VECTRA®
SECURITY THAT THINKS

ÉTUDE

# La sécurité de Microsoft 365 dans le secteur public passée à la loupe :

## Réduire l'avance des attaquants sur les défenseurs

VECTRA
SECURITY THAT THINKS

## Sommaire



# Avant-propos

Microsoft 365 est devenu indissociable de la productivité des entreprises dans le secteur des administrations publiques, des soins de santé et de l'enseignement. Lorsque la pandémie de COVID-19 s'est déclarée au début de l'année 2020, les organisations fournissant des services publics critiques aux quatre coins de la planète ont pu passer rapidement au télétravail et à la prestation de services à distance grâce aux méthodes de travail agiles et flexibles prises en charge par Microsoft 365. Qu'il s'agisse de fonctionnaires en télétravail, de cliniciens en vidéoconférence avec leurs patients ou d'enseignants dispensant des cours en ligne, il est clair que l'utilisation de Microsoft 365 est bien plus étendue qu'elle ne l'a jamais été.

Cela étant, la généralisation du cloud au sein des organisations fournissant des services publics critiques a également élargi la surface d'attaque susceptible d'être exploitée par les cyberpirates. Les administrations publiques et les établissements de soins de santé et d'enseignement sont aujourd'hui tenus de défendre leur environnement Microsoft 365 face aux cybercriminels qui cherchent à exploiter les précieuses données qu'il héberge pour orchestrer des cyberattaques dommageables.

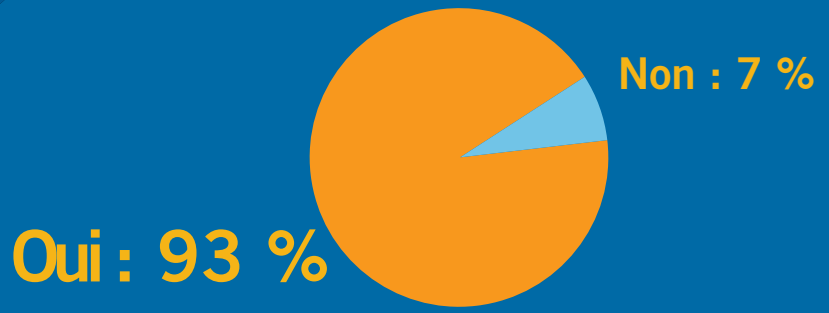
Cet eBook pose un regard neuf sur le paysage de Microsoft 365. Il est le résultat d'une enquête mondiale menée auprès de quelque 1 100 responsables de la sécurité informatique et s'intéresse plus particulièrement aux réponses données par les 302 professionnels employés par des institutions et des organisations gouvernementales, d'enseignement et de soins de santé dans le monde. Nous avons non seulement recueilli leurs avis sur les principales menaces planant sur les environnements Microsoft 365, mais aussi sur leur capacité à s'en protéger.

Nous évoquerons aussi les mesures pratiques à prendre pour améliorer la sécurité de l'infrastructure Microsoft 365 et Azure Active Directory (AD), notamment les solutions à mettre en place pour identifier et bloquer les tentatives de prise de contrôle de comptes d'utilisateur.

VECTRA
SECURITY THAT THINKS

# Explosion de l'utilisation du cloud dans le secteur public pendant la pandémie

Autrefois considérées comme un avantage stratégique, les fonctionnalités cloud sont devenues une nécessité pendant la pandémie et les services publics se sont empressé d'élargir le cadre d'utilisation de Microsoft 365. Certains ont même avancé leur calendrier d'adoption du cloud de plusieurs années.




**93 % des responsables de la sécurité informatique interrogés ont utilisé davantage Microsoft 365 en raison de la pandémie.**

VECTRA
SECURITY THAT THINKS

Le télétravail devenant la norme, il n'est guère étonnant que l'utilisation de Microsoft 365 ait gagné du terrain au sein de la plupart des organisations, notamment dans la sphère professionnelle. En mars 2020, Microsoft recensait 258 millions d'utilisateurs actifs de Microsoft Teams, soit une hausse de plus de 70 millions par rapport à l'année précédente.

« La solution de Vectra a réduit le délai nécessaire à la neutralisation des attaques. Auparavant, il était difficile de détecter un incident, car nous manquions d'une visibilité globale. Aujourd'hui, nous en sommes très rapidement informés grâce à une vue d'ensemble sur tous les événements. »

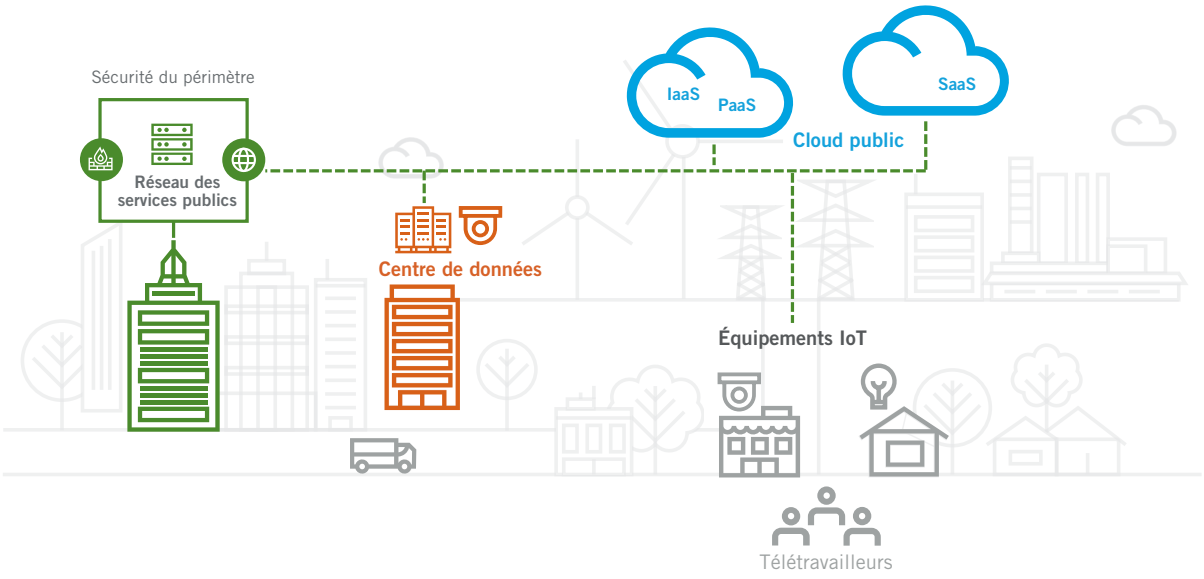
**Gestionnaire de projet d'une université**

