Guide pratique

Cybersécurité : les 4 failles à combler dans une TPE/PME

bouygues TELECOM Pro

Édito

Bouygues Telecom Pro : le partenaire de votre cybersécurité

À l'heure où les cyberattaques se multiplient, votre PME se retrouve en première ligne. Selon une étude récente[1] **72 % des PME ne disposent pas de personne spécifiquement en charge de l'informatique.** Or, cela vous rend particulièrement vulnérable. Dans les faits, la question n'est plus de savoir si votre entreprise sera attaquée, mais quand.

Face à cette réalité implacable, vous pouvez agir simultanément autour de 4 axes essentiels : **l'accès internet, les messageries électroniques, les postes utilisateurs, et le réseau.** Pour mettre en œuvre cette stratégie globale, Bouygues Telecom Pro s'impose comme votre partenaire légitime dans la protection du patrimoine numérique de votre entreprise.

Situés au cœur de l'infrastructure numérique, nous bénéficions d'une vision panoramique des flux de données et des menaces potentielles. Nous sommes en mesure de mutualiser les solutions de protection, rendant accessibles aux plus petites structures des technologies habituellement réservées aux grandes organisations. Cette démocratisation de la cybersécurité permet aux TPE et PME de bénéficier d'une protection de qualité à coût maîtrisé.

Notre valeur ajoutée réside dans notre capacité à proposer un **accompagnement sur mesure et continu.** C'est pourquoi nous assurons une veille constante en vue d'adapter nos solutions à l'évolution des menaces et des besoins spécifiques de chaque entreprise. Alors que votre dépendance au digital explose, la résilience cyber ne repose pas tant sur l'accumulation d'outils techniques que sur la qualité des partenariats noués. Notre expertise et notre position centrale au cœur de l'écosystème de la connectivité nous permet de nous positionner, à vos côtés, comme une sentinelle naturelle de votre environnement numérique.

Benjamin Laygnez
Responsable marketing data, cloud & cybersécurité,
Bouygues Telecom division Entreprises

Source : (1) Étude OpinionWay 2024

Sommaire

01

Contexte & enjeux

Votre urgence ? Comprendre la menace qui pèse sur votre entreprise

En tant que dirigeant de TPE/PME, vous ne pouvez plus ignorer la réalité : le risque cyber est omniprésent. Une prise de conscience collective est indispensable. Retenez ce chiffre : **49 % des PME ont déjà été victimes d'une cyberattaque**(1).

Cette statistique révèle l'ampleur du problème et la nécessité d'une action immédiate ! L'heure est à l'action. Abandonnez toute forme de déni : l'enjeu n'est plus d'éviter une attaque, mais de s'y préparer efficacement.

Source : (1) OpinionWay pour WatchGuard

Cybermenace : portrait d'une famille un peu trop nombreuse

L'EXPLOITATION DES VULNÉRABILITÉS

Les attaquants recherchent activement les failles des systèmes pour s'y infiltrer. **Le nombre d'attaques utilisant l'exploitation des vulnérabilités comme principal vecteur d'intrusion et de compromission a presque triplé en 12 mois (+ 180 %)**[1].

LE PHISHING

Cette technique d'ingénierie sociale reste un outil privilégié des cybercriminels. **24 % des attaques sont liées à du phishing**[1].

LES RANSOMWARES

Ces logiciels malveillants, qui prennent en otage les données, représentent une menace majeure pour votre organisation. Selon le rapport DBIR 2024 de Verizon[1], **près d'un tiers des compromissions impliquaient un ransomware ou d'autres techniques d'extorsion.**

LES ATTAQUES PAR DÉNI DE SERVICE (DDOS)

Ces attaques, qui visent à rendre un service indisponible en le surchargeant de requêtes, sont en forte augmentation. Dans son dernier rapport sur les menaces DDoS, Cloudflare[2] note une augmentation de 53 % des attaques par rapport à 2023.

Les conséquences : au-delà des pertes financières

- **L'impact opérationnel sur votre activité**
  29 % des PME ont connu des perturbations allant jusqu'à un arrêt de service[3]. Les conséquences sur la production, la logistique et les ventes peuvent être considérables..

- **La perte de vos données**
  la destruction ou le vol d'informations sensibles est une menace majeure. 25 % des entreprises victimes ont connu un vol de données via leur messagerie[1].
  La confidentialité et l'intégrité des informations sont compromises.

Sources : (1) cybermalveillance.gouv.fr (2) blog.cloudflare
(3) OpinionWay pour WatchGuard

- **Des risques juridiques**
  Le non-respect des réglementations sur la protection des données, comme le RGPD, peut entraîner des sanctions financières importantes. Bien que le montant exact dépende de l'infraction et de la taille de l'entreprise, les amendes liées aux violations de données peuvent être substantielles. **En 2023, la CNIL a sanctionné 36 entreprises et infligé des amendes pour près de 90 millions d'euros[1] !**

- **Les risques financiers directs**
  Selon les plaintes enregistrées par la cellule IC3 du FBI et relayées dans le DBIR 2024, les pertes médianes associées à la combinaison rançongiciels et extorsions s'élèvent en moyenne à **46 000 $[2]**. Les attaques de type BEC (Compromission de messagerie d'entreprise) entraînent également des pertes financières importantes, avec un montant d'environ **50 000 $[2].**

- **L'atteinte à votre réputation**
  80 % des entreprises craignent pour leur image en cas de cyberattaque. La communication de crise est un enjeu crucial.

