VECTRA®
SECURITY THAT THINKS

ÉTUDE

Sécuriser Microsoft Office 365 face à la nouvelle normalité –

Réduire l'avance des attaquants sur les défenseurs

VECTRA
SECURITY THAT THINKS

Sommaire

Explosion de l'utilisation du cloud pendant la pandémie.....3

Évolution rapide du paysage des menaces.....6

Sécuriser Microsoft Office 365 est une priorité absolue.....9

Prises de contrôle de comptes d'utilisateur : une menace croissante.....11

Le manque de visibilité induit un excès de confiance.....13

Une confiance adaptée à la réalité.....16

Améliorer les niveaux de sécurité en 2021.....18

Dix mesures pour se protéger des cyberattaques basées sur l'identité dans Microsoft Office 365.....20

Comment Vectra protège Microsoft Office 365 et Azure AD.....22

Avant-propos

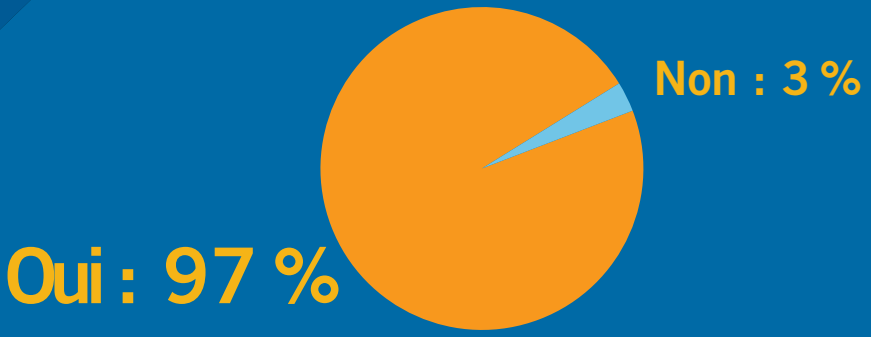
Aujourd'hui, Microsoft Office 365 est devenu indissociable de la productivité des entreprises. La nécessité d'adopter des méthodes de travail plus flexibles et agiles sur fond de pandémie de COVID-19 a encore consolidé sa place au cœur des processus métiers. Par ailleurs, la généralisation du cloud a élargi la surface d'attaque susceptible d'être exploitée par les cyberpirates. Les entreprises doivent être certaines de pouvoir défendre leur environnement Microsoft Office 365 face aux cybercriminels qui cherchent à exploiter ses puissantes fonctionnalités pour orchestrer des cyberattaques dommageables.

Cet eBook pose un regard neuf sur ce paysage nouveau et en rapide mutation. Nous avons interrogé 1 112 responsables de la sécurité informatique à travers le monde et avons recueilli leurs avis sur les principales menaces qui planent sur les environnements Microsoft Office 365, ainsi que sur leur capacité à s'en protéger.

Nous évoquerons aussi les mesures pratiques à prendre pour améliorer la sécurité de votre infrastructure Microsoft Office 365 et Azure Active Directory (AD), notamment les solutions à mettre en place pour identifier et neutraliser les menaces subtiles et dangereuses, dont les attaques de prise de contrôle de comptes d'utilisateur qui cherchent à exploiter les fonctionnalités de Microsoft Office 365 et d'autres applications SaaS pour vous nuire.

Explosion de l'utilisation du cloud pendant la pandémie

Autrefois considéré comme un avantage stratégique, le cloud est rapidement devenu indispensable au sein des entreprises. Son adoption, ainsi que l'efficacité et l'agilité qu'il procure, figurent en bonne place de l'ordre du jour des conseils d'administration depuis plusieurs années maintenant. Toutefois, il a fallu attendre 2020 pour que la plupart des entreprises voient leurs stratégies cloud réellement mises à l'épreuve.



97 % des responsables de la sécurité informatique interrogés ont utilisé davantage Microsoft Office 365 en raison de la pandémie.

