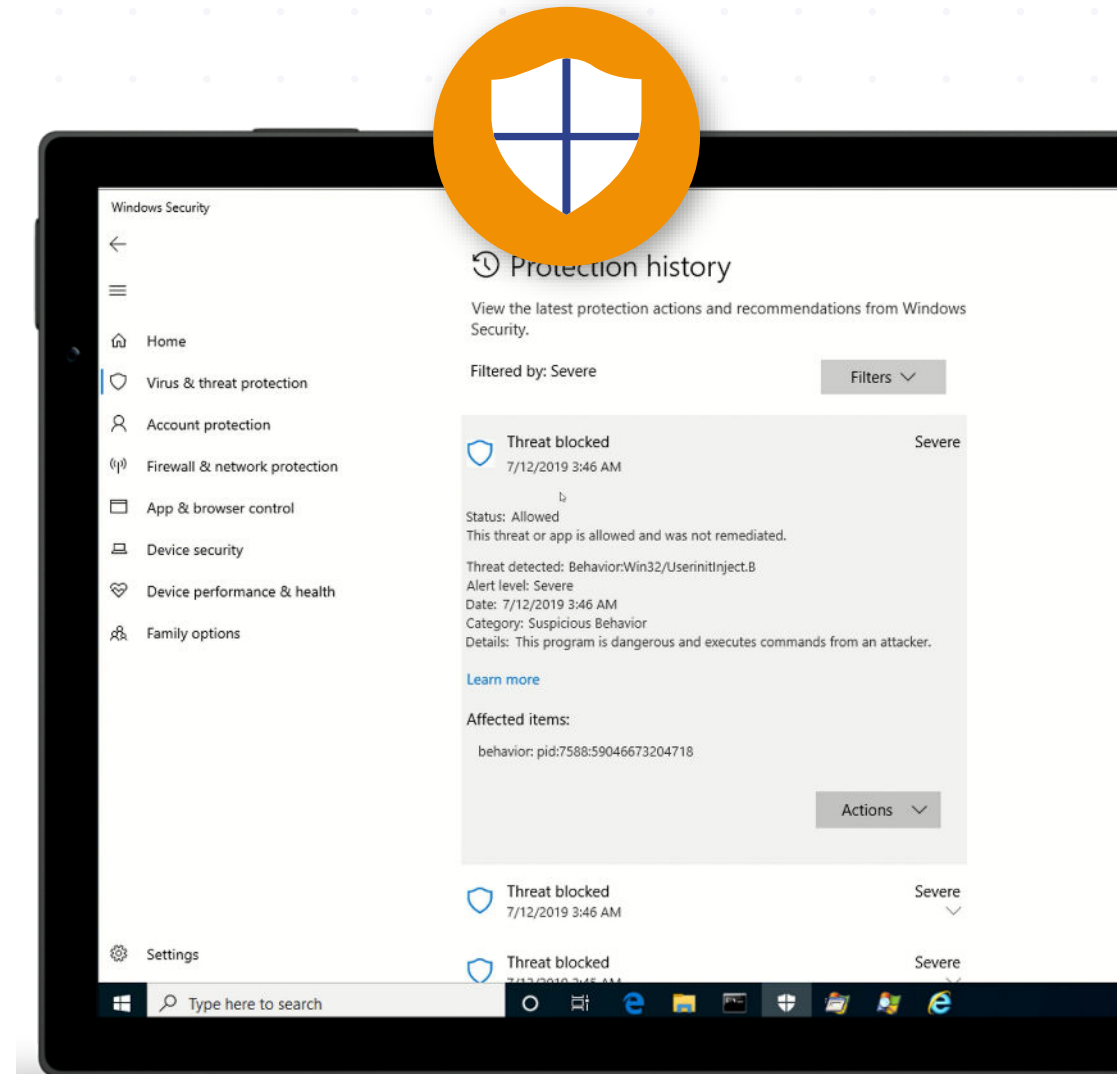
NEXT GENERATION
PROTECTION



ENDPOINT DETECTION
& RESPONSE



AUTO INVESTIGATION
& REMEDIATION



Endpoint Detection & Response

Détection et analyse avancée des attaques



Correlation des alertes



Investigation et "chasse" (Hunting)