Bon à savoir

Votre impératif ?
Agir dès aujourd'hui !

Vous ne pouvez plus vous permettre d'ignorer la menace cyber. La sécurité numérique doit devenir une priorité stratégique pour garantir non seulement la croissance sereine de votre activité, mais aussi pour préserver l'énergie de vos équipes.

Le facteur humain : votre première ligne de défense

Avec près de 7 compromissions de données sur 10 impliquant le facteur humain[3], vos collaborateurs sont à la fois votre plus grande vulnérabilité et votre meilleure protection face aux cybermenaces. Les risques principaux proviennent de comportements quotidiens : clic sur un lien frauduleux, utilisation de mots de passe faibles, partage d'informations sensibles sur des canaux non sécurisés.

Le temps de réaction est crucial : moins d'une minute suffit entre l'ouverture d'un e-mail malveillant et la saisie d'identifiants.

Pour transformer cette vulnérabilité en atout :

- Formez régulièrement vos équipes
- Mettez en place l'authentification multifactorielle
- Établissez des procédures de signalement
- Créez une culture de vigilance collective avec des challenges internes autour des questions de sécurité.

La cybersécurité n'est pas qu'une affaire technique ; c'est avant tout une question d'humains conscients et vigilants.

Sources : (1) blog.cloudflare (2) OpinionWay pour WatchGuard
(3) cybermalveillance.gouv.fr

Les 4 failles critiques dans votre système de défense

1. LES ACCÈS INTERNET

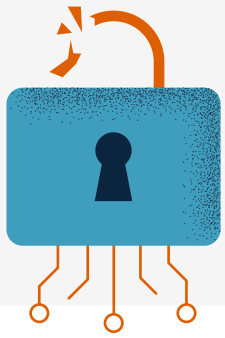
Point d'entrée privilégié pour les attaquants via des sites malveillants, téléchargements douteux ou connexions non sécurisées. Sans filtrage web efficace ni supervision des flux, votre entreprise reste exposée à de multiples vecteurs d'attaque invisibles.

2.LES MESSAGERIES ÉLECTRONIQUES

Cible prioritaire avec 24 % des attaques liées au phishing, le canal e-mail est un véritable cheval de Troie ! Un simple e-mail peut introduire des logiciels espions.

3. LES POSTES DE TRAVAIL

Maillons vulnérables à travers leurs systèmes d'exploitation et logiciels rarement mis à jour, l'absence d'antivirus performants ou des droits administrateur trop largement distribués. Les ordinateurs portables, souvent utilisés hors du périmètre sécurisé, multiplient les risques.



4. LE RÉSEAU D'ENTREPRISE

Dans les PME, le réseau (aussi bien local, notamment le WiFi, qu'étendu, c'est à dire l'interconnexion entre sites) est souvent insuffisamment segmenté. Il permet ainsi une propagation rapide des attaques d'un service à l'autre. Les équipements connectés non sécurisés et l'absence de surveillance des flux internes créent des angles morts exploitables par les cybercriminels.

02

Pourquoi protéger vos accès internet ?

66 %[1] des entreprises en France sont équipées d'un pare-feu. Ce chiffre peut sembler rassurant mais toutes les solutions de pare-feu ne se valent pas ! Un pare-feu obsolète ou mal configuré offre une protection illusoire. De plus, de nombreuses TPE/PME négligent leur mise à jour régulière, les exposant ainsi à de nouvelles vulnérabilités.

Quels sont les risques ?

Supposez qu'un de vos salariés se rende sur internet sans que vous n'ayez déployé de pare-feu ou mis en place une stratégie de filtrage web. S'il navigue sur un site web dangereux et télécharge un logiciel malveillant, celui-ci peut se propager sur votre réseau interne et paralyser votre activité.

Disposer d'un pare-feu ne suffit pas à garantir votre protection. S'il est mal configuré, les cybercriminels peuvent voler des données sensibles comme des informations clients, des documents commerciaux confidentiels. Cette fuite de données peut avoir de graves conséquences financières et réputationnelles !

Source : (1) Étude de Notoriété auprès des TPE/PME - Octobre 2024

Un pare-feu : comment ça marche ?

Imaginez un firewall comme un agent de sécurité posté à l'entrée de votre réseau d'entreprise. **Son rôle principal est de contrôler et de filtrer le trafic qui entre et qui sort de ce réseau.** Il agit comme une barrière de sécurité, examinant chaque « paquet » de données qui tente de passer.
Voici comment cela se passe !

1. INSPECTION DES PAQUETS

Chaque information qui transite sur Internet est divisée en morceaux appelés « paquets ».
Le firewall inspecte ces paquets en analysant : l'adresse IP de l'expéditeur et du destinataire, le port utilisé par l'application et le contenu du paquet.