Face à l'adoption rapide du télétravail, il n'est pas étonnant que l'utilisation de Microsoft Office 365 ait gagné du terrain au sein de nombreuses entreprises à des fins de collaboration. En mars 2020, on recensait 258 millions d'utilisateurs actifs, soit une hausse de plus de 70 millions par rapport à l'année précédente.

« Avec Vectra, nous sommes passés de zéro à 100 % de visibilité sur les comportements des attaquants. Nous avons été stupéfaits par ce que Vectra parvenait à déceler dans le trafic réseau. Nous bénéficions désormais d'un contexte et de détails sur chaque attaque, ainsi que sur son degré de dangerosité. »

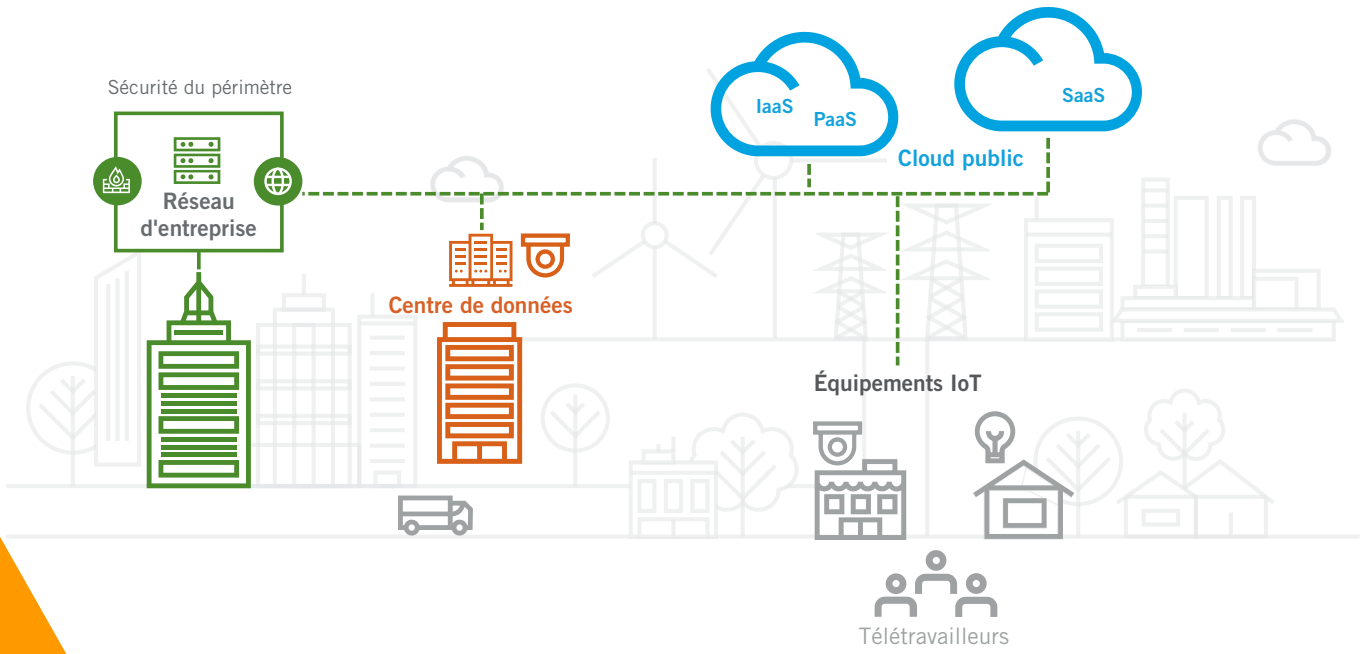
Responsable de la sécurité
Multinationale de services financiers

Cette transition contrainte et forcée a bouleversé irrémédiablement le paysage informatique. Nous avons interrogé des responsables informatiques du monde entier sur les conséquences de cette migration vers le télétravail sur leurs activités. Presque tous ont déclaré avoir accéléré leurs stratégies de transformation cloud et numérique en conséquence. Certains ont même pris deux ans d'avance sur leur planning.

