LE GUIDE POUR LES MSP

OPTIMISEZ VOS TÂCHES ET AUGMENTEZ VOTRE RENTABILITÉ

HORNETSECURITY

AMY BABINCHAK

Amy Babinchak est une éminente professionnelle de l'informatique, propriétaire d'entreprise et leader d'opinion avec plus de vingt ans d'expérience dans l'industrie technologique. Elle possède plusieurs entreprises informatiques, dont Harbor Computer Services, qui a été classée 40ème parmi les 501 premiers MSP aux États-Unis, avant de vendre son entreprise MSP en 2023.

Amy assure actuellement la gestion de Third Tier, où elle propose des services d'assistance informatique avancés aux fournisseurs et aux consultants, en se concentrant sur les technologies Microsoft.

Les prouesses techniques d'Amy ne sont plus à démontrer dans le secteur. Elle a reçu le titre de Microsoft Most Valuable Professional (MVP) pendant 18 ans, ce qui témoigne de ses connaissances approfondies et de ses contributions à l'écosystème Microsoft. Ses compétences avancées en matière de conception, de gestion et de mise en œuvre de réseaux lui ont valu d'être reconnue comme l'un des 100 meilleurs professionnels de l'informatique par MSP Mentor. Outre son statut de MVP, Amy est titulaire de plusieurs certifications Microsoft, dont celle d'administrateur d'identité et d'accès.

PAUL SCHNACKENBURG

Paul a fait ses premiers pas dans l'informatique à l'époque où DOS et les processeurs 286 étaient à la pointe de la technologie. Il dirige Expert IT Solutions, une société de conseil en informatique pour petites entreprises située sur la Sunshine Coast, en Australie. Il est également professeur d'informatique à la Microsoft IT Academy.

Paul est un auteur technologique très respecté et actif dans la communauté, rédigeant des articles techniques approfondis, axés sur Hyper-V, System Center, le cloud privé et hybride et les technologies de cloud public Office 365 et Azure. Il est titulaire des certifications MCSE, MCSA et MCT.

HORNETSECURITY

TABLE DES MATIÈRES

HORNETSECURITY

CHAPITRE 1

INTRODUCTION À L'AMÉLIORATION DE L'EFFICACITÉ DES MSP

L'essence même de cet eBook est de fournir aux MSP des stratégies pratiques leur permettant d'opérer plus efficacement dans plusieurs domaines d'activité et de rester compétitifs dans un secteur qui évolue rapidement. En lisant cet eBook, vous comprendrez comment les MSP les plus efficaces fonctionnent, vous améliorerez votre rentabilité et resterez en tête de la demande.

Les MSP sont confrontés à des défis et à des opportunités sans précédent. Nous verrons comment les MSP les plus performants ont exploité les outils d'automatisation pour rationaliser leurs opérations et réduire leurs coûts tout en maintenant la relation client, qui est d'une importance capitale. Cet eBook vous guidera à travers les stratégies essentielles pour prospérer dans cet environnement dynamique.

COMPRENDRE COMMENT NOUS EN SOMMES ARRIVÉS LÀ

Le modèle d'entreprise que nous appelons fournisseur de services gérés (MSP) a été créé lorsque l'infrastructure était conservée dans les locaux du client et lui appartenait. Les serveurs étaient omniprésents, les ordinateurs n'étaient rien d'autre que des objets stationnaires sur des bureaux reliés à des câbles Ethernet et le personnel de bureau ne travaillait pas ou très peu le week-end. Le MSP aspirait à incarner le service informatique externalisé de l'entreprise et à réaliser des économies en partageant son temps entre un petit nombre de clients. Le personnel du MSP était lui-même hautement technique en matière de configuration d'infrastructure, de déploiement et de dépannage.

La majorité des opérations effectuées par le MSP sinon toutes, sont réalisées manuellement et en personne. Les outils utilisés étaient des aides au dépannage minimales comme TechNet, Wireshark et des testeurs de câbles. Beaucoup de pizzas et de boissons sucrées à base de caféine ont été consommées pendant les mises à niveau des serveurs, les sessions marathon de dépannage avec Microsoft au bout du fil et les réunions des groupes d'utilisateurs.

Puis le Cloud fit son apparition.

Le Cloud a donné lieu à un changement d'ensemble de compétences. Au lieu de se concentrer sur l'installation du serveur et la connectivité, le MSP devait désormais comprendre comment gérer les applications à distance. Du fait de la demande de services ainsi que de la demande d'une plus grande variété de services, les MSP ont dû embaucher davantage de personnel et le répartir sur un plus grand nombre de clients afin de maintenir leur rentabilité, car certaines sources de revenus sont passées de projets d'infrastructure très rentables à des abonnements à des logiciels à faible marge avec des frais de comptabilité permanents.

Puis les cybercriminels sont apparus.

L' avènement du Cloud a augmenté la probabilité que le cybercriminel puisse atteindre les données de l'entreprise, du coup il était question de mettre en place des outils plus élaborés, inventant les fléaux que nous combattons aujourd'hui avec le ransomware et l'hameçonnage. Le piratage informatique a toujours existé, mais à partir de 2013, avec l'invention des ransomwares, la perturbation des activités s'est accrue rapidement.

Puis le secteur de la cyberassurance et les réglementations en matière de conformité sont apparus.

Lorsque des rançons ont été payées, la cybercriminalité a explosé et une série d'exigences de conformité à la loi sur la cybercriminalité, spécifiques à chaque secteur, a vu le jour. Les MSP se sont retrouvés en première ligne de défense, sans les compétences ou le modèle de tarification nécessaires pour répondre aux besoins des clients, et ont dû s'adapter rapidement pour faire face à ces nouvelles demandes. La plupart d'entre eux ont investi massivement dans un nombre croissant d'outils logiciels pour les aider à combler leurs lacunes en matière de compétences et à automatiser les tâches répétitives. Aujourd'hui, les MSP consacrent généralement 20 % ou plus de leur chiffre d'affaires à l'achat d'outils logiciels. C'est devenu une crise due à l'inefficacité.