2. APPLICATION DES RÈGLES DE SÉCURITÉ

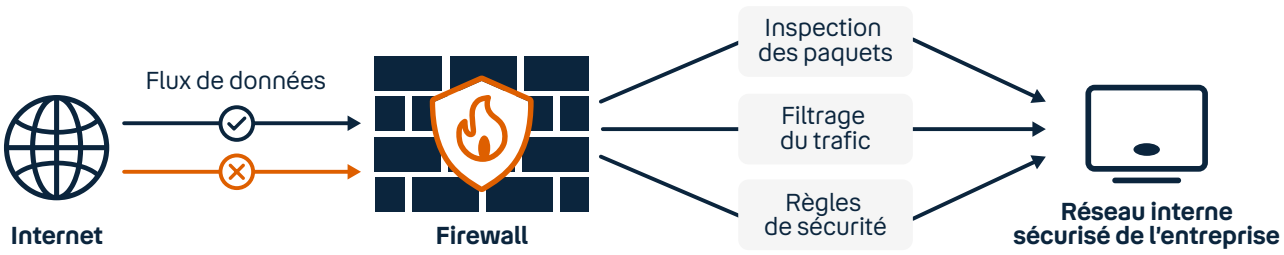
Le firewall fonctionne selon un ensemble de règles pré-établies par l'administrateur réseau. Elles définissent quels types de trafic sont autorisés à passer et quels types sont bloqués.

3. FILTRAGE DU TRAFIC

En fonction des paquets et des règles de sécurité, le firewall peut :

- **Autoriser le trafic :** si le paquet correspond aux règles définies.
- **Bloquer le trafic :** si le paquet ne correspond pas aux règles ou s'il est identifié comme malveillant.

Comment fonctionne un firewall ?



Protégez votre entreprise avec Fortinet

Selon un sondage réalisé par OpinionWay pour WatchGuard[1],

49 % des PME ont déjà été victimes d'une cyberattaque

dont

29 % d'entre elles ont connu des pertubations allant jusqu'à un arrêt de service

19 % des cyberattaques concernent un rançongiciel

21 % concernent le vol d'argent, à égalité avec la destruction et l'exfiltration de données

Face à la croissance des cyberattaques, la protection de votre accès internet est devenue une priorité absolue. Chez Bouygues Telecom Pro, nous nous engageons à vous fournir une solution répondant, point par point, aux besoins réels d'une entreprise comme la vôtre en s'appuyant sur un partenaire de premier plan : FORTINET.

Fortinet : un leader incontesté de la cybersécurité

Fortinet est un acteur majeur et un leader mondial dans le domaine de la cybersécurité. Sa position de leader se traduit par :

- **Une reconnaissance internationale**
  Fortinet est un éditeur reconnu pour la protection des réseaux, des utilisateurs et des données des entreprises.
- **Une part de marché significative**
  1 pare-feu sur 2 vendu dans le monde est un Fortinet, ce qui témoigne de la confiance accordée par les entreprises à ses solutions.
- **Une technologie éprouvée**
  Fortinet investit continuellement dans l'innovation pour proposer des solutions de sécurité performantes et adaptées aux enjeux actuels.
- **Une plateforme de sécurité intégrée**
  Sa plateforme Security Fabric offre une cybersécurité complète sur toute la surface d'attaque de votre PME en prenant en charge le trafic de données sur l'ensemble des accès.

Source : (1) WatchGuard

L'avis de l'expert

« Ce que les entreprises doivent comprendre, c'est l'adhérence totale entre l'accès internet et sa protection. Ils sont indissociables. Le pare-feu Fortinet n'est pas un simple ajout, mais une composante organique de l'accès internet. À ce titre, il constitue le socle de l'offre que nous avons élaboré avec soin pour les PME. Notre mission consiste à garantir aux entreprises cet ajustement pointilleux et cet accompagnement expert. »

Benjamin Laygnez
Responsable marketing data, cloud & cybersécurité,
Bouygues Telecom division Entreprises

À RETENIR

- Un pare-feu obsolète ou mal configuré expose votre entreprise aux intrusions et au vol de données sensibles.
- Le firewall inspecte chaque paquet de données, applique des règles de sécurité et filtre le trafic entrant et sortant.
- Le pare-feu doit être régulièrement mis à jour et adapté aux usages spécifiques de votre entreprise pour maintenir son efficacité.
- Un accompagnement expert permet d'ajuster précisément les règles de sécurité pour garantir une protection rigoureuse sans entraver la fluidité des accès.

03

Pourquoi protéger votre messagerie d'entreprise ?

Selon le Baromètre Cyber de Mailinblack[1], **2,5 % des e-mails reçus contiennent une cyberattaque**. Un chiffre rassurant ?
Pas vraiment car cela représente déjà près de **102 millions d'attaques !** La messagerie reste la porte d'entrée privilégiée des cybercriminels. Une vulnérabilité que de nombreuses TPE/PME sous-estiment encore. Selon l'étude de Notoriété[2] **67 % des PME françaises ont déjà subi une attaque informatique**, et **25 % des entreprises victimes ont connu un vol de données via leur messagerie.** Plus alarmant, **24 % des attaques étaient liées à du phishing**, ciblant directement les boîtes mail. Pourtant, **57 % des entreprises continuent d'utiliser une messagerie externe** (Gmail, Yahoo...) plutôt qu'une solution professionnelle sécurisée avec leur nom de domaine.