L'évolution rapide du paysage informatique et l'accélération forcée de la migration vers le cloud ont aussi exacerbé la vulnérabilité des entreprises aux cybermenaces.

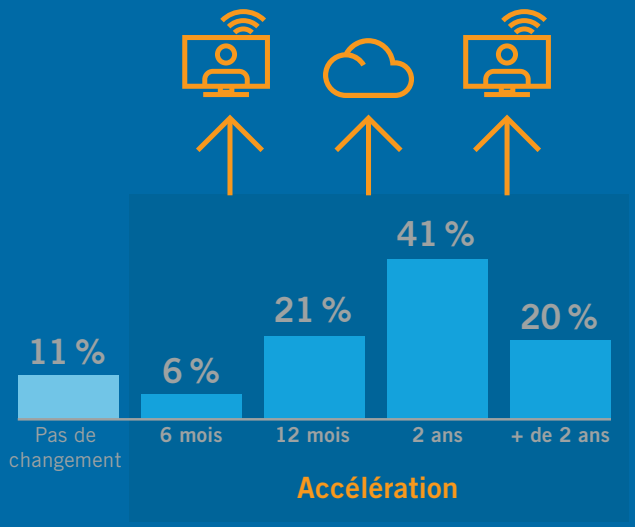
Cette adoption accélérée, qui tient plus du baptême du feu compte tenu des circonstances, semble avoir apporté des avantages tangibles pendant la pandémie. La plupart des responsables interrogés font état d'une amélioration de la productivité, de la satisfaction au travail et des horaires, même si certains ont observé l'inverse, en particulier dans le secteur des soins de santé.

Néanmoins, les aléas des confinements aux quatre coins du monde ont aussi mis à rude épreuve tous les secteurs économiques. Outre les répercussions sur les effectifs, l'évolution rapide du paysage informatique et l'accélération forcée de la migration vers le cloud ont aussi exacerbé la vulnérabilité des entreprises aux cybermenaces.



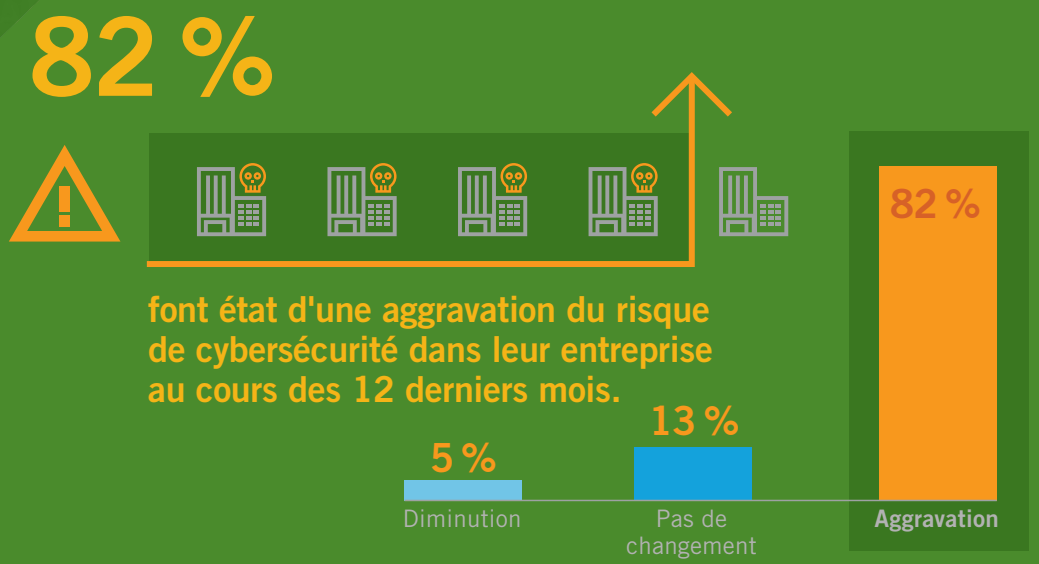
88 %

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.