Cette transition contrainte et forcée a bouleversé irrémédiablement le paysage informatique. Lorsque nous avons interrogé des responsables de la sécurité informatique des secteurs de l'administration publique, des soins de santé et de l'enseignement sur les conséquences de la pandémie sur leurs activités, plus de 80 % d'entre eux ont déclaré avoir accéléré leurs stratégies de migration vers le cloud et de transition numérique en conséquence. Plus étonnant encore, 20 % ont admis avoir pris deux ans d'avance sur leur planning et, en ce qui concerne les administrations publiques, ce chiffre s'élève à 25 %.

**L'évolution du paysage informatique et l'accélération forcée de la migration vers le cloud ont aussi exacerbé la vulnérabilité de ces organisations aux cybermenaces.**

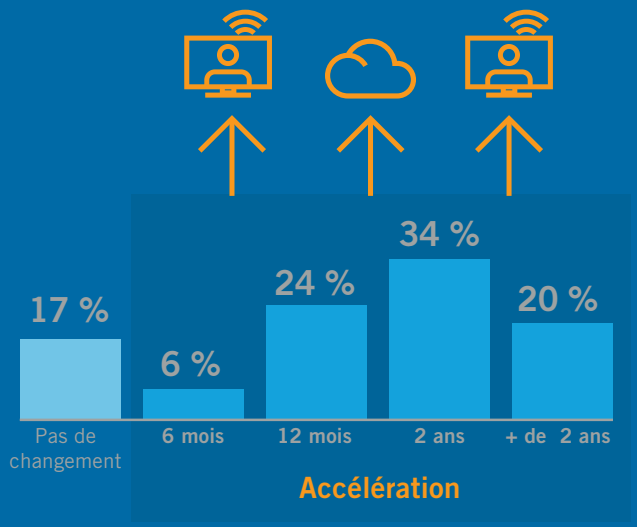
Et si ces douze derniers mois s'apparentent plus à un baptême du feu pour nombre d'entre eux, cette accélération semble avoir conféré plusieurs avantages tangibles. Un peu plus de 40 % des répondants éprouvent plus de satisfaction dans leur travail et une proportion similaire y voit un gain de productivité.

Il est clair, cependant, que les épreuves de la pandémie ont également conduit à une augmentation du stress. Un peu moins de la moitié des responsables de la sécurité informatique des services publics interrogés ont constaté une aggravation du stress pendant le confinement lié à la pandémie. Outre les répercussions sur le personnel, l'évolution du paysage informatique et l'accélération forcée de la migration vers le cloud ont aussi exacerbé la vulnérabilité de ces organisations aux cybermenaces.




**83 %**

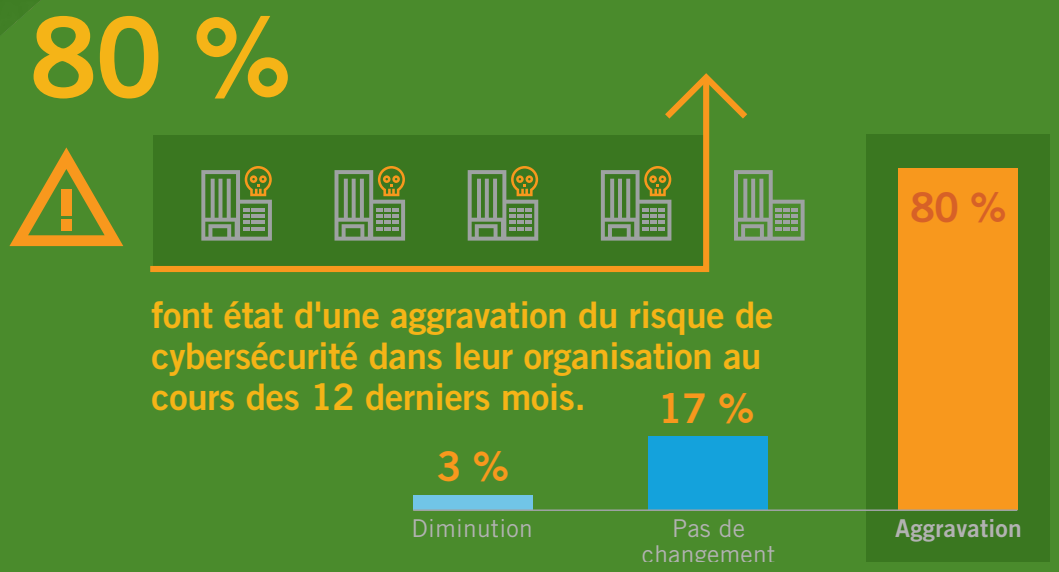
ont vu la migration vers le cloud et la transition numérique de leur entreprise **s'accélérer pendant la pandémie**. 20 % ont constaté que leur entreprise avait gagné plus de 2 ans.



VECTRA
SECURITY THAT THINKS

# Évolution rapide du paysage des menaces

La hausse du télétravail et l'adoption de Microsoft 365 et Azure AD ont inévitablement augmenté la surface d'attaque. De nombreux professionnels de la sécurité ont rencontré bien des difficultés pour comprendre et protéger cet environnement en pleine mutation. Dans de nombreux cas, les outils et stratégies mis en œuvre sur site étaient inadaptés pour surveiller et protéger efficacement les utilisateurs. Naturellement, les cybercriminels n'ont pas tardé à exploiter ce filon et à multiplier les attaques. Dès avril 2020, Google indiquait bloquer quotidiennement plus de 18 millions d'e-mails de phishing et contenant des malwares sur le thème de la COVID-19.