Sources : (1) Baromètre cyber 2023 (2) Étude de Notoriété - Octobre 2024

Quels sont les risques ?

Imaginez qu'un de vos salariés reçoive un e-mail semblant provenir de votre banque. Le message paraît légitime et contient un lien vers un « document important ». En cliquant, il est dirigé vers une page de connexion falsifiée où il saisit ses identifiants. Quelques heures plus tard, votre compte professionnel est vidé et votre système d'informations est paralysé.

Ce scénario de **phishing** n'est qu'un exemple parmi d'autres. Les cybercriminels utilisent aussi des pièces jointes infectées qui, une fois ouvertes, déclenchent **l'installation d'un malware**. Dans les cas les plus graves, ces attaques conduisent au chiffrement complet de vos données et à des **demandes de rançons** conséquentes, paralysant votre activité pendant des jours, voire des semaines.

Sécuriser votre messagerie : comment ça marche ?

Protéger votre messagerie nécessite une approche multicouche, capable d'analyser en profondeur chaque e-mail avant qu'il n'atteigne vos équipes. Voici comment fonctionne une solution de sécurité e-mail :

1. Analyse des expéditeurs : la solution vérifie l'authenticité de l'expéditeur grâce à des technologie comme :

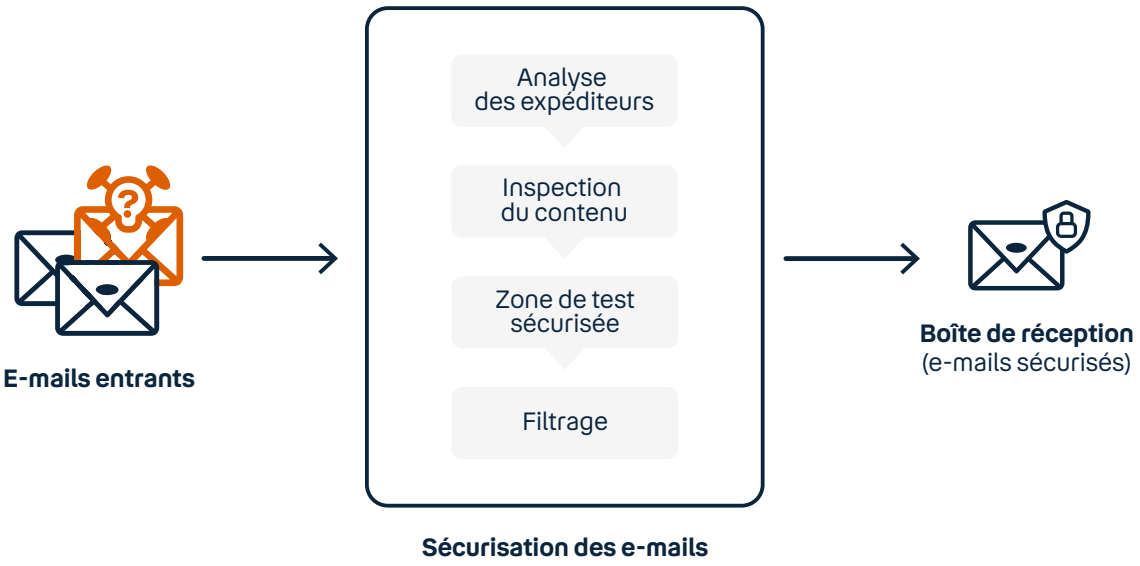
- **Sender Policy Framework** qui vérifie l'identité de l'émetteur,
- **DomainKeys Identified Mail** qui garantit que l'e-mail a été envoyé par le domaine qui prétend l'avoir envoyé et qu'il n'a pas été altéré,
- **Domain-based Message Authentification Reporting & Conformance** qui authentifie les e-mails pour éviter l'usurpation d'identité et le phishing.

2. Inspection du contenu : chaque e-mail est scanné pour détecter les contenus suspects, les liens malveillants et les pièces jointes dangereuses. Les technologies d'IA identifient même les menaces jamais vues auparavant.

3. Zone de test sécurisée (Sandbox) : les pièces jointes suspectes sont automatiquement ouvertes dans un environnement isolé pour observer leur comportement et s'assurer qu'elles sont sans risque.

4. Filtrage adaptatif des messages : la solution s'adapte aux nouvelles tactiques des cybercriminels et renforce ses capacités de détection.

Comment fonctionne une protection e-mail ?



Protégez votre messagerie d'entreprise

La boîte de réception de vos collaborateurs est la porte d'entrée privilégiée de toutes les organisations cybercriminelles. Prenez les mesures qui s'imposent sans délai.

Une solution de sécurité e-mail efficace doit réunir plusieurs fonctionnalités :

- **Une protection multicouche**
  La solution doit combiner plusieurs technologies de détection pour identifier et neutraliser les e-mails malveillants, du simple spam aux attaques les plus sophistiquées.
- **Une sandbox intégrée**
  Le système isole automatiquement les pièces jointes suspectes dans un environnement sécurisé pour les analyser sans risque pour votre infrastructure.
- **Une intelligence artificielle avancée**
  Permettant d'identifier les nouvelles tactiques d'attaque et assurant une protection proactive contre les menaces émergentes.
- **Une protection contre la fuite de données**
  La solution surveille également les e-mails sortants pour empêcher l'exfiltration accidentelle ou malveillante de données sensibles.