Évolution rapide du paysage des menaces

En accélérant le déploiement de Microsoft Office 365 et d'Azure AD, de nombreuses entreprises ont étendu leur surface d'attaque et isolé des effectifs qu'elles ne sont peut-être pas en mesure de surveiller et de protéger efficacement. Dans cette nouvelle normalité, les responsables de la sécurité ont du retard à rattraper. Ils doivent en effet comprendre et sécuriser leurs environnements cloud, avec des outils et des stratégies de sécurité souvent lacunaires. Les cybercriminels n'ont pas tardé à flairer le bon 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.



VECTRA
SECURITY THAT THINKS

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 plupart des responsables de la sécurité estiment qu'au cours des 12 derniers mois, cette nouvelle donne a multiplié le risque de sécurité de leur entreprise.

Les administrateurs et les dirigeants sont nettement plus enclins à observer une accentuation de l'écart que les cadres de niveau inférieur.

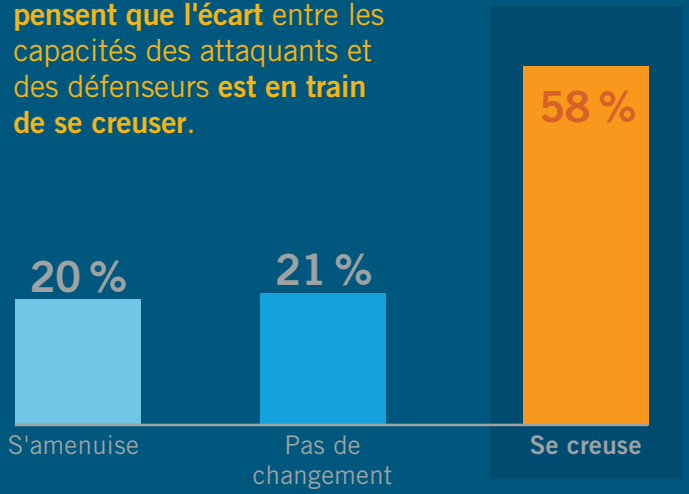
De leur côté, les attaquants peaufinent leurs techniques et mettent leur expérience à profit pour s'aventurer sur ce nouveau terrain et en exploiter les failles. C'est ainsi que les attaques de malware traditionnelles sont aujourd'hui délaissées au profit d'attaques ciblant les comptes, les identifiants,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

À l'heure où les cybercriminels redoublent d'ingéniosité et intensifient leurs attaques, les responsables de la sécurité sont nombreux à se montrer pessimistes. Près de trois sur cinq pensent que les pirates ont désormais plusieurs coups d'avance. Les administrateurs et les dirigeants sont nettement plus enclins à observer une accentuation de l'écart que les cadres de niveau inférieur.

La plupart des responsables de la sécurité estiment qu'au cours des 12 derniers mois, cette nouvelle donne a multiplié le risque pour la sécurité de leur entreprise.

58 %

pensent que l'écart entre les capacités des attaquants et des défenseurs **est en train de se creuser**.