FONCTIONNER EN MSP EFFICACE

Le secteur dans lequel les MSP opèrent a connu une évolution fulgurante, mais le modèle d'entreprise a mis du temps à s'adapter et de nombreux MSP peinent à maintenir leur rentabilité dans un secteur qui était réputé pour ses bénéfices élevés et sa source d'emplois bien rémunérés. La bonne nouvelle est que les entreprises savent qu'elles ont besoin des MSP et que les MSP savent qu'ils doivent se moderniser pour rester prospères et rentables.

Dans cet eBook, nous allons examiner plusieurs domaines majeurs des opérations des MSP, souligner les gains d'efficacité et suggérer des moyens de les obtenir. L'accent sera mis sur Microsoft 365 et la cybersécurité, car nous examinerons les MSP qui fondent leurs pratiques sur ces produits. Nous n'aborderons pas de solutions techniques très spécifiques, ni de questions financières, mais nous vous aiderons à apprécier la vue d'ensemble du fonctionnement d'un MSP efficace. Vous comprendrez ainsi comment le secteur peut continuer à créer de bons emplois, à fournir un service nécessaire et à maîtriser des questions techniques qui ne sont pas près de disparaître, comme la cybersécurité et la conformité. Le MSP joue un rôle très important dans la réussite de toutes les entreprises, dans toutes les économies du monde. Lorsqu'un MSP réussit, tout le monde y gagne.

Êtes-vous prêt à révolutionner votre activité de MSP et à franchir de nouvelles étapes en termes d'efficacité ? Nous allons nous plonger dans le vif du sujet et découvrir les secrets de la réussite, en commençant par la première tâche qu'un MSP rencontre avec un nouveau client : l'onboarding.

HORNETSECURITY

CHAPITRE 2

L'INTÉGRATION

L'intégration est souvent considérée comme une dépense et une perte de ressources humaines. Toutefois, ce chapitre vise à changer votre point de vue en soulignant les avantages d'un processus d'intégration bien exécuté et en fournissant des conseils pour en améliorer l'efficacité.

DEUX VISIONS DE L'INTÉGRATION

Il peut être difficile de comprendre comment un client perçoit le travail d'un MSP.

Des clients qui n'ont pas forcément des connaissances techniques très poussées, se concentrent sur l'expérience de travailler avec vous, alors que les MSP ont tendance à se focaliser sur les résultats. Cette différence de perspective fait du processus d'intégration une occasion cruciale d'impressionner et de ravir les nouveaux clients.

Qu'est-ce qui impressionnera le client ? Qu'est-ce qui le ravira ?

IMPRESSIONNER	RAVIR
Professionnalisme	Personnalisation
Efficacité	Réactivité
Expertise	Amabilité
Fiabilité	Souci du détail

Graphique 1 **Impressionner et ravir les clients**

RÉSULTATS DE L'INTÉGRATION	
Joindre les points d'accès à la solution de gestion	Migrer vers les solutions Microsoft 365
Sécuriser les terminaux	Réduire les temps d'arrêt
Déployer des applications	Déployer les outils MSP
Configurer les exigences de conformité	Terminer rapidement

Graphique 2 **Les points sur lesquels les MSP se concentrent**

L'INTÉGRATION DU POINT DE VUE DU CLIENT

De plus en plus, c'est sur les compétences non techniques que votre client vous évalue. Au début, il pensera probablement qu'il peut s'adresser à n'importe qui et tirer son épingle du jeu en engageant de bonnes compétences techniques. Mais c'est votre processus de vente qui les a incités à vous choisir. C'est votre argumentaire, votre site web, la communication de votre proposition de valeur unique, qui les a convaincus de vous choisir par rapport aux autres MSP qu'ils ont interrogés. Si nous gâchons ce « bon ressenti » lors de l'intégration, la relation avec le client peut être entachée à jamais. Nous devons les impressionner dès le premier jour de l'intégration.

Si l'on met en pratique les deux tableaux ci-dessus, voici ce sur quoi l'équipe du MSP devrait se concentrer.

1. LE PROFESSIONNALISME :

Communication claire : maintenir une communication claire et cohérente avec le client tout au long du processus d'intégration. Expliquez chaque étape en des termes clairs et définissez des attentes précises. Une bonne communication aide les clients à rester calmes et patients, tout en abordant les problèmes potentiels de l'entreprise.

Documentation : fournir une documentation en langage clair pour tous les processus et procédures. Cela permet au client de comprendre ce qui est fait et de s'assurer qu'il dispose d'une référence pour ce qu'il voit se produire autour de lui.

Apparence : veillez à ce que toutes les interactions, qu'elles soient personnelles ou virtuelles, se déroulent de manière professionnelle. Cela implique de s'habiller de manière appropriée et de maintenir un comportement professionnel et amical.

2. EFFICACITÉ :

Processus rationalisés : les clients ne comprennent peut-être pas les détails techniques, mais ils savent reconnaître l'inefficacité. Mettez en œuvre des stratégies pour faire de l'intégration un processus reproductible et appliquez les enseignements tirés de chaque nouveau client pour améliorer l'expérience du suivant.

Automatisation : automatisez l'intégration à Intune pour simplifier la configuration, la conformité, la configuration de la sécurité et le déploiement d'applications sur les terminaux Windows et d'autres plates-formes.

Résolution rapide : traitez rapidement et efficacement tout problème ou préoccupation afin de minimiser les temps d'arrêt et d'assurer une expérience d'intégration harmonieuse. N'oubliez pas de communiquer le processus en cours de route et de vérifier auprès du client comment il réagit au processus de résolution.

3. EXPERTISE :

Partage des connaissances : préparez le client au processus d'intégration en organisant une brève réunion pour lui expliquer les étapes à suivre. Ensuite, partagez votre expertise avec le client en lui proposant des sessions de formation et des ressources qui l'aideront à comprendre et à utiliser les services fournis.

Résolution de problèmes : démontrez votre expertise en résolvant efficacement tous les problèmes techniques qui surviennent au cours du processus d'intégration. Ne les gardez pas pour plus tard. Le client est susceptible de considérer toute anomalie laissée comme un échec du processus d'intégration.

La Personnalisation : En adaptant le processus d'intégration aux besoins et aux exigences spécifiques du client, vous démontrez votre capacité à fournir des solutions personnalisées. Une chose aussi simple que le téléchargement du logo, du nom de l'entreprise et d'une photo d'arrière-plan montre que vous proposez une solution qui leur est propre.