L'avis de l'expert

« S'appuyer sur un acteur de la stature de Fortinet, est un gage de sécurité indéniable. Le volume considérable de données traitées offre une connaissance approfondie des menaces qui rôdent. L'ampleur des données permet de décrypter les méthodes employées par les attaquants, de comprendre leurs logiques et de lire leurs actions. Déceler les signaux avant-coureurs est d'une importance capitale. Il faut savoir lire les signaux faibles. »

Benjamin Laygnez
Responsable marketing data, cloud & cybersécurité,
Bouygues Telecom division Entreprises

À RETENIR

- La messagerie constitue la voie d'accès privilégiée des cybercriminels, exposant les entreprises à des risques majeurs tant opérationnels que financiers et réputationnels.
- Une protection e-mail multicouche permet d'identifier et neutraliser efficacement toutes les menaces, du spam aux attaques ciblées les plus sophistiquées.
- L'utilisation d'une sandbox intégrée isole les pièces jointes suspectes dans un environnement sécurisé, préservant l'intégrité de votre infrastructure.

04

Comment renforcer la sécurité des équipements de vos collaborateurs ?

Selon une récente étude de Google Mandiant[1], les attaquants sont de plus en plus rapides pour mettre à profit les failles de sécurité qui peuvent apparaitre au gré des mises à jour des logiciels. **Là où il fallait auparavant (en 2023) 32 jours aux cyberattaquants pour identifier une faille et la mettre à projet, 5 jours suffisent aujourd'hui.**

Cette réalité met en lumière l'insuffisance des antivirus traditionnels face aux cyberattaques modernes. Dans ce contexte, une protection avancée des postes devient indispensable pour garantir la continuité de votre activité et seule une solution EDR (Endpoint Detection and Response) peut l'assurer efficacement.

Source : (1) How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

Quels sont les risques ?

Imaginez qu'un de vos collaborateurs reçoive un e-mail semblant provenir d'un fournisseur habituel. Il contient un document qui semble professionnel. Votre antivirus n'y détecte rien d'anormal et votre salarié ouvre la pièce jointe. En quelques secondes, un logiciel malveillant exploitant une faille « Zero-Day » (une vulnérabilité informatique n'ayant aucun correctif connu, s'installe sur son poste de travail, sans déclencher la moindre alerte). Le programme opère en toute discrétion pendant des semaines, exfiltrant des données sensibles.

Lorsque l'attaque est finalement détectée, le préjudice est considérable : fuite de données clients, vol d'informations bancaires et compromission des identifiants d'accès aux systèmes critiques de l'entreprise.

EDR : comment ça marche ?

Contrairement aux antivirus traditionnels, une solution EDR surveille le comportement des applications en temps réel. Cette approche permet de détecter des menaces jamais observées auparavant. Voici comment fonctionne un système EDR :

1. SURVEILLANCE COMPORTEMENTALE

L'EDR observe en permanence l'activité sur le poste utilisateur, analysant les connexions réseau, les modifications de registre et les accès aux fichiers pour détecter toute activité anormale, même si la menace est totalement inconnue.

2. INTELLIGENCE ARTIFICIELLE

Des algorithmes d'IA avancés analysent les schémas comportementaux pour identifier les activités suspectes qui pourraient indiquer une menace Zero-Day.

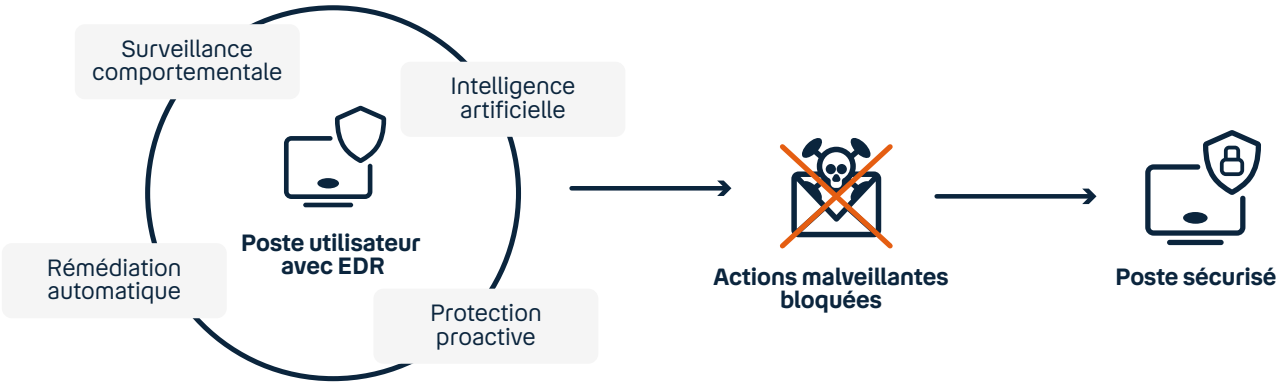
3. PROTECTION PERMANENTE ET PROACTIVE

L'EDR bloque les actions malveillantes avant qu'elles ne causent des dommages, même face à des menaces jamais rencontrées auparavant.