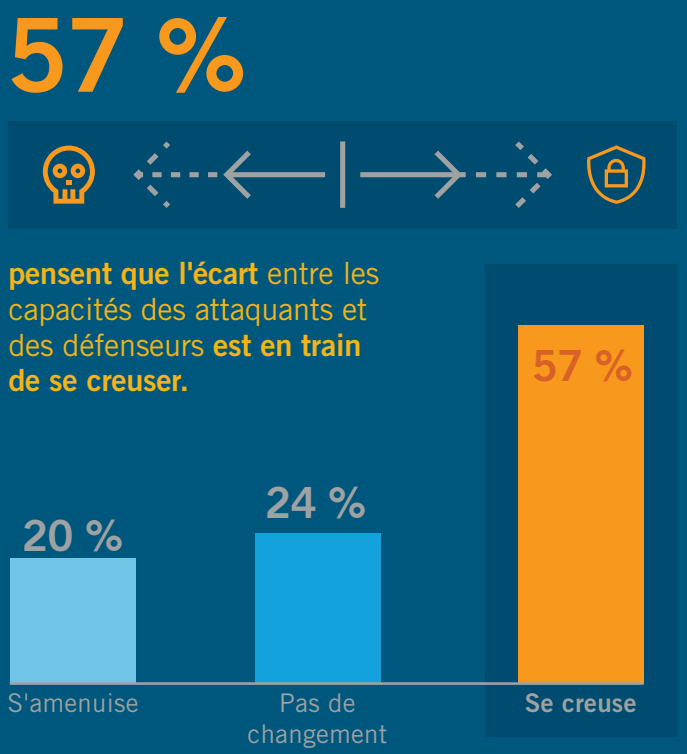
Si la prévalence des attaques de phishing sur le thème de la COVID-19 semble aujourd'hui en recul, les failles de sécurité liées à l'essor des déploiements dans le cloud n'ont quant à elles pas disparu. La majorité des responsables de la sécurité au sein des secteurs de l'administration publique, des soins de santé et de l'enseignement estiment que les risques ont augmenté au cours des douze derniers mois.

**Trois responsables de la sécurité sur cinq pensent que l'écart entre les capacités des attaquants et des défenseurs est en train de se creuser.**

De leur côté, les attaquants redoublent d'ingéniosité et mettent leur expérience à profit pour s'aventurer sur ce nouveau terrain et en exploiter les failles. C'est ainsi que les attaques de malware traditionnelles sont aujourd'hui délaissées au profit d'attaques ciblant les comptes, les identifiants, les autorisations et les rôles, que les outils de sécurité traditionnels sont incapables de détecter.

À l'heure où les cybercriminels redoublent d'ingéniosité et intensifient leurs attaques, les responsables de la sécurité au sein des services publics sont nombreux à se montrer pessimistes. Près de trois sur cinq pensent que les pirates ont désormais plusieurs coups d'avance sur les équipes de sécurité.

La majorité des responsables de la sécurité au sein des secteurs de l'administration publique, des soins de santé et de l'enseignement estiment que les risques ont augmenté au cours des douze derniers mois.



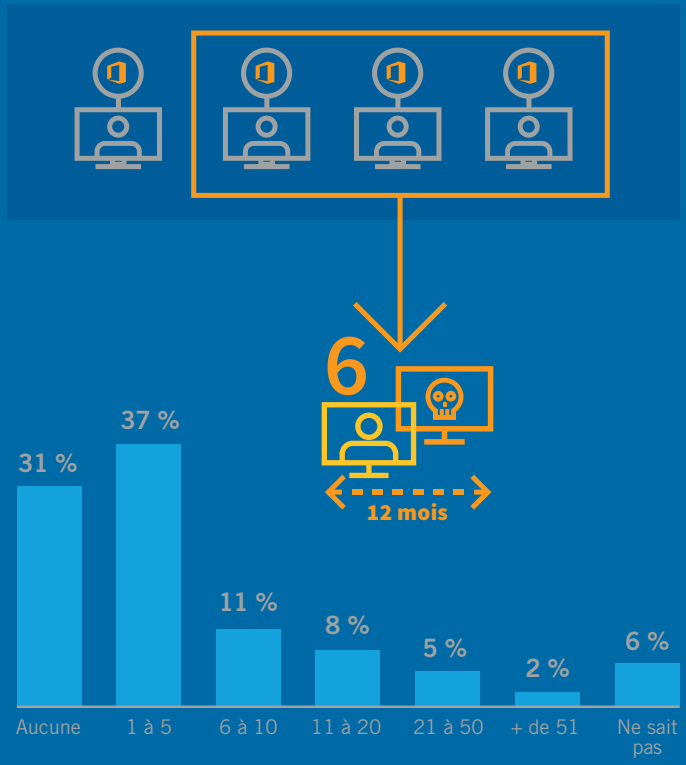
Pourtant, grâce à la mise en place d'outils tels que les solutions de détection et de résolution des incidents (NDR) et les analyses optimisées par l'intelligence artificielle (IA), c'est en réalité l'inverse. Une fois que les attaquants parviennent à infiltrer un environnement, ils comptent habituellement sur leur aptitude à se faire oublier dans le maelström des activités normales de l'entreprise. Les pirates prudents peuvent très bien exploiter les applications métiers légitimes et leurs outils (tactique « live off the land »), notamment ceux intégrés à la suite Microsoft 365, tels que Power Automate et eDiscovery, pour se déplacer latéralement, se dissimuler au sein du réseau et exfiltrer des données. Heureusement, les solutions NDR optimisées par l'IA qui s'intègrent aux applications et services cloud sont capables d'exposer cette couverture et d'identifier le moindre indice suggérant une intrusion active.