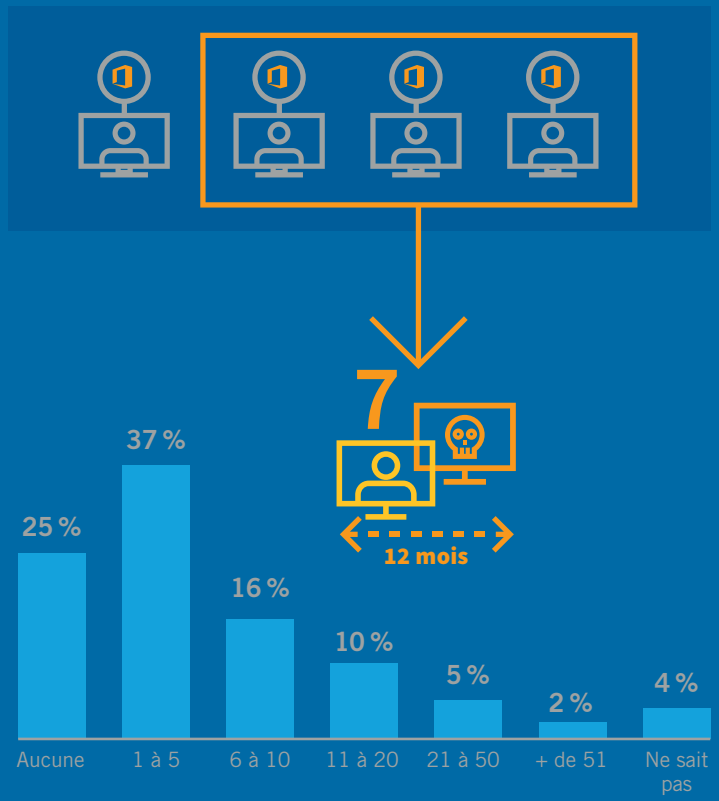
En réalité, compte tenu des progrès majeurs enregistrés par des outils tels que les solutions de détection et d'aide à la résolution des incidents (NDR) réseau ou les analyses optimisées par l'intelligence artificielle (IA), ce devrait être l'inverse. Une fois que les attaquants parviennent à infiltrer un environnement, ils comptent habituellement sur leur aptitude à se faire oublier dans le maelström des activités normales de l'entreprise. Les pirates prudents n'hésitent pas à exploiter les applications métiers légitimes (tactique « live off the land »), notamment celles intégrées à la suite Microsoft O365, telles que Power Automate et eDiscovery, pour se déplacer latéralement, se tapir dans le trafic HTTP, HTTPS et DNS, et exfiltrer des données. Les solutions NDR optimisées par l'IA qui s'intègrent aux applications et services cloud sont capables d'exposer cette couverture et d'identifier rapidement le moindre indice qu'un intrus est à l'œuvre.

Les solutions NDR optimisées par l'IA qui s'intègrent aux applications et services cloud sont capables d'exposer cette couverture et d'identifier rapidement le moindre indice qu'un intrus est à l'œuvre.

Cependant, si l'écart entre attaquants et défenseurs s'amenuise sur papier, cela ne concerne que les entreprises qui ont investi dans de telles fonctionnalités. Pour celles qui ne disposent pas des capacités nécessaires pour détecter les signes subtils d'activité malveillante, l'écart va continuer à se creuser, et les attaquants pourront profiter pleinement de leur infrastructure cloud. Si l'utilisation accrue du cloud n'est pas une surprise, l'attitude de certains responsables de la sécurité s'agissant de la gravité de la menace et de leur aptitude à y faire face est en revanche surprenante.

Pour celles qui ne disposent pas des capacités nécessaires pour détecter les signes subtils d'activité malveillante, l'écart va continuer à se creuser, et les attaquants pourront profiter pleinement de leur infrastructure cloud.

71 % des utilisateurs Microsoft Office 365 ont subi en moyenne sept prises de contrôle de comptes d'utilisateur légitimes au cours de l'année écoulée.



VECTRA
SECURITY THAT THINKS

Sécuriser Microsoft Office 365 est une priorité absolue

Microsoft Office 365 continue de jouer un rôle essentiel dans la continuité des activités métiers. Les entreprises doivent dès lors veiller à disposer des capacités nécessaires pour sécuriser leurs environnements cloud. Le problème est particulièrement pressant pour les entreprises 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 des comptes d'utilisateur.