4. RÉMÉDIATION AUTOMATIQUE

En cas de détection d'une menace, l'EDR isole automatiquement un poste compromis, bloque les processus malveillants et même annule les modifications causées par une attaque Zero-Day.

Comment fonctionne l'EDR ?



Protégez votre entreprise avec une solution EDR

Les cybermenaces qui pèsent sur les équipements de vos collaborateurs évoluent en permanence et à une vitesse vertigineuse. C'est pour cette raison que nous avons rendu accessible au plus grand nombre, une solution de protection des PC et des serveurs par l'EDR.

L'EDR offre une protection complète des endpoints qui sécurise efficacement vos postes utilisateurs contre les menaces les plus sophistiquées. Ses points forts :

- **Une solution compatible avec tous les OS**
  L'EDR utilise un agent ultraléger qui n'affecte pas les performances de vos systèmes, tout en étant compatible avec l'ensemble des systèmes d'exploitation (Windows, macOS, Linux).
- **Protection contre les menaces Zero-Day**
  Grâce à son analyse comportementale avancée, l'EDR détecte et neutralise les menaces Zero-Day qui exploitent des vulnérabilités encore inconnues.
- **Protection contre l'exfiltration de données**
  Il empêche la fuite de données sensibles, protège contre les ransomwares et peut même annuler automatiquement les changements malveillants effectués sur vos systèmes.
- **Détection et contrôle en temps réel** des comportements anormaux, offrant une visibilité complète sur votre parc informatique et une protection performante contre les menaces émergentes.

L'avis de l'expert

« La protection des postes utilisateurs nécessite aujourd'hui une approche radicalement différente. Les antivirus traditionnels se contentent de comparer des signatures, c'est comme si vous cherchiez uniquement les criminels déjà fichés. Face aux attaques Zero-Day, cette approche est vouée à l'échec. L'EDR, lui, analyse les comportements suspects, peu importe si la menace est connue ou non. Lorsqu'une menace Zero-Day est détectée, cette information est immédiatement partagée avec l'ensemble de l'infrastructure de sécurité, créant ainsi une défense coordonnée et intelligente qui s'adapte en temps réel aux nouvelles menaces. »

Benjamin Laygnez
Responsable marketing data, cloud & cybersécurité,
Bouygues Telecom division Entreprises

À RETENIR

- Les antivirus traditionnels ne permettent plus de faire face aux menaces modernes qui exploitent les failles de sécurité avant même leur identification.
- Une solution EDR (Endpoint Detection and Response) surveille en temps réel le comportement des applications pour détecter les activités suspectes, même inconnues.
- L'intelligence artificielle intégrée à l'EDR analyse les schémas comportementaux pour identifier et bloquer préventivement les menaces Zero-Day avant qu'elles ne causent des dommages.
- La protection proactive offerte par l'EDR permet d'isoler automatiquement un poste compromis et d'annuler les modifications causées par une attaque.

05

Comment défendre votre réseau avec le SD-WAN sécurisé ?

Solution préconisée pour des TPE/PME de 50 à 250 salariés réparties sur plusieurs sites en France.

La sécurisation des réseaux d'entreprise est aujourd'hui un enjeu majeur. Les entreprises sont de plus en plus dépendantes de leur réseau pour échanger des données et communiquer avec leur écosystème de partenaires et de clients. Dans ce contexte, les solutions *Software-Defined Wide Area Network* (SD-WAN) vous permettent **d'optimiser et de sécuriser les connexions entre les différents sites** de votre organisation. Une étude publiée par IDC[1] met en lumière l'engouement des entreprises pour les solutions SD-WAN.
Elle révèle que le marché mondial du SD-WAN était évalué à 7,2 milliards de dollars en 2023 et devrait enregistrer une croissance moyenne annuelle de 27 % entre 2024 à 2032.

Source : (1) IDC - Worldwide SD-WAN Infrastructure Forecast, 2024–2028

Quels sont les risques ?

Votre entreprise est organisée autour d'un maillage de plusieurs agences ou filiales reliées par des connexions réputées sûres ? Imaginez qu'un de vos salariés dans une agence récemment inaugurée télécharge un fichier infecté. **Le malware peut alors se propager sur l'ensemble du réseau,** compromettant les données de votre entreprise et paralysant son activité. Les cybercriminels peuvent alors exploiter les failles de sécurité pour accéder aux informations sensibles de l'entreprise, voler vos données clients, paralyser vos systèmes d'information ou exiger des rançons.

Ce scénario, malheureusement fréquent, illustre les limites des solutions réseau traditionnelles. Une solution SD-WAN sécurisé apporte, entre autres avantages, un filtrage des échanges entre les sites pour éviter un tel scénario.

Le SD-WAN : comment ça marche ?