**Heureusement, les solutions NDR optimisées par l'IA qui s'intègrent aux applications et services cloud sont capables d'exposer cette couverture et d'identifier le moindre indice suggérant une intrusion active.**

Bien sûr, la simple existence de ces outils ne suffit pas à combler l'écart entre attaquants et défenseurs. Seules les organisations qui auront investi dans de telles solutions seront capables de détecter les signes ténus d'une activité malveillante. Jusque-là, il faut malheureusement s'attendre à voir les cyberpirates continuer à exploiter les infrastructures cloud non protégées, par exemple, en prenant le contrôle de comptes d'utilisateurs légitimes afin d'accéder aux données sensibles qu'ils contiennent. Parmi nos répondants, plus de trois organisations sur cinq dans le secteur de l'administration publique, des soins de santé et de l'enseignement ont été victimes d'au moins une prise de contrôle de comptes ciblant leurs utilisateurs Microsoft 365 l'année dernière.

> Il faut malheureusement s'attendre à voir les cyberpirates continuer à exploiter les infrastructures cloud non protégées.

**63 %** des organisations fournissant des services publics ont subi en moyenne une prise de contrôle de compte d'utilisateur légitime **au cours de l'année écoulée.**



VECTRA
SECURITY THAT THINKS

# Sécuriser Microsoft 365 est une priorité absolue

Compte tenu de la valeur de leurs données, les administrations publiques et les établissements de soins de santé et d'enseignement constituent des cibles de choix pour les cybercriminels. Par conséquent, les équipes responsables de la sécurité informatique doivent être préparées à un large éventail de cybermenaces. Les répondants de ces secteurs se disent très préoccupés par les menaces ciblant les équipements connectés et IoT, les usurpations d'identité visant des utilisateurs autorisés et la menace croissante posée par le ransomware.

**La principale préoccupation de la moitié des répondants est le risque de compromission des données stockées dans Microsoft 365.**

Toutefois, leur toute première crainte concerne les attaques contre les données hébergées dans Microsoft 365, suivie de près par le risque que les cyberpirates puissent effacer leurs traces en s'aidant d'outils Microsoft légitimes tels que Power Automate et eDiscovery. Microsoft 365 est souvent au cœur des activités des administrations publiques et des établissements de soins de santé et d'enseignement. Il facilite le stockage et le partage d'une part considérable des données et fait office de fournisseur d'identité pour l'accès à une multitude d'autres applications SaaS. L'environnement Microsoft 365 constitue par conséquent une cible de choix pour les cybercriminels. Avec plus de 250 millions d'utilisateurs mensuels, ce ne sont pas les cibles qui manquent. Notre récent rapport Spotlight consacré à Microsoft 365 a passé au crible plus de quatre millions de comptes. 96 % d'entre eux présentaient des signes de déplacement latéral.

**Microsoft 365 est souvent au cœur des activités des administrations publiques et des établissements de soins de santé et d'enseignement. Il facilite le stockage et le partage d'une part considérable des données et fait office de fournisseur d'identité pour l'accès à une multitude d'autres applications SaaS.**

De même, de nombreux répondants s'inquiétaient également du risque d'utilisation abusive des identifiants, à l'origine de la prise de contrôle de comptes par des utilisateurs non autorisés.

Au vu du large éventail de fonctionnalités et de données auxquelles un utilisateur de Microsoft 365 a accès, la compromission d'un compte peut causer des dégâts majeurs, sans la moindre difficulté. Les attaquants peuvent notamment exploiter les comptes à privilèges pour accélérer les déplacements latéraux et apporter des changements systémiques qui leur permettront de s'installer à demeure sans être repéré. La protection de ces comptes ainsi que la détection et l'arrêt de leur détournement doivent être au cœur de toute stratégie de sécurité cloud.

Au vu du large éventail de fonctionnalités et de données auxquelles un utilisateur de Microsoft 365 a accès, la compromission d'un compte peut causer des dégâts majeurs, sans la moindre difficulté.

**S'agissant des menaces les plus inquiétantes pour leur sécurité en 2021, l'enquête dresse les constats suivants :**

**43 %**

Les attaques par l'entremise d'équipements IoT/connectés vont augmenter.

**43 %**

Les attaques basées sur l'identité à l'encontre des utilisateurs autorisés vont augmenter.

**40 %**

Les attaques par ransomware vont s'intensifier.

**40 %**

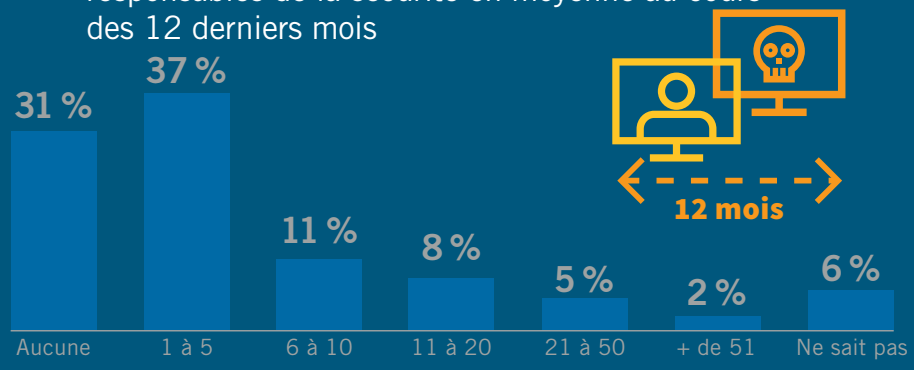
Les attaques contre le cloud vont sensiblement s'accélérer.

VECTRA
SECURITY THAT THINKS

# Prises de contrôle de comptes d'utilisateur : une menace croissante

L'agilité et l'interconnectivité offertes par certaines applications, dont celles de la suite Microsoft 365, sont une aubaine pour le travailleur lambda, mais aussi pour les cyberpirates. Les environnements cloud sont beaucoup plus accessibles que les applications traditionnelles installées dans le périmètre réseau. Les attaquants ciblant Microsoft 365 savent combien il est simple d'y effectuer un repérage et de trouver les clients et leurs conventions de nommage probables.