Découvrez les

10 mesures pour se protéger des cyberattaques basées sur l'identité dans Microsoft Office 365

cliquez ou allez à la page 20

VECTRA
SECURITY THAT THINKS

Microsoft Office 365 est souvent au cœur des processus métiers d'une entreprise. Il facilite le stockage et le partage de la quasi-totalité des données et fait office de fournisseur d'identité pour l'accès à une multitude d'autres applications SaaS. Un environnement Microsoft Office 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 rapport Spotlight consacré à Microsoft Office 365 a passé au crible plus de quatre millions de comptes. 96 % d'entre eux présentaient des signes de déplacement latéral.

Microsoft Office 365 est souvent au cœur des processus métiers d'une entreprise. Il facilite le stockage et le partage de la quasi-totalité des données et fait office de fournisseur d'identité pour l'accès à une multitude d'autres applications SaaS.

Par ailleurs, de nombreux répondants s'inquiètent de la capacité des attaquants à exploiter les ressources locales et notamment des outils Microsoft légitimes, tels que Power Automate et eDiscovery. Il s'agit même du principal problème épinglé par les répondants établis à Singapour, ainsi que par ceux travaillant dans le commerce de détail au niveau mondial.

Cette évolution s'accompagne d'une menace accrue d'attaques basées sur l'identité. Au vu du large éventail de fonctionnalités et de données auxquelles un utilisateur de Microsoft Office 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 en 2021.

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

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

45 %

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

40 %

Les attaques par ransomware vont s'intensifier.

45 %

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

45 %

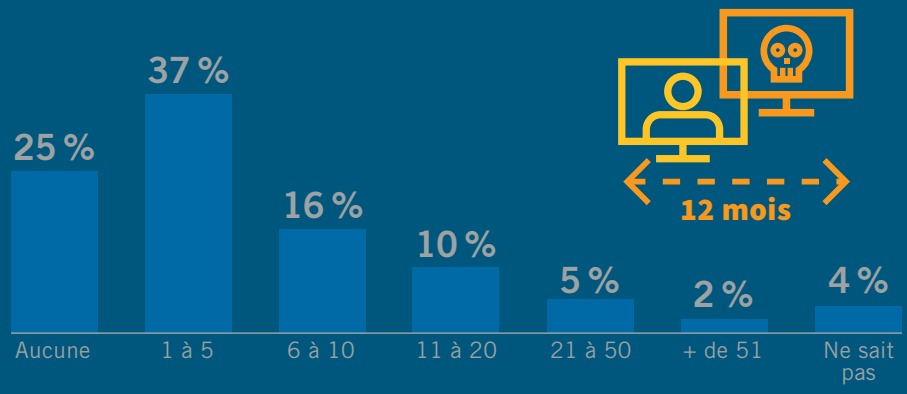
Capacité des pirates à brouiller les pistes en détournant des outils Microsoft légitimes tels que Power Automate et e-Discovery.

VECTRA
SECURITY THAT THINKS

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

L'agilité et l'interconnectivité offertes par le cloud public 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. Les attaquants avouent qu'il est simple d'y effectuer un repérage et de trouver les clients et leurs conventions de nommage probables.

7 **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'entreprise, 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 Office 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. Dès qu'un compte à privilèges est compromis, les attaquants peuvent utiliser les API légitimes de l'entreprise pour exfiltrer les informations convoitées.

Des responsables de la sécurité informatique avouent avoir subi en moyenne sept prises de contrôle de comptes d'utilisateur autorisés au cours des douze derniers mois.

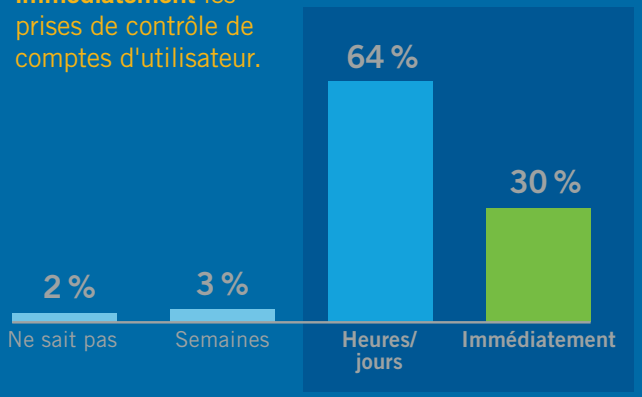
Force est de constater qu'en dépit du nombre d'incidents et du risque élevé que présente ce type de compromission, la majorité des répondants sont plutôt confiants en leur capacité à faire face à des prises de contrôle de comptes d'utilisateur.