Le SD-WAN permet de créer un réseau intelligent, flexible et sécurisé qui s'adapte aux besoins de votre entreprise et vous offre une visibilité et un contrôle accrus sur le trafic réseau.
Voici comment cela se passe :

1. SÉCURISATION DES FLUX

Le SD-WAN permet de chiffrer les données qui transitent sur le réseau, protégeant ainsi la confidentialité et l'intégrité des échanges entre les différents sites de l'entreprise.

2. SEGMENTATION DU RÉSEAU

Le SD-WAN permet de diviser le réseau en zones distinctes et isolées, ce qui limite la propagation des incidents de sécurité et renforce la protection des données sensibles.

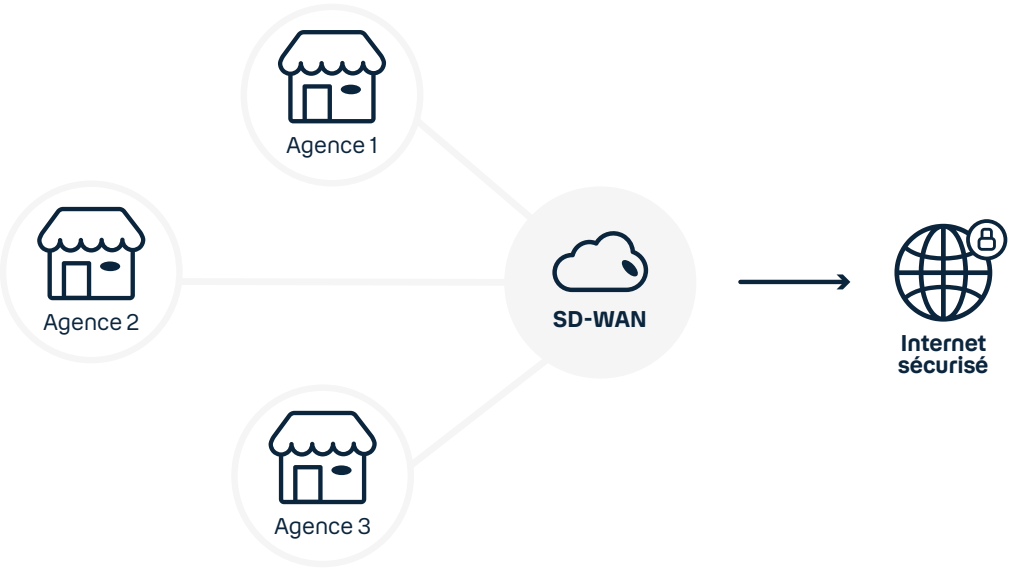
3. INSPECTION DU TRAFIC

Le SD-WAN analyse en profondeur le trafic réseau, en inspectant les paquets de données, pour détecter et bloquer les menaces potentielles, telles que les malwares, les intrusions et les attaques DDoS.

4. APPLICATION DES POLITIQUES DE SÉCURITÉ

Le SD-WAN permet de définir et d'appliquer des politiques de sécurité centralisées sur l'ensemble du réseau, simplifiant la gestion de la sécurité et assurant une protection homogène.

Comment fonctionne un SD-WAN sécurisé ?



Protéger votre entreprise avec le SD-WAN

Face aux enjeux de performance et de sécurité, ainsi qu'à la dépendance croissante des entreprises à la connectivité, vous devez mettre en place des solutions performantes, fiables et adaptées aux besoins spécifiques de votre entreprise. Le SD-WAN offre ainsi une solution de connectivité moderne, flexible et sécurisée qui permet à votre entreprise et ses différentes succursales de protéger efficacement votre réseau et d'optimiser vos opérations.

Ses points forts :

- **Une sécurité renforcée**
  Le SD-WAN intègre des fonctionnalités de sécurité, telles que le chiffrement des données, la segmentation, l'inspection du trafic et l'application de politiques de sécurité, pour protéger votre réseau contre les menaces internes et externes.
- **Des performances optimisées**
  Le SD-WAN permet d'optimiser l'utilisation de la bande passante, de réduire la latence, d'améliorer la qualité de service (QoS) et d'assurer la disponibilité des applications critiques.
- **Une gestion centralisée**
  Le SD-WAN permet de centraliser la gestion du réseau via une interface unique, facilitant ainsi la configuration, le déploiement et la supervision des connexions entre les différents sites de votre l'entreprise.

L'avis de l'expert

« La protection des échanges qui circulent entre les différents sites est une composante essentielle de la sécurité globale. Les solutions doivent se moduler en fonction de la complexité et de l'évolution des architectures réseau, une réponse unique à chaque besoin. Notre expertise permet de configurer et de gérer les réseaux avec une efficacité optimale et un accompagnement constant. Une approche partenariale qui fait la différence. »

Benjamin Laygnez
Responsable marketing data, cloud & cybersécurité,
Bouygues Telecom division Entreprises

À RETENIR

- Le SD-WAN sécurisé renforce la protection des réseaux d'entreprise en chiffrant les données et en segmentant le réseau pour limiter la propagation des menaces.
- Le SD-WAN effectue une inspection approfondie du trafic en temps réel pour détecter et bloquer les malwares, les intrusions et les attaques DDoS, tout en optimisant la bande passante.
- La gestion centralisée du SD-WAN simplifie l'administration du réseau tout en optimisant les performances et la qualité des connexions multisites.