4. FIABILITÉ :

Des performances constantes : les nouveaux clients peuvent avoir eu des expériences négatives avec des MSP précédents. Veillez à ce que toutes les tâches et tous les processus soient exécutés avec précision et dans les délais impartis afin d'instaurer la confiance dans vos services.

Suivi : assurez un suivi avec le client après le processus d'intégration afin de résoudre tout problème persistant et de vous assurer de la satisfaction dudit client. Le client pense que vous avez oublié quelque chose ? Réglez-le immédiatement.

Un soutien fiable : fournissez une assistance fiable tout au long du processus d'intégration et au-delà, en veillant à ce que le client se sente soutenu et valorisé.

Si votre MSP coche toutes ces cases, l'enchantement suivra. En se concentrant sur le professionnalisme, l'efficacité, l'expertise et la fiabilité, les MSP sont à même de créer une expérience d'accueil agréable pour les clients. Lorsque vous faites un suivi pour connaître l'impression du client sur l'expérience d'accueil, vous devriez entendre des mots de satisfaction de la part de votre client, tels que « amical », « professionnel », « expert » et « bien informé ». Vous saurez alors que vous avez fait du bon travail pour consolider la relation avec le client en lui offrant une expérience d'intégration exceptionnelle.

Ce sont souvent les petites choses qui comptent - je me souviens avoir accueilli un client qui avait encore un serveur sur place, et le propriétaire de l'entreprise était stupéfait que nous ayons pris le temps d'imprimer de petites étiquettes pour chaque câble connecté au serveur, ainsi que pour les câbles de réseau. Il a dit que personne d'autre n'avait jamais fait cela, et j'ai expliqué que le peu de temps supplémentaire passé maintenant pourrait faire gagner beaucoup de temps en cas de crise à l'avenir. Tout étiqueter et tout documenter fait partie d'un bon processus d'intégration.

L'INTÉGRATION DU POINT DE VUE DU MSP

Bien que nous comprenions ce que le client perçoit comme une expérience d'intégration réussie, il est important de reconnaître que, du point de vue du MSP, une grande partie du travail se fait en coulisses pour assurer ce succès.

Dans la **le graphique 2**, vous vous demandez peut-être pourquoi l'expression « terminer rapidement » figure sur la liste. La rapidité d'exécution permet de satisfaire le client en évitant que la migration vers vos services ne s'éternise et ne perturbe son activité. Du point de vue du MSP, terminer rapidement signifie que nous ne consacrons que le nombre d'heures de travail nécessaire au projet, ce qui optimise nos ressources et notre efficacité.

EFFICACITÉ DE L'INTÉGRATION

La première étape pour améliorer l'efficacité de l'intégration des nouveaux clients consiste à concevoir un processus de collecte d'informations. Par exemple, le MSP doit rassembler les licences existantes, les mots de passe des administrateurs et la transition MFA, ainsi que consolider la documentation dans votre système. L'expérience démontre que la plupart de ces informations ne seront pas disponibles auprès du client ou de l'ancien MSP. Dans ce cas, vous aurez besoin d'une méthode éprouvée pour rassembler rapidement ces informations.

L'efficacité de l'intégration passe par la répétabilité et l'automatisation. Ces deux concepts permettent à votre MSP de rester rentable tout en impressionnant les clients par votre professionnalisme et votre comportement. Dans votre compte partenaire Microsoft, avec l'achat d'un plan Action Pack ou supérieur, vous avez accès à au moins un environnement de démonstration. Les environnements de démonstration sont excellents pour la mise en place de vos paramètres standard.

L'une des limites de l'utilisation d'un environnement de démonstration pour mettre en scène vos paramètres est que vous n'avez pas l'expérience de ce que c'est que de vivre avec ces paramètres. Par conséquent, vous pouvez envisager d'utiliser l'environnement de production de votre MSP pour les paramètres en tant que "test". C'est une bonne idée pour le MSP d'expérimenter le niveau de sécurité de son environnement le plus sûr et de le maintenir comme standard de référence. Ce concept est affectueusement connu dans l'industrie sous le nom de « manger sa propre nourriture pour chien ». Testez ensuite les paramètres sur un groupe de clients tolérants au changement pour votre prochain test avant de procéder à un déploiement à grande échelle. Grâce à ce processus, vous commettrez moins d'erreurs et vous donnerez l'occasion à votre équipe marketing de préparer des messages sur les nouveaux paramètres et au personnel du service support de modifier ses procédures.