63 % d'entre eux pensent pouvoir identifier et bloquer une prise de contrôle de comptes en quelques jours, voire en quelques heures. Ils sont 30 % à s'estimer capables d'endiguer immédiatement une telle attaque.

Les comptes compromis peuvent servir à infliger de lourds dégâts dans un laps de temps très court. Les entreprises qui estiment à plusieurs jours le délai nécessaire pour identifier une prise de contrôle restent donc extrêmement vulnérables. Il est impératif qu'elles 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.

Près de **30 %** indiquent que leur équipe de sécurité est à même d'identifier et de bloquer **immédiatement** les prises de contrôle de comptes d'utilisateur.

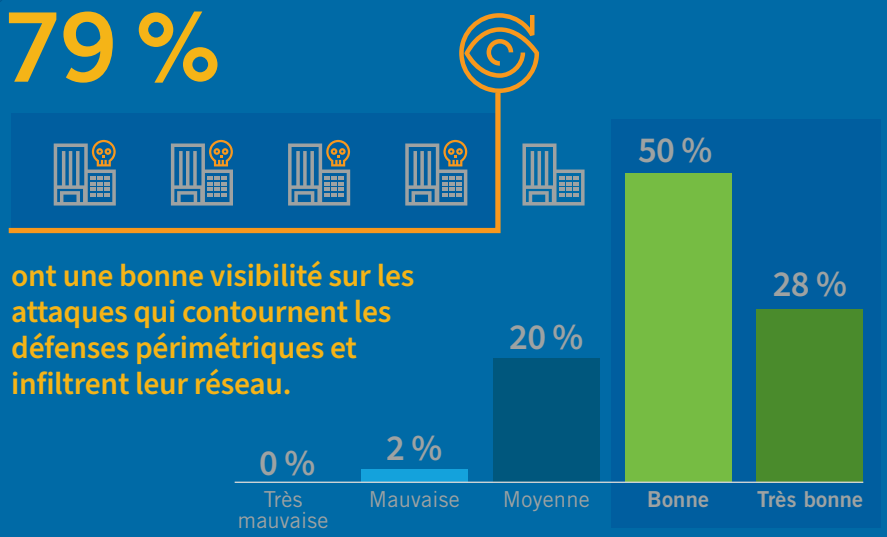
64 % déclarent pouvoir bloquer les prises de contrôle de comptes d'utilisateur en quelques heures ou jours.



VECTRA
SECURITY THAT THINKS

Le manque de visibilité induit un excès de confiance

Les responsables de la sécurité 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. La durée moyenne d'une attaque est estimée à 43 jours – et les outils de sécurité préventifs sont incapables de détecter les prises de contrôle de comptes d'utilisateur.



De manière générale, les répondants sont également assez confiants en leurs capacités 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 Office 365 analysés présentent des signes de déplacement latéral.

La durée moyenne d'une attaque est estimée à 43 jours.

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

Notons que 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.

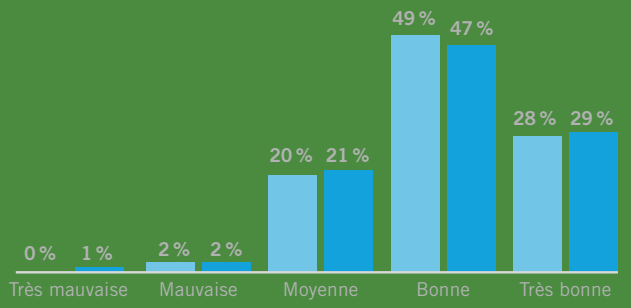
Par exemple, un centre d'opérations de sécurité (SOC) peut être confronté à des centaines de menaces au quotidien. Si l'on considère le nombre d'incidents déjoués comme principal indicateur de succès, tout va pour le mieux dans le meilleur des mondes. Cependant, cette approche élude les vraies questions 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.