06

Déploiement & mise en place

Comment passer à l'action et rester efficace à long terme ?

La mise en place d'une stratégie de cybersécurité efficace est un défi pour les TPE/PME. Sans compétences dédiées en interne, comment déployer et maintenir des solutions adaptées ? La réponse : **se faire accompagner par des experts spécialisés**, pas seulement dans la définition d'une stratégie mais dans son application au quotidien ! Un partenariat avec un fournisseur de services managés s'impose alors comme la solution idéale, car il vous permet de bénéficier d'une protection de niveau grand compte, adaptée à vos besoins et à vos moyens.

Tracez votre plan d'action : les étapes clés

La mise en œuvre d'une stratégie de cybersécurité efficace pour votre entreprise n'est pas une action ponctuelle, mais un processus itératif qui comprend plusieurs phases essentielles.

1 L'AUDIT INITIAL

L'expert en cybersécurité installe un équipement qui observe vos flux réseaux. Cette phase permet d'obtenir une vision précise de votre environnement numérique. Elle permet d'identifier les applications utilisées, les comportements à risque, et les vulnérabilités existantes.

2 LA PHASE DE PARAMÉTRAGE

Les experts configurent des règles de sécurité adaptées à vos besoins. Ils élaborent un cadre de protection qui prend en compte vos flux légitimes tout en bloquant les menaces potentielles.

3 UN DÉPLOIEMENT PROGRESSIF

La mise en place des solutions de sécurité s'effectue par étapes pour minimiser l'impact sur votre activité. Les experts s'assurent que chaque composant de sécurité s'intègre harmonieusement dans votre écosystème numérique.

4 LA VALIDATION ET L'AJUSTEMENT CONTINU

Une phase de validation permet de s'assurer que tout fonctionne correctement. Par la suite, les experts affinent en continu les paramètres en fonction de vos usages et des menaces.

Comment construire une cybersécurité efficace et durable ?

La cybersécurité représente un enjeu majeur pour les TPE/PME, mais sa mise en œuvre peut sembler complexe et coûteuse. Vous devez comprendre les principes fondamentaux qui garantissent l'efficacité et la pérennité de votre protection.

- **Une supervision continue**
  Contrairement aux idées reçues, la cybersécurité ne se résume pas à l'installation d'équipements. Elle repose sur une supervision constante qui **permet d'adapter les protections à l'évolution des menaces et de vos usages.** Cette surveillance permanente assure que vos solutions de sécurité restent efficaces dans le temps.
- **L'équilibre entre protection et productivité**
  Une sécurité trop restrictive peut entraver votre activité et inciter vos collaborateurs à contourner les mesures de protection, créant ainsi de nouvelles vulnérabilités. L'enjeu consiste à trouver le juste équilibre entre un niveau de protection optimal et la fluidité nécessaire à votre productivité quotidienne.
- **Des solutions adaptées à vos besoins spécifiques**
  Chaque entreprise possède des caractéristiques propres qui nécessitent une approche personnalisée. **Les protections doivent être configurées en fonction de vos usages réels, de vos applications critiques et de vos contraintes métier.** Cette personnalisation garantit une sécurité pertinente et non intrusive.
- **Une réactivité immédiate face aux incidents**
  Malgré les mesures préventives, des incidents peuvent survenir. La capacité à les détecter rapidement et à y répondre efficacement est déterminante. Les solutions modernes associent l'automatisation (pour une réaction instantanée) à l'expertise humaine (pour l'analyse approfondie et la remédiation).

L'avis de l'expert

« Le Security Operation Center (SOC) est une infrastructure dédiée où des experts surveillent en permanence votre environnement numérique. En effet, la cybersécurité ne se limite pas au déploiement d'un équipement ou d'une solution. L'enjeu réside dans la supervision constante des points de protection. »

« Notre philosophie consiste à prendre des solutions habituellement réservées aux plus grandes entreprises et de les rendre accessibles aux TPE et PME en apportant la couche de management dont elles ont besoin. Notre SOC fonctionne 24h/24 grâce à des playbooks automatisés qui sont plus restrictifs la nuit que le jour. Nous avons investi dans des solutions d'automatisation qui traitent des dizaines de milliers d'événements, bloquant 98 % à 99 % des attaques potentielles. Le reste est analysé par nos experts qui réalisent un travail d'investigation approfondi ».

Emmanuel Blanc
Expert en cybersécurité,
Alleo de Bouygues Telecom

À RETENIR

- La cybersécurité est un processus continu qui nécessite une expertise spécifique et une surveillance constante.
- Une stratégie efficace commence par un audit approfondi de votre environnement numérique, suivi d'un paramétrage sur mesure qui s'adapte à vos besoins.
- L'équilibre optimal entre niveau de protection et fluidité opérationnelle est essentiel pour garantir l'adhésion de vos équipes aux mesures de sécurité.
- Le Security Operation Center (SOC) joue un rôle central dans la détection précoce des menaces et la réponse rapide aux incidents, combinant automatisation intelligente et expertise humaine.

Contactez-nous

Au **3100**

Sur le site
bouyguestelecom-pro.fr

Retrouvez notre actualité

le Mag Business

bouygues TELECOM **Pro**