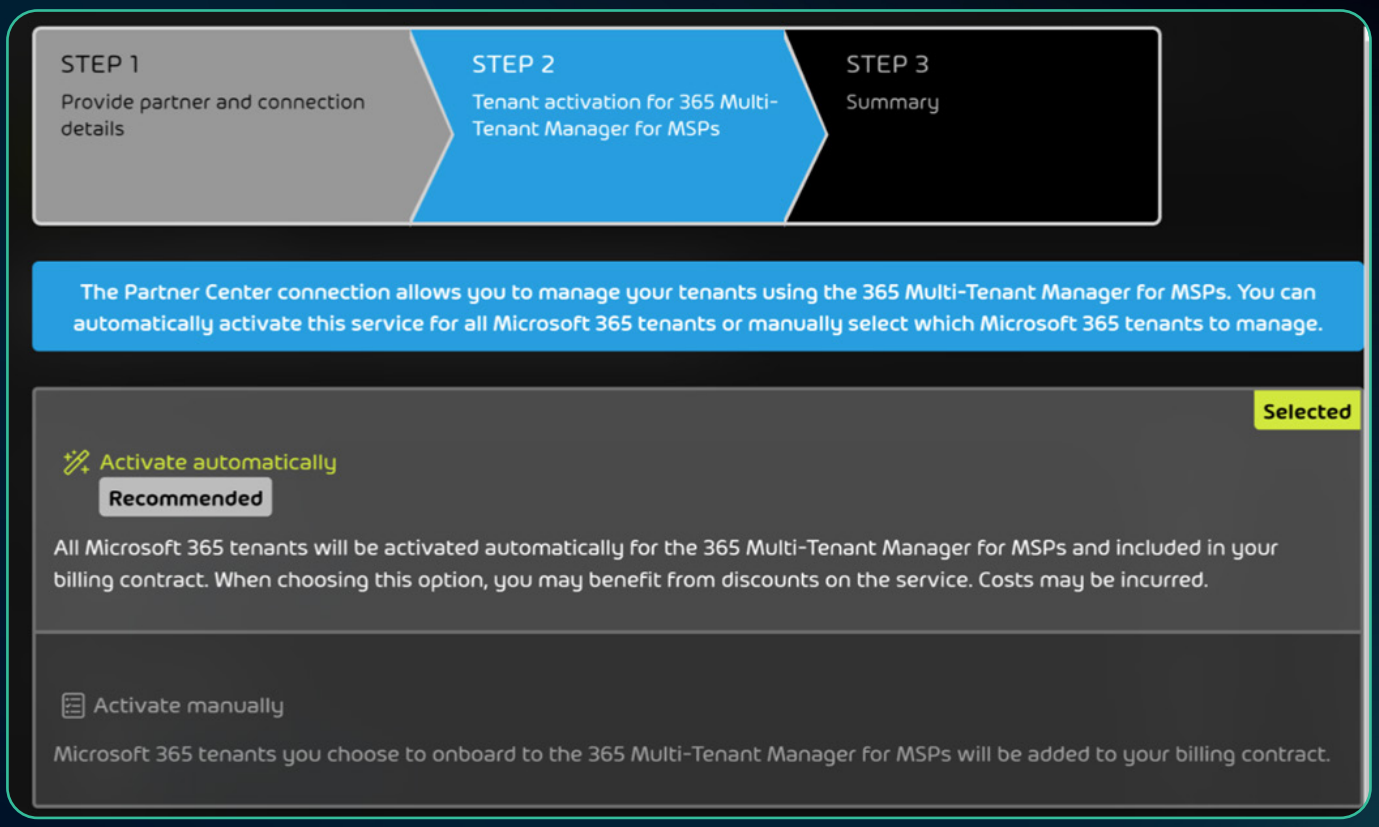
ACCOMPLIR NOS TÂCHES

Pour que l'intégration soit efficace, nous devons accomplir les quatre tâches suivantes :

Automatiser l'intégration des appareils	Automatiser la configuration des appareils	Normaliser la configuration du portail	Normaliser les contrôles de sécurité

Graphique 3 Tâches d'onboarding

Vos environnements peuvent être intégrés assez facilement dans un portail « à guichet unique » en utilisant le **365 Multi-Tenant Manager pour les MSPs de Hornetsecurity**. Cela vous permet de sélectionner tous vos clients à partir du portail des partenaires Microsoft ou une sélection d'entre eux, comme le souligne la **le graphique 3** ci-dessous.



Graphique 4 Utilisez l'assistant pour intégrer rapidement vos tenants dans votre portail de gestion

Une fois vos environnements rassemblés, Microsoft propose plusieurs outils pour faciliter l'intégration des appareils, chacun d'entre eux étant adapté à différents scénarios de clients.

- **Windows Autopilot** est idéal pour automatiser l'enrôlement et la configuration des appareils, en offrant une connexion Microsoft Entra rationalisée pendant l'expérience Windows Out-of-Box (OOBE). Il permet de déployer de nouveaux appareils sans aucune intervention.
- **L'inscription en bloc** est adaptée aux appareils existants ou aux scénarios où l'Autopilot n'est pas applicable.
- **L'inscription à Microsoft Device Management (MDM)** avec Intune permet aux appareils d'être automatiquement inscrits à MDM au cours du processus d'adhésion à Microsoft Entra, ce qui permet de les gérer dès qu'ils rejoignent votre entreprise.
- **L'inscription en libre-service** est idéale pour les scénarios BYOD. Les utilisateurs peuvent inscrire leurs propres appareils via les paramètres Windows ou OOBE.
- **PowerShell et les tâches** planifiées peuvent être utilisées pour les appareils Entra AD existants qui doivent être enrôlés dans Intune. Un script PowerShell peut déclencher deviceenroller.exe avec les paramètres appropriés, ou une tâche planifiée exécutée dans le contexte du système peut exécuter le script d'enrôlement.

Une fois les appareils intégrés à l'aide de l'une des méthodes ci-dessus, ils seront prêts à être configurés avec Intune. Intune est votre outil pour pousser la configuration des appareils et les paramètres de conformité. Microsoft fournit des lignes de base et des modèles de sécurité pour vous aider à créer vos normes.

L'une des clés de l'efficacité est d'avoir une norme bien documentée avec un ensemble de listes de contrôle et de procédures opérationnelles standard (POS) afin que le processus puisse être répété par l'ensemble de votre personnel à chaque fois qu'un nouveau client est intégré. Aucun outil automatisé n'est inclus dans la suite Microsoft 365. Au lieu de cela, vous devez acheter un outil sectoriel ou utiliser OneNote, par exemple.

La prochaine étape vers l'efficacité de l'intégration consiste à normaliser la configuration du portail et les contrôles de sécurité. Ces deux éléments interviennent lors de l'intégration, mais nous devons également maintenir les normes au fil du temps. Microsoft propose des outils d'aide à la configuration initiale, tels que les lignes de base de sécurité et l'outil de configuration de l'état souhaité. Cependant, chacun de ces outils comporte ses limites. Si vous choisissez d'utiliser les lignes de base de sécurité, vous devrez tester et adopter les changements au fur et à mesure de leur publication par Microsoft. En outre, les lignes de base fournies ont tendance à être très strictes, et de nombreux utilisateurs peuvent trouver difficile d'exercer leur fonction avec l'implémentation complète. Vous devrez les tester avec chaque client. Une fois la norme établie, vous pouvez créer une « image de référence » à l'aide de l'outil de configuration de l'état désiré. Cet outil vous permet ensuite de pousser cette configuration vers un environement que vous devez intégrer avec des paramètres identiques.

En pratique, la plupart des MSP trouvent ces outils assez difficiles à utiliser. De meilleures options peuvent être disponibles dans des solutions tierces comme **365 Multi-Tenant Manager pour les MSPs** de Hornetsecurity. Cette solution vous permet d'enregistrer une « image de référence » personnalisée et d'utiliser votre propre ensemble de paramètres pour l'envoyer à un nouveau client.