Variété étendue d'actions de rémédiation



THREAT &
VULNERABILITY
MANAGEMENT



ATTACK SURFACE
REDUCTION



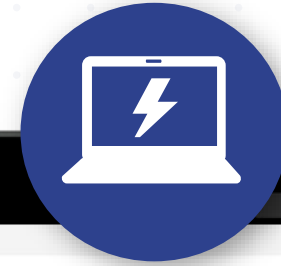
NEXT GENERATION
PROTECTION



ENDPOINT DETECTION
& RESPONSE



AUTO INVESTIGATION
& REMEDIATION



| Incident name | Severity | Category | Alerts | Machines | Users | Last activity | Classification |
|---------------|----------|---|--------|----------|-------|-------------------|----------------|
| 2195 | Medium | General, Persistence, Suspicious Activity, Delivery | 11 | ... | ... | 10/17/18, 5:25 PM | Not set |
| 2195 | Medium | Installation | 1 | ... | ... | 10/17/18, 4:04 PM | Not set |
| 2191 | Medium | General, Suspicious Activity | 2 | ... | ... | 10/16/18, 6:57 AM | Not set |
| 2184 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 7:31 AM | Not set |
| 2182 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 7:12 AM | Not set |
| 2193 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 7:25 AM | Not set |
| 2190 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 5:59 AM | Not set |
| 2189 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 6:30 AM | Not set |
| 2188 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 2:04 AM | Not set |
| 2185 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/15/18, 5:32 PM | Not set |
| 2187 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/15/18, 5:55 PM | Not set |
| 2186 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/15/18, 5:48 PM | Not set |
| 2184 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/15/18, 5:26 PM | Not set |
| 2185 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/15/18, 5:19 PM | Not set |
| 2182 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 2:59 PM | Not set |
| 2181 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 2:27 PM | Not set |
| 2180 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 2:30 PM | Not set |
| 2178 | Low | Suspicious Network Traffic | 1 | ... | ... | 10/16/18, 2:22 PM | Not set |