**6 prises de contrôle de comptes d'utilisateur légitimes** subies par les responsables de la sécurité en moyenne au cours des 12 derniers mois



À partir de là, les attaquants peuvent déployer des attaques hautement automatisées à l'encontre de milliers de comptes en effectuant des tentatives de connexion. Il suffit d'un seul utilisateur aux pratiques de gestion des mots de passe déficientes pour que l'attaquant infiltre l'organisation, l'authentification multifacteur n'étant généralement pas difficile à contourner. Cette approche présente un grand attrait aux yeux des cybercriminels, car elle peut leur rapporter gros sans que ceux-ci ne doivent lancer une attaque ciblée mobilisant beaucoup de temps et de moyens.

**Les comptes Microsoft 365 compromis peuvent servir à infliger de lourds dégâts dans un laps de temps très court.**

Les environnements cloud permettent en outre aux pirates de raccourcir considérablement leur cycle d'attaque, la durée du repérage étant beaucoup plus courte.

Des responsables de la sécurité informatique des secteurs de l'administration publique, des soins de santé et de l'enseignement avouent avoir subi en moyenne six prises de contrôle de comptes d'utilisateur autorisés au cours des douze derniers mois.

Force est de constater qu'en dépit du nombre d'incidents et du risque élevé que présente ce type de compromission, la majorité des responsables de la sécurité de ces secteurs sont confiants en leur capacité à faire face à des tentatives de prise de contrôle de comptes d'utilisateur.

Près de 7 répondants sur 10 estiment que leur équipe est en mesure d'identifier et de bloquer une prise de contrôle de comptes en quelques jours, voire en quelques heures. Ils sont 3 sur 10 à s'estimer capables d'endiguer immédiatement une telle attaque.

Les comptes Microsoft 365 compromis peuvent servir à infliger de lourds dégâts dans un laps de temps très court. Un délai de quelques jours pour identifier une prise de contrôle peut donc rendre une organisation extrêmement vulnérable. Il est impératif que les équipes de sécurité puissent identifier en temps réel les comportements suspects sur site et dans le cloud afin de repérer l'attaquant avant qu'il ne soit trop tard.

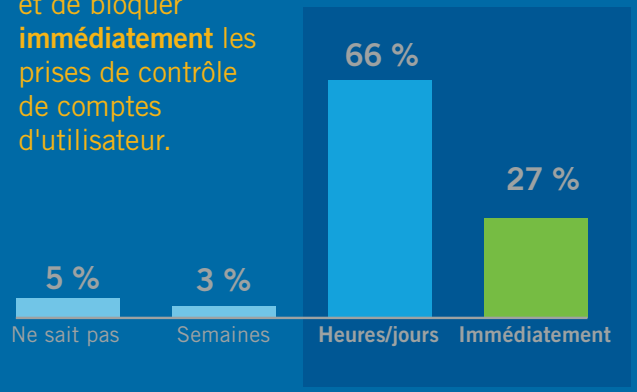
Les équipes qui pensent pouvoir repérer sans délai une compromission doivent être sûres de leur coup ou se préparer à la douche froide en cas de compromission.

Près de
**27 %**

indiquent que leur équipe de sécurité est à même d'identifier et de bloquer **immédiatement** les prises de contrôle de comptes d'utilisateur.

**66 %**

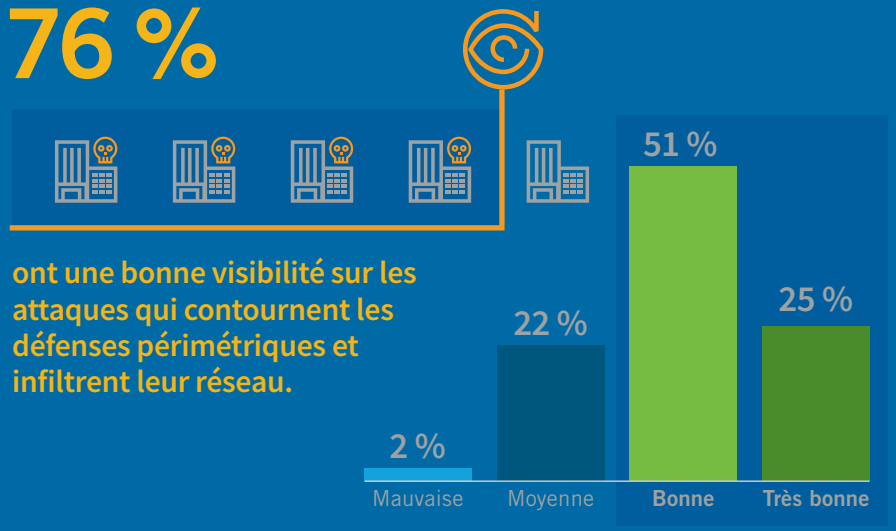
déclarent pouvoir bloquer les prises de contrôle de comptes d'utilisateur en **quelques heures ou jours**.



VECTRA
SECURITY THAT THINKS

# Le manque de visibilité induit un excès de confiance

Les responsables de la sécurité informatique sont confiants en leur capacité à prévenir les prises de contrôle de comptes d'utilisateur, une confiance en totale contradiction avec le nombre croissant d'attaques et les longues durées d'implantation signalées par le secteur dans son ensemble. La durée moyenne d'une attaque est estimée à 43 jours – et pourtant seuls 3 % des répondants déclarent avoir besoin de plusieurs semaines pour repérer et neutraliser un compte compromis.



De manière générale, les répondants sont également assez confiants en leur capacité à identifier et à endiguer d'autres formes d'attaques. La plupart estiment avoir une bonne visibilité sur les attaques qui contournent leur périmètre et être en mesure de détecter et de neutraliser tout déplacement latéral. De nouveau, on note une discordance avec le fait que 96 % des environnements Microsoft 365 analysés par Vectra présentent des signes de déplacement latéral.