RÉSUMÉ

Pour conclure, l'efficacité de cette intégration est cruciale pour maintenir la rentabilité et impressionner les clients par le professionnalisme et l'attitude adoptée. En exploitant des outils tels qu'Intune pour la configuration des appareils et les paramètres de conformité, et en utilisant les lignes de base et les modèles de sécurité fournis par Microsoft, les MSP peuvent créer un processus d'intégration standardisé et reproductible. Cependant, il est essentiel de disposer de normes, de listes de contrôle et de procédures opérationnelles standard (POS) bien documentées pour garantir la cohérence entre tous les membres du personnel.

Il est essentiel de normaliser la configuration du portail et les contrôles de sécurité lors de l'intégration et de maintenir ces normes au fil du temps. Alors que Microsoft fournit des outils tels que les lignes de base de sécurité et l'outil Desired State Configuration, les MSP peuvent trouver des solutions tierces telles que **365 Multi-Tenant Manager** pour les MSPs de Hornetsecurity plus conviviales et plus efficaces pour créer et déployer des « images de référence » personnalisées et même, comme nous le verrons dans les chapitres suivants, pour maintenir et mettre à jour la posture de sécurité du réseau.

En se concentrant sur l'automatisation, la standardisation et une documentation complète, les MSP peuvent rationaliser le processus d'intégration, minimiser les temps d'arrêt et assurer une transition en douceur pour les nouveaux clients. Cette approche permet non seulement d'améliorer l'efficacité, mais aussi de renforcer la confiance pour ce qui est des services fournis, ce qui se traduit en fin de compte par une expérience d'intégration réussie et agréable pour les clients.

HORNETSECURITY

CHAPITRE 3

SUIVI ET MAINTENANCE

Le suivi et la maintenance sont depuis belle lurette la pierre angulaire du MSP. La maintenance nous donne un coup de pouce dans notre travail proactif, tandis que le suivi automatisé nous tient au courant des changements et des menaces. Avec l'augmentation des exigences en matière de cybersécurité et de conformité, ces tâches n'ont jamais été aussi importantes. Elles n'ont jamais non plus occupé autant de cycles cérébraux qu'aujourd'hui.

L'efficacité du suivi et de la maintenance peut s'avérer délicate. Il est facile de penser que nous devrions tout automatiser, mais la réalité est que les cerveaux humains et l'expertise ont toujours leur place majeure. Nous devons également réfléchir à ce qui se passe lorsque notre suivi détecte un problème grave. C'est en conjuguant le besoin d'efficacité et la mise en œuvre humaine de la réponse que le MSP doit trouver le juste milieu en ce qui concerne la rentabilité. D'une certaine manière, notre travail est plus difficile et plus complexe aujourd'hui que jamais, ce qui a créé beaucoup de stress pour les propriétaires et le personnel des MSP. C'est en mettant en place des procédures et des plans que nous restons efficaces et que nous gérons efficacement la charge de travail.

MAINTENANCE PROACTIVE

La maintenance proactive est essentielle pour prévenir les problèmes avant qu'ils ne passent en mode critiques. Les logiciels traditionnels de suivi et de maintenance à distance (RMM) disponibles sur le marché sont lourdement chargés de dettes techniques. Ils se concentrent principalement sur la gestion des mises à jour logicielles et la recherche de défauts au niveau du matériel. Bien que cela soit important, la balance penche beaucoup moins dans cette direction aujourd'hui. Les mises à jour du système d'exploitation sont désormais plus sûres et les utilisateurs sont devenus plus avertis. Les mises à jour peuvent être programmées pour être installées nativement dans le système d'exploitation et les applications.

Backblaze SSD Lifetime Annualized Failure Rates

Reporting period: 10/1/2018 to 06/30/2023 inclusive for active drive models as of 06/30/2023

MFG	Model	Size (GB)	Drive Count	Drive Days	Drive Failures	AFR	Confidence Interval	
Crucial	CT250MX500SSD1	250	598	205,743	9	1.60%	0.9%	3.3%
Dell	DELLBOSS VD	500	411	304,937	0	0.00%	0.0%	0.4%
Micron	MTFDDAV240TCB	250	88	83,259	9	3.95%	1.8%	7.5%
Seagate	SSDSCKKB240GZR	250	1	133	1	274.44%	0.0%	1012.4%
Seagate	ZA250CM10003	250	1,114	924,856	14	0.55%	0.3%	0.9%
Seagate	ZA500CM10003	500	3	1,125	0	0.00%	0.0%	119.7%
Seagate	ZA2000CM10002	2,000	3	5,538	1	6.59%	0.2%	36.7%
Seagate	ZA250CM10002	250	547	667,680	17	0.93%	0.5%	1.5%
Seagate	ZA500CM10002	500	18	29,739	0	0.00%	0.0%	4.5%
Seagate	ZA500GM10001	500	2	682	0	0.00%	0.0%	197.4%
Seagate	ZA250NM1002	250	80	15,523	0	0.00%	0.0%	8.7%
Seagate	SSD	250	106	151,465	3	0.72%	0.1%	2.1%
WDC	WD Blue SA510 2.5	250	65	3,716	4	39.29%	10.7%	100.6%
WDC	WDS250G2B0A	250	108	38,914	2	1.88%	0.6%	8.2%
		Totals	**3,144**	**2,433,310**	**60**	**0.90%**		

Backblaze

Graphique 5 https://www.backblaze.com/blog/how-reliable-are-ssds/

Les défaillances matérielles sont également moins nombreuses, car l'industrie s'est éloignée des composants interchangeables et de ceux qui nécessitent un refroidissement important. Cette étude réalisée par Backblaze sur 5 ans et plusieurs milliers de disques SSD a montré que le taux de défaillance était inférieur à 1 %.