Auto Investigation & Remediation

Investigation automatique des menaces complexes en quelques minutes



Reproduit les actions qu'un analyste ferait



Gère les attaques par fichiers et attaques basées sur la mémoire



Fonctionne en 24x7, sans limitation de capacité



THREAT &
VULNERABILITY
MANAGEMENT



ATTACK SURFACE
REDUCTION



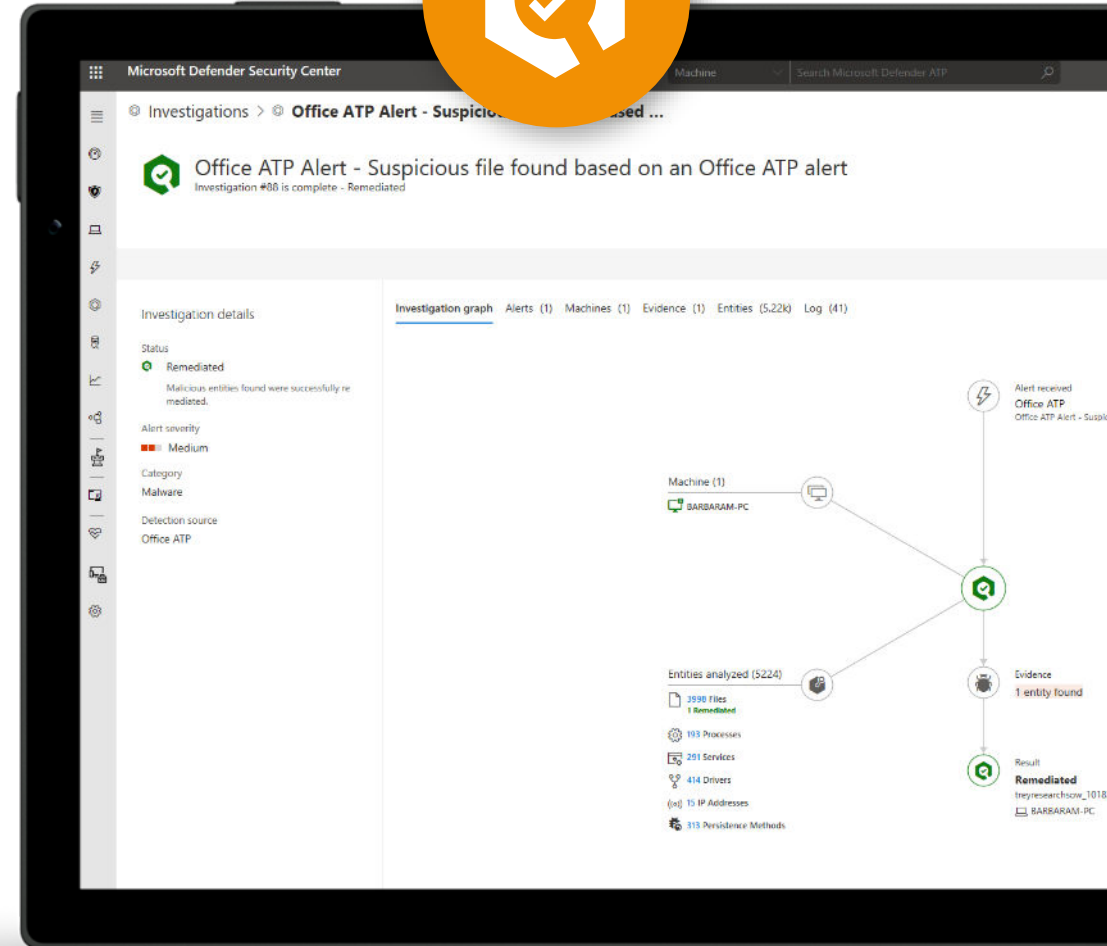
NEXT GENERATION
PROTECTION



ENDPOINT DETECTION
& RESPONSE



AUTO INVESTIGATION
& REMEDIATION



API partenaires
Connexion avec la
plateforme



Microsoft Defender for Business

Améliorez votre sécurité



Gestion des menaces
et des vulnérabilités



Réduction de la
Surface d'Attaque



Protection Next
Generation



Endpoint Detection
& Response



Auto Investigation &
Remédiation



APIs and Integration



Périphériquess



Rapports



Applications



Données SIEM



Outils

Comparaison de produit

Cross platform and enterprise grade protection with next-gen protection, endpoint detection and response, and threat and vulnerability management

Preview as a standalone offering and generally available as part of Microsoft 365 Business Premium

Standalone offering will serve non-Microsoft 365 customers. No licensing prerequisites

Supports multi-customer viewing of security incidents with Microsoft 365 Lighthouse for partners

| Customer size | < 300 licences | | > 300 licences | |
|--|---------------------------------|--|--|--|
| Endpoint capabilities\SKU | Microsoft Defender for Business | Microsoft Defender for Endpoint Plan 1 | Microsoft Defender for Endpoint Plan 2 | |
| Centralized management | X | X | X | |
| Simplified client configuration for Windows | X | | | |
| Threat and Vulnerability Management | X | | X | |
| Attack Surface Reduction | X | X | X | |
| Next-Gen Protection | X | X | X | |
| Endpoint Detection and Response | X ¹ | | X | |
| Automated Investigation and Response | X ¹ | | X | |
| Threat Hunting and 6-months data retention | | | X | |
| Threat Analytics | X ¹ | | X | |
| Cross platform support for Windows, MacOS, iOS, and Android | X ³ | X | X | |
| Microsoft Threat Experts | | | X | |
| Partner APIs | X | X | X | |
| Microsoft 365 Lighthouse for viewing security incidents across customers | X ² | | | |



¹Optimized for SMB. ²Additional capabilities planned ³iOS, and Android requires Microsoft Endpoint Manager. Please see [Documentation](#) for more detail.



04. Approche et déploiement

Onboarding des machines



L'intégration des machines à Defender for Business se nomme « onboarding » ou « intégration ».

Windows Defender se *connecte* à Defender for Business et remonte les données d'investigation des machines vers Microsoft Azure.

Intégration des Clients :

Windows 10 + :

- + Par Script
- + Par GPO (via fichier d'onboarding)
- + Par Microsoft Intune
- + Par SCCM

MacOS :

- + Par Script
- + Par Microsoft Intune

Intégration des Serveurs :

Windows Serveur 1809 et supérieur :

- + Par Script (pour test)
- + Par GPO (via fichier d'onboarding)
- + Par Microsoft Intune
- + Par SCCM

Windows Serveur 2012^{R2} et 2016 :

- + Par Script (pour test)
- + Par GPO (mdw4s.msi + onboarding)
- + Par SCCM

Windows Serveur 2008^{R2} sp1 et 2012 :

- + Par Script (pour test)
- + Par GPO (Microsoft Monitoring Agent)
- + Par SCCM

Linux :

- + Par Script

Configuration de Microsoft Defender for Business



Après avoir intégré des machines, il faut configurer l'agent.

Configuration des Clients :

Windows 10 + :

- + Par Script Powershell
- + Par GPO
- + Par Microsoft Intune
- + Par SCCM

MacOS :

- + Par Script
- + Par Microsoft Intune

Configuration des Serveurs :

Windows Serveur 2012R2 et supérieur :

- + Par Script Powershell
- + Par GPO
- + Par Microsoft Intune
- + Par SCCM

Linux :

- + Déploiement de fichiers de config (via Ansible ou tout autre outil de déploiement)

05. Corpus



Blue Soft Empower — Corpus

Microsoft 365 Defender
sécurise tout l'environnement
M365

Comment Microsoft 365 peut
vous aider à faire face à
l'inflation

Sécuriser vos périphériques

Comment construire une
stratégie de sécurité efficace ?

Comprendre le concept de
Confiance Zéro (Zero Trust) en 2
minutes

Les solutions Microsoft pour se
prémunir contre les
cyberattaques



06. Questions & Réponses



Questionnaire de satisfaction





Merci !

www.bluesoft-group.com