**La durée moyenne d'une attaque est estimée à 43 jours – et pourtant seuls 3 % des répondants déclarent avoir besoin de plusieurs semaines pour repérer et neutraliser un compte compromis.**

Cet optimisme est en décalage avec la réalité observée lors de l'examen des organisations. Si certains répondants sont en mesure d'étayer leurs affirmations, la plupart pèchent par excès de confiance.

Le pessimisme est beaucoup plus répandu chez les cadres que chez les administrateurs et les dirigeants. Cette confiance illusoire trouve sans doute son origine dans les indicateurs et les objectifs biaisés circulant dans les hautes sphères, bien loin de la réalité du terrain.

Cette confiance illusoire trouve sans doute son origine dans les indicateurs et les objectifs biaisés circulant dans les hautes sphères, bien loin de la réalité du terrain.

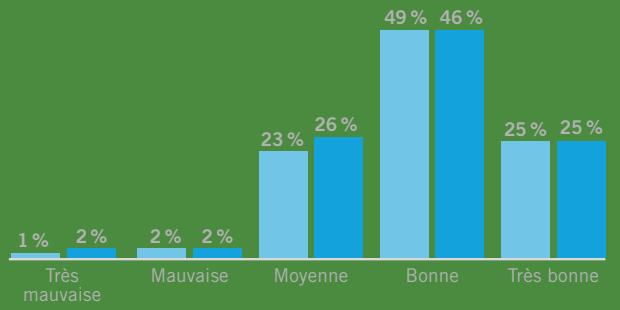
Par exemple, un centre d'opérations de sécurité (SOC) peut être confronté à des centaines de menaces au quotidien. Si l'on considère le nombre d'incidents déjoués comme principal indicateur de succès, tout va pour le mieux dans le meilleur des mondes. Cependant, cette approche élude les vraies questions à se poser : combien de temps a-t-il fallu avant de détecter les menaces et de les neutraliser ? Combien d'entre elles constituaient des tentatives répétées ? La capacité à neutraliser les nombreuses attaques en masse de bas niveau est à distinguer de la détection des menaces sophistiquées, en particulier celles qui visent les utilisateurs.

**74 %**

qualifient leur organisation de bon élève en matière de **détection des attaques**.

**71 %**

qualifient leur organisation de bon élève en matière de **prévention des attaques**.



S'agissant d'attaques telles que les prises de contrôle de comptes d'utilisateur, les indicateurs de compromission ont évolué vers des facteurs comportementaux plus difficiles à cerner et potentiellement disséminés de façon subtile sur plusieurs environnements.

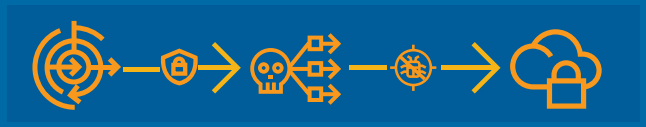
**Le fait est que les cybercriminels ajustent constamment leurs tactiques pour balayer tous les obstacles placés sur leur chemin.**

Enfin, l'impression que le respect des bonnes pratiques de sécurité protège des attaques peut aussi expliquer cet excès de confiance. Néanmoins, le fait est que les cybercriminels ajustent constamment leurs tactiques pour balayer tous les obstacles placés sur leur chemin.

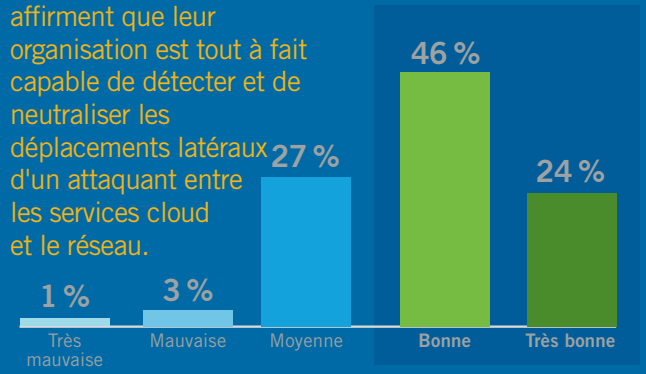
L'authentification multifacteur est quasiment devenue une constante et beaucoup la considèrent comme un rempart infranchissable en cas de tentative de piratage de compte. Cependant, Microsoft a récemment mis en garde contre les failles de l'authentification multifacteur appliquée aux SMS et aux appels téléphoniques. Aux États-Unis, la Cybersecurity and Infrastructure Security Agency (CISA) a signalé une nouvelle technique de détournement de cookies (« pass the cookie ») permettant de contourner l'authentification pour accéder aux services cloud. Les processus de sécurité ne font que ralentir les attaquants, sans pour autant les arrêter.

Microsoft a récemment mis en garde contre les failles de l'authentification multifacteur appliquée aux SMS et aux appels téléphoniques.

# 70 %



affirment que leur organisation est tout à fait capable de détecter et de neutraliser les déplacements latéraux d'un attaquant entre les services cloud et le réseau.




# 96 %

des 4 millions de comptes échantillonnés par Vectra présentaient des signes de déplacement latéral*.

* Rapport Spotlight de Vectra

VECTRA
SECURITY THAT THINKS

# Une confiance adaptée à la réalité

Pour se faire une idée précise des capacités de sécurité, il est indispensable de disposer des bons indicateurs. Les trois plus importants sont les suivants :

1. Délai moyen de détection d'une menace
2. Délai moyen de réponse
3. Fréquence de répétition des mêmes problèmes

L'analyse de ces trois indicateurs permettra de recueillir des informations contextuelles précieuses sur l'efficacité des dispositifs de sécurité de l'organisation. Les attaques à longue durée d'implantation constituent la principale menace, en particulier si elles impliquent un compte Microsoft 365 compromis avec accès à une série de données et d'applications et que quelques secondes suffisent pour causer de graves dégâts. Il est également essentiel de repérer à quel endroit le même problème survient continuellement. C'est le signe qu'il est temps d'envisager un changement fondamental de stratégie ou d'infrastructure.