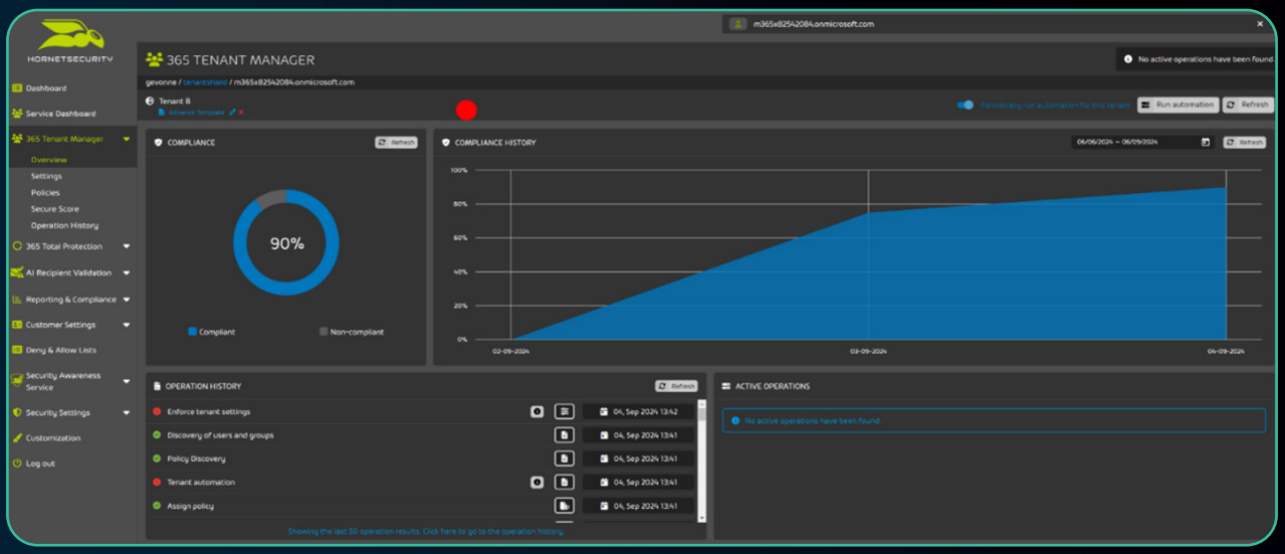
La tendance à l'utilisation d'ordinateurs portables a également contribué à cette évolution. Pendant un certain temps, le cycle de 3 à 4 ans pour le matériel était un objectif, mais aujourd'hui, de nombreux MSP constatent que des machines vont bien au-delà de 4, 5 et même 6 ans.

Qu'est-ce que cela implique pour le volet maintenance ? Cela signifie que vous devez chercher à automatiser autant que possible et à surveiller les exceptions au déploiement réussi. Les activités de maintenance devraient être réduites grâce à l'amélioration de la fiabilité du matériel.

SUIVI AUTOMATISÉ

Si le temps consacré à la maintenance a diminué, celui consacré au suivi a augmenté, même avec l'aide de l'automatisation. Alors que les alertes liées à des problèmes tels que des disques durs pleins ont diminué en raison du stockage en Cloud, les alertes liées au phishing, au vol d'identité et aux activités des applications sont montées en flèche. En effet, le suivi automatisé joue un rôle crucial dans l'identification des menaces potentielles, car il couvre les questions de continuité des activités et de cybersécurité. Les MSP ont besoin d'une solution de surveillance robuste et intelligente pour pouvoir faire face à l'avalanche d'informations découvertes dans les journaux, les changements de paramètres et les indicateurs d'activité des logiciels malveillants. Le programme de surveillance est l'épine dorsale de tout plan de détection des menaces.

Le programme de surveillance automatisé doit être suffisamment intelligent pour comprendre le niveau de gravité d'un seul changement ou de plusieurs changements pris ensemble. La combinaison des outils intégrés de Microsoft, comme Intune pour la surveillance des appareils, Sentinel pour la gestion des alertes et Defender XDR pour le suivi des incidents, permet de fournir une solution de surveillance intelligente qui peut prendre des mesures automatisées tout en cartographiant l'activité et en envoyant des messages d'alerte. Des suites tierces, comme **365 Multi-Tenant Manager de Hornetsecurity** pour les MSP et les plans de protection des entreprises, utilisent plusieurs de leurs produits ainsi que l'intelligence artificielle pour aider les MSP à obtenir des informations et une protection automatisée à partir du programme de surveillance. Quel que soit le produit choisi, il doit s'agir d'une suite complète d'outils qui fonctionnent ensemble pour construire non seulement une solution de surveillance, mais aussi une solution qui peut agir en votre nom lorsque certaines conditions sont réunies.



Graphique 6 Vue d'ensemble des tenants dans le Multi-Tenant Manager

RÉPONSE AUX INCIDENTS ET REPRISE APRÈS SINISTRE

La complexité de la réponse aux incidents et de la reprise après sinistre n'a jamais été aussi grande. Avec l'augmentation des demandes de rançon par les cybercriminels, les compagnies d'assurance et les organismes de réglementation sont de plus en plus impliqués dans le processus de reprise. Cela implique qu'aujourd'hui, la composante technique n'est pas la seule à entrer en ligne de compte, les exigences en matière de conformité et d'assurance doivent également être intégrées dans les plans d'intervention en cas d'incident et de reprise des activités après sinistre.

Alors que de nombreux plans d'assurance cybernétique utilisent des termes généraux tels que « bientôt » ou « rapidement », d'autres prévoient des délais spécifiques tels que 72 heures. La plupart des techniciens MSP souhaitent passer immédiatement en mode de reprise pour que l'activité reprenne le plus rapidement possible, mais les cyber-assurances ont souvent des exigences qui limitent la réponse immédiate à l'endiguement, la première étape du processus étant de les contacter pour que leurs experts puissent aider au rétablissement de l'activité. En outre, les réglementations en matière de conformité peuvent imposer des obligations de déclaration. Comme si cela ne suffisait pas, de nombreuses entreprises ne veulent pas investir autant qu'elles le devraient dans la prévention et la planification de la reprise. Il ne fait aucun doute que les menaces de cybersécurité ont rendu l'activité des MSP beaucoup plus difficile et complexe.