77 %

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

76 %

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



S'agissant des attaques les plus dangereuses, comme 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.

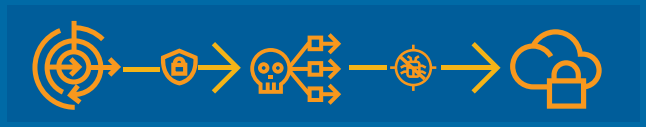
Enfin, l'impression que le respect des bonnes pratiques de sécurité protège des attaques peut aussi expliquer cet excès de confiance. Néanmoins, le fait est que les cybercriminels ajustent constamment leurs tactiques pour balayer tous les obstacles placés sur leur chemin.

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.

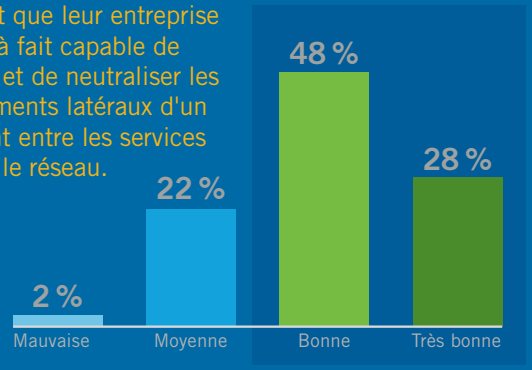
« Vectra fournit à nos analystes SOC toutes les informations nécessaires sur les menaces. Cognito constitue un atout inestimable pour les environnements Microsoft Office 365. »

Responsable de la sécurité
Multinationale de services financiers

76 %



affirment que leur entreprise 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'entreprise. Les attaques à longue durée d'implantation constituent la principale menace pour les entreprises. L'accès à une série de données et d'applications en quelques secondes seulement suffit pour causer de nombreux problèmes dans les entreprises. 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 des analystes en sécurité : 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 Office 365. »

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

Améliorer les niveaux de sécurité en 2021

La plupart des responsables de la sécurité ont adopté une approche assez visionnaire pour améliorer les niveaux de sécurité en 2021. C'est encourageant. La plupart prévoient d'investir davantage dans la technologie et les personnes, mais ils tendraient à privilégier des solutions capables de protéger efficacement les environnements Microsoft Office 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 45 % des personnes interrogées citent la technologie NDR comme étant l'une des solutions pour leurs équipes SOC.

Le déploiement de solutions d'IA et le renforcement de l'automatisation sont deux 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 NDR optimisées par l'IA font partie de l'équation.

Enfin, l'augmentation des investissements dans la traque des menaces et d'autres mesures proactives fait aussi partie des priorités évoquées et permettra aux entreprises 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 Office 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 :

58 %
Augmentation prévue des investissements dans les technologies et les ressources humaines pour améliorer le niveau de sécurité en 2021

52 %
Recours accru à l'automatisation et à l'intelligence artificielle

47 %
Utilisation de la cyberveille

45 %
Évolution vers une traque proactive des menaces

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

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 Office 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 Office 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 NDR 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 Office 365 et Azure AD

Cognito, la solution NDR de Vectra optimisée par l'IA, peut identifier et bloquer les attaquants opérant dans votre environnement Microsoft Office 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 Office 365, d'Azure AD et de l'infrastructure locale de votre entreprise

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, cette étude a été menée par Sapio Research auprès de 1 112 responsables de la sécurité informatique dans des entreprises utilisant Microsoft Office 365 et comptant plus de 1 000 collaborateurs, dans les secteurs suivants : pharmaceutique, administration, finance, vente au détail, fabrication, soins de santé et enseignement.

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 Office 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 **032521**