**Toute mesure doit reposer sur un flux suffisant de données reproductibles.**

Toute mesure doit reposer sur un flux suffisant de données reproductibles. La réalisation de tests d'intrusion et d'exercices de simulation d'attaques peut contribuer à obtenir davantage de données fiables sur les menaces. C'est un moyen d'identifier rapidement les failles de la stratégie de sécurité et l'efficacité réelle des défenses en place.

Outre l'aspect « mesure », ce type de test est une compétence essentielle de l'équipe du centre SOC : les serruriers ne doivent pas seulement réparer les serrures, ils doivent aussi pouvoir les forcer.

Les attaques à longue durée d'implantation constituent la principale menace pour les entreprises.

« Nous sommes désormais plus confiants en notre capacité à détecter et à endiguer l'usage abusif d'identifiants, devenu monnaie courante dans Microsoft 365. »

**Kevin Orritt**
*Responsable de la sécurité des TIC*
*Greater Manchester Mental Health*

VECTRA
SECURITY THAT THINKS

# Améliorer les niveaux de sécurité en 2021

La plupart des responsables de la sécurité dans les administrations publiques et les établissements de soins de santé et d'enseignement ont adopté une approche assez visionnaire pour améliorer les niveaux de sécurité en 2021. C'est encourageant. Près de 3 sur 5 prévoient d'investir davantage dans la technologie et les personnes, mais ils tendraient à privilégier des solutions capables de protéger efficacement les environnements Microsoft 365 contre des menaces telles que la prise de contrôle de comptes d'utilisateur.

Le déploiement de solutions d'IA et le renforcement de l'automatisation sont deux des grandes priorités en matière d'investissements en 2021. Une telle approche est essentielle pour analyser efficacement de gros volumes de données sur les menaces et identifier les signes subtils révélateurs d'une compromission. En outre, le recours à l'IA pour alléger la charge de travail peut s'expliquer par la difficulté à recruter du personnel et à le garder.

## Il est aussi intéressant de noter que près de 40 % des répondants citent la technologie NDR comme étant l'un des outils prioritaires pour leurs équipes SOC.

**Le déploiement de plus de solutions d'IA et d'automatisation est l'une des grandes priorités en matière d'investissements en 2021.**

La clé de la sécurité dans un environnement cloud complexe réside dans la capacité à ne pas se laisser distraire et à identifier les signes d'activité suspecte dans l'ensemble de l'environnement, en abordant les réseaux cloud et sur site comme un tout. Les solutions de détection et de résolution des incidents optimisées par l'IA font partie de l'équation.

Enfin, l'utilisation accrue de la cyberveille et l'augmentation des investissements dans la traque des menaces et d'autres mesures proactives font aussi partie des priorités évoquées et permettront aux équipes de sécurité des services publics de mieux cerner leur niveau de sécurité et d'identifier les vulnérabilités et les chemins d'attaque à l'avance.

« Avant de déployer Vectra, nous disposions d'une visibilité limitée sur les comportements malveillants au sein du trafic réseau ou de Microsoft 365. Nous sommes impressionnés par ce que nous pouvons voir maintenant. »

**Kevin Orritt**
*Responsable de la sécurité des TIC*
*Greater Manchester Mental Health*

**Autres constats dressés par l'enquête :**

**59 %**
prévoient d'investir davantage dans les technologies et les ressources humaines pour améliorer le niveau de sécurité en 2021.

**49 %**
ont l'intention de recourir davantage à l'automatisation et à l'intelligence artificielle.

**45 %**
souhaitent mieux exploiter la cyberveille.

**41 %**
vont évoluer vers une traque proactive des menaces.

# Dix mesures pour se protéger des cyberattaques basées sur l'identité dans Microsoft 365

Microsoft 365 continue de jouer un rôle essentiel dans la continuité des activités. Les organisations fournissant des services publics doivent dès lors veiller à disposer des capacités nécessaires pour sécuriser leurs environnements cloud. Le problème est particulièrement pressant pour les administrations publiques et les établissements de soins de santé et d'enseignement qui ont dû revoir rapidement leur fonctionnement au cours de l'année écoulée et qui pourraient avoir du mal à adapter les défenses du périmètre aux frontières plus floues du cloud. La priorité absolue doit être de se prémunir contre la prise de contrôle de comptes d'utilisateur.

Voici les dix principales mesures à prendre pour protéger les environnements Microsoft 365 des compromissions de comptes :


**Ayez une parfaite connaissance des comptes à privilèges.** Vous devez avoir une parfaite connaissance des comptes autorisés à accéder aux données sensibles ou à utiliser les puissants outils de Microsoft 365, dont eDiscovery. Ces comptes constituent une cible de choix pour les cyberpirates. En limitant strictement l'accès des systèmes et des outils aux utilisateurs qui en ont l'usage dans l'exercice de leurs fonctions, vous limiterez les dégâts qu'un compte compromis peut infliger.


**Mesurez les bons indicateurs.** Tout indicateur utilisé pour évaluer l'efficacité de la sécurité doit passer le cap du passage à l'acte. Il ne doit pas seulement informer, il doit inciter à agir. La mesure du délai d'identification, du délai d'intervention, des incidents répétés et des taux de réinfection donnera une bonne indication de l'efficacité avec laquelle votre équipe identifie et élimine les menaces.


**Implémentez l'authentification multifacteur.** L'authentification multifacteur n'est peut-être pas la panacée en matière de sécurisation des comptes, mais elle reste un outil très important pour ralentir les attaquants. Si ce n'est pas encore fait, assurez-vous que tous les comptes utilisent l'authentification multifacteur.


**Simplifiez la configuration.** Les environnements cloud hybrides de transition cumulent les inconvénients en matière de sécurité : ils créent des redondances et des angles morts que les pirates ont tôt fait d'exploiter. Les longues transitions mettent à rude épreuve vos ressources informatiques et de sécurité et augmentent les risques. Faites dès lors en sorte d'accélérer le processus de simplification et de rationalisation de votre environnement.