Une petite PME cliente a été victime d'une atteinte à la cybersécurité et s'est empressée de remasteriser les ordinateurs portables des utilisateurs finaux afin de « reprendre rapidement le travail », alors que nous lui avions recommandé de prendre le temps d'établir comment ils étaient entrés et ce qui avait été compromis. Quelques jours plus tard, les attaquants sont revenus à la charge, utilisant à nouveau un ransomware. Ce n'est que lorsque cela s'est produit une troisième fois que le client nous a demandé de faire appel à des experts en Digital Forensics Incident Response (DFIR), et leur enquête a permis de découvrir un rootkit UEFI qui donnait aux attaquants une porte dérobée pratique, même après que les ordinateurs portables ont été réimagés. La seule solution a été d'acheter de nouveaux ordinateurs portables pour tout le monde.

REPRISE APRÈS SINISTRE

Avec tout ce qui se passe, beaucoup ont malheureusement perdu de vue la ligne de base, c'est-à-dire la sauvegarde « en cas d'échec ». C'est comme s'ils avaient oublié la reprise d'activité une fois que les données sont dans le Cloud ! Mais la sauvegarde n'a jamais été une fonction intégrée. Elle a toujours dû être ajoutée par un tiers. La plupart des fournisseurs de cloud computing vantent leurs capacités de sauvegarde, mais celle-ci n'est pas destinée au client ou au MSP, mais à eux. En cas de panne, ils peuvent restaurer le service et vos données. Mais si vous souhaitez bénéficier de l'expérience de sauvegarde qu'exige un plan de reprise après sinistre, vous devez faire appel à une tierce partie.

Hornetsecurity propose une solution de sauvegarde **moderne 365 Total** qui inclut non seulement les données stockées dans Microsoft 365, un composant de surveillance complet, mais aussi la sauvegarde des points d'extrémité.

» **Multi-tenant**
gérez et surveillez toutes les organisations Microsoft 365 et les sauvegardes de points finaux Windows à partir d'une console de gestion en ligne unique et multi-tenant.

» **Tableau de bord de sauvegarde facile à utiliser**
contrôlez de manière centralisée l'activité de sauvegarde et de restauration, l'état de santé des sauvegardes et l'historique des restaurations récentes. Définissez des notifications en cas de réussite, d'échec ou d'avertissement, des alertes par e-mail ou un résumé quotidien.

» **Sauvegardes automatisées de Microsoft 365**
les sauvegardes M365 sont effectuées automatiquement plusieurs fois par jour. Pour les terminaux, les sauvegardes peuvent être exécutées toutes les 1 à 24 heures.

» **Sauvegarde des terminaux sur site et itinérants**
sauvegarde de n'importe quel terminal au bureau ou n'importe où dans le monde sans avoir besoin d'un VPN.

» **Sauvegarde des points d'extrémité et stratégies**
sauvegarde au niveau des fichiers des ordinateurs de bureau et des ordinateurs portables Windows, pilotée par des règles. Configurez les paramètres pour de grands groupes de terminaux Windows en définissant des règles pour définir les répertoires de sauvegarde, le stockage dans le Cloud, la fréquence et la conservation.

» **Sauvegarde à tout moment et en tout lieu**
sauvegardez à tout moment des utilisateurs, des groupes, MS Planner, des bibliothèques de documents SharePoint et des terminaux spécifiques.

» **Processus d'approbation à quatre yeux**
une couche de sécurité supplémentaire qui réduit le risque de perte de données par des administrateurs malhonnêtes et inexpérimentés en exigeant que les actions sensibles telles que la suppression de données, la modification des paramètres de l'entreprise et plus encore nécessitent au moins une approbation d'un administrateur approbateur sélectionné, distinct de l'administrateur initiateur.

Ce type de solution de sauvegarde complète pour assurer la reprise après sinistre est indispensable à l'instar du contexte actuel de la cybercriminalité. La probabilité de devoir restaurer des données a augmenté ces dernières années, parallèlement à la cybercriminalité.

RÉPONSE AUX INCIDENTS

Même si nous aimerions revenir à l'époque où la restauration à partir d'une sauvegarde constituait une réponse à un incident, nous ne pouvons malheureusement pas le faire. La complexité a augmenté à un tel point que les MSP ont besoin d'un processus défini pour la réponse aux incidents. Voici une liste des 6 domaines qui constituent la réponse aux incidents aujourd'hui. Notez que la restauration se classe en numéro 5 de cette liste descendante.

1. **Confinement :** la première étape consiste à contenir l'incident afin d'éviter d'autres dommages. Il peut s'agir d'isoler les systèmes affectés, de désactiver les comptes compromis et d'arrêter les processus malveillants. Votre application de surveillance devrait vous avoir alerté de la menace, tandis que la solution de cybersécurité que vous avez choisie devrait avoir commencé à interrompre la chaîne d'attaque.

2. **Notification:** ensuite, nous devons notifier les organismes de réglementation qui doivent l'être. Pour les petites entreprises, il s'agira probablement de la compagnie d'assurance cybernétique, tandis que pour les organismes réglementés et publics, ce sera le service juridique. Ils devront être informés de l'incident et feront probablement intervenir leurs experts dans le processus de rétablissement.

3. **Enquête :** c'est probablement à ce stade que les experts font leur intervention pour mener une enquête approfondie afin de déterminer la cause et l'étendue de la violation. Cela implique l'analyse des journaux, l'identification des systèmes compromis et la collecte de preuves. Le prestataire de services de gestion peut se retrouver à enfiler une casquette de conseiller, en fournissant des informations à l'équipe de récupération, et devra probablement jouer un rôle de communication. En tant que conseiller de confiance, le MSP connaît la personnalité des dirigeants et des fonctions de l'entreprise. Il se trouve donc dans une position clé pour combler les lacunes en matière de communication et définir les attentes.

4. **Remédiation :** le MSP peut alors être appelé à s'attaquer à la cause première de l'incident, par exemple en supprimant les logiciels malveillants, en corrigeant les vulnérabilités et en réinitialisant les mots de passe.

5. **Récupération :** si le réseau a été endommagé ou si la sécurité d'une zone ne peut être garantie, le MSP devra restaurer les systèmes et les données concernés à partir de sauvegardes et s'assurer que tous les systèmes sont pleinement opérationnels.

6. **Examen après l'incident :** en fin de compte, le MSP et tout autre acteur impliqué dans l'enquête rédigent un rapport et procèdent à un examen post-incident afin d'identifier les enseignements tirés et d'améliorer le plan d'intervention en cas d'incidents ultérieurs.

Il est probable que l'entreprise et le MSP tireront de nombreux enseignements qui amélioreront à jamais la sécurité du réseau de l'entreprise. Le client est confronté à quelque chose qu'il ne comprend pas sur le plan technique, une interruption d'activité, et il se tournera vers le MSP non seulement pour le rétablissement technique décrit ci-dessus, mais aussi pour être rassuré et se faire expliquer les mesures prises à chaque étape. Il s'agit d'une période très stressante pour eux et pour vous. Une communication optimale contribuera grandement à surmonter l'inadéquation des attentes qui est souvent à l'origine de toute insatisfaction éventuelle.

Si le MSP exécute bien le plan de reprise après sinistre, la relation avec le client devrait être plus forte que jamais.

ÉQUILIBRER L'EFFICACITÉ ET L'EXPERTISE HUMAINE

Toutes ces activités prennent du temps, mais heureusement, l'apprentissage automatique et l'IA sont venus à la rescousse. En souscrivant à un ensemble de solutions modernes qui incluent l'automatisation et l'IA pour retirer une partie des compétences et du temps au personnel du service d'assistance du MSP, ce dernier devrait être en mesure de gérer un scénario de reprise après sinistre parallèlement à ses activités habituelles de provisionnement, de surveillance et d'alerte. Trouver le bon équilibre entre l'efficacité et l'expertise humaine est la clé d'une surveillance et d'une maintenance réussies.

De nombreux MSP ont tendance à embaucher des employés peu qualifiés. Dans le même temps, les développeurs se sont attachés à réduire la charge de travail du personnel moins qualifié. Comme les outils utilisés par les MSP pour leurs opérations quotidiennes sont conçus pour réduire le travail des personnes peu qualifiées, le MSP doit embaucher du personnel plus qualifié, capable de gérer la continuité des activités et la reprise après sinistre. Ce personnel doit comprendre la motivation des entreprises, les communications, la cybersécurité et la reprise après sinistre. Le personnel moins qualifié sera toujours nécessaire, mais il sera davantage axé sur les outils et le service à la clientèle.

Plus important encore, le personnel peu qualifié est celui auquel vos clients s'adressent le plus souvent. Ce sont eux qui répondent au téléphone, assurent le triage et fournissent une assistance de premier plan. Prêtez attention à vos points de contact, car l'évaluation du service client d'un MSP repose en grande partie sur la sensation qu'il procure au client dans les moments de stress.

RÉSUMÉ

> Dans ce chapitre, nous avons exploré les aspects critiques de l'efficacité des MSP dans les activités de surveillance et de maintenance. Nous avons abordé l'importance de la maintenance proactive, le rôle de la surveillance automatisée, l'importance de la procédure de réponse aux incidents et de la planification de la reprise après sinistre, ainsi que la nécessité de trouver un équilibre entre l'efficacité et l'expertise humaine. En mettant en œuvre des procédures et des plans efficaces, les MSP peuvent améliorer leurs performances, réduire le stress et atteindre une plus grande rentabilité.

HORNETSECURITY

CHAPITRE 4

PERSONNALISATION

La personnalisation est un sujet délicat. Si, en tant que MSP, nous sommes tenus de normaliser, nous devons reconnaître que chaque client est unique et éviter la tentation de déployer des solutions à l'emporte-pièce que n'importe quel concurrent pourrait reproduire. Nous avons besoin de personnalisation pour nous définir sur le marché.

La motivation de la personnalisation est complexe, mais notre objectif ici est de personnaliser efficacement et là où l'impact est important. Dans ce chapitre, nous allons tracer une ligne de démarcation entre la personnalisation et le déploiement personnalisé et réfléchir au moment et à la raison d'effectuer chacune de ces opérations.

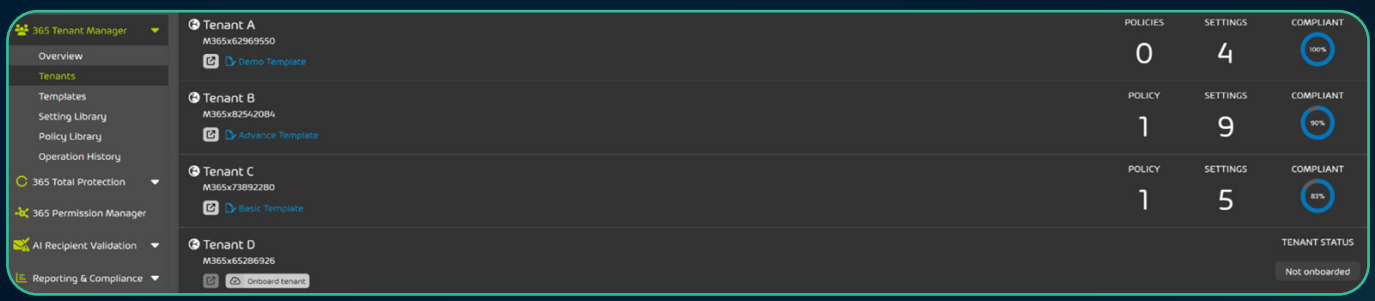
QU'EST-CE QUE LA PERSONNALISATION ?

Cette question peut sembler ridicule, mais elle occupe une place de premier plan. Qu'est-ce qu'un déploiement personnalisé et qu'est-ce qu'une personnalisation ? Il est important de les différencier afin de ne pas perdre notre objectif d'efficacité.

UNE SOLUTION POUR DÉPLOYER UNE CONFIGURATION PERSONNALISÉE

Grâce à l'outil **365 Multi-Tenant Manager** pour les MSPs de Hornetsecurity, nous pouvons rapidement créer une configuration personnalisée sur la base de nos procédures opérationnelles standard (POS). Cet outil nous permet de déployer la configuration d'un tenant entier en quelques instants, en veillant à ce que notre conception soit immédiatement envoyée à tous les tenant que nous prenons en charge. Chaque fournisseur de services gérés devrait avoir un déploiement personnalisé qui reflète ses normes tout en tenant compte des lignes de base recommandées.

Voici un exemple de ce à quoi cela pourrait ressembler. Chaque client de la liste ci-dessous se voit attribuer un modèle qui représente notre configuration standard pour un client comme lui.