**Effectuez des tests réguliers.** En identifiant les vulnérabilités et les chemins d'attaque, des exercices tels que les tests d'intrusion et les simulations d'attaques vous indiqueront si vous pouvez faire confiance à votre infrastructure de sécurité. Répétez ces tests régulièrement pour vous assurer que les corrections apportées améliorent votre niveau de sécurité.


**Formez toutes vos équipes – y compris celles chargées de la sécurité.** Dans le cadre de la poursuite de la transformation de vos activités, vous devez vous assurer que vos équipes savent utiliser les nouveaux outils en toute sécurité, de même que les sensibiliser aux menaces, telles que l'usurpation de l'identité de membres de l'équipe informatique dans des e-mails de phishing. Cette sensibilisation accrue permettra de battre en brèche les tentatives de compromission initiales. Assurez-vous également que votre équipe de sécurité maîtrise parfaitement votre nouvel environnement et est en mesure de passer des stratégies périmétriques traditionnelles aux frontières plus ouvertes du cloud.


**Ayez une bonne compréhension de l'utilisation des outils.** Placés entre les mains de personnes malintentionnées, les outils de Microsoft 365, tels qu'eDiscovery et Power Automate, peuvent faire des dégâts. Vous devez cerner le contexte d'utilisation de ces outils et avoir une idée précise de leur comportement normal. Il est essentiel d'identifier immédiatement les activités suspectes ou malveillantes et de les neutraliser avant qu'elles ne fassent des dégâts.


**Assurez-vous de disposer d'une vue unifiée de vos environnements.** Les cybercriminels n'hésitent pas à se déplacer entre vos réseaux traditionnels et vos environnements cloud pour atteindre leurs objectifs. Cependant, avec des outils de sécurité distincts qui surveillent des environnements différents, il n'est pas facile de s'en rendre compte. Vous devez être en mesure d'identifier les comportements malveillants sur l'ensemble de votre réseau informatique, de votre environnement cloud SaaS, de votre centre de données et de tout autre système susceptible d'être exploité par les attaquants. Les solutions NDR sont essentielles à cette fin.


**Utilisez l'IA pour accélérer et automatiser vos temps de réponse.** Vous n'êtes pas le seul à bénéficier de la vitesse et de l'étendue accrues du cloud. Les cybercriminels aussi. En ayant recours à des interfaces API bien définies, les attaquants consacrent moins de temps au repérage et sont plus vite opérationnels. L'analyse optimisée par l'intelligence artificielle et l'apprentissage automatique est essentielle pour identifier rapidement les signes d'activité malveillante et automatiser la réponse.


**Ne vous laissez pas distraire.** Des capacités de réaction rapide sont essentielles, mais ne représentent qu'une partie de l'équation. Sans un signalement efficace qui va à l'essentiel, des défenses automatisées trop zélées risquent d'être activées par des faux positifs. Avec une solution de détection des menaces optimisée par l'IA, vous pouvez orchestrer une intervention en aval à la fois précise, fiable et rapide.

VECTRA
SECURITY THAT THINKS

# Comment Vectra protège Microsoft 365 et Azure AD

Cognito, la solution de détection des menaces et de résolution des incidents de Vectra optimisée par l'IA, peut identifier et bloquer les attaquants opérant dans votre environnement Microsoft 365 et toute application SaaS fédérée utilisant Azure AD. Nous savons que les attaquants ne fonctionnent pas en vase clos. Nous pouvons suivre les signes de leur comportement dans les entreprises, les systèmes hybrides, les centres de données, les IaaS et les SaaS, le tout à partir d'un point de contrôle unique.

VECTRA
SECURITY THAT THINKS

Vectra Cognito émet des alertes priorisées très fiables plutôt que de gonfler le flux des alertes de sécurité continues. Il identifie les menaces critiques, telles que l'utilisation de comptes d'accès à privilèges, et les classe par ordre de priorité pour les éliminer avant que l'attaquant n'ait le temps de passer à l'acte.

Déploiement en un clin d'œil grâce à une approche native au cloud qui accélère la surveillance, la détection et la neutralisation des attaques

Couverture de sécurité complète de Microsoft 365, d'Azure AD et de l'infrastructure informatique locale

Blocage en temps réel des attaques connues et inconnues et des prises de contrôle de comptes d'utilisateur, avant qu'elles ne conduisent à des violations de données

« Avec Vectra, nous sommes plus proactifs que réactifs, ce qui constitue un avantage considérable à nos yeux. Au lieu de traquer des alertes dans des journaux non pertinents, je peux consacrer plus de temps à sensibiliser notre communauté d'utilisateurs finaux aux pratiques de sécurité importantes. »

**Kevin Orritt**
*Responsable de la sécurité des TIC*
*Greater Manchester Mental Health*

VECTRA
SECURITY THAT THINKS

Annexes

# Méthodologie

Commandée par Vectra, l'étude a été réalisée par Sapio Research auprès de 1 112 responsables de la sécurité informatique dans des organisations utilisant Microsoft 365 et comptant plus de 1 000 collaborateurs. Un sous-ensemble de 302 répondants, appartenant aux secteurs de l'administration publique, des soins de santé et de l'enseignement, a été utilisé pour produire les statistiques présentées dans cet eBook.

Dans l'ensemble, les résultats affichent une précision de ± 2,9 %, avec des intervalles de confiance de 95 %, en supposant un résultat de 50 %.

Les entretiens ont été menés en ligne par Sapio Research en février 2021 au moyen d'une invitation par e-mail et d'une enquête en ligne.

Pour découvrir comment Vectra peut vous aider à protéger votre environnement Microsoft 365 et Azure AD contre les prises de contrôle de comptes d'utilisateur et d'autres menaces majeures, contactez-nous à l'adresse **info_france@vectra.ai**.

E-mail : info_france@vectra.ai vectra.ai.fr


Version **071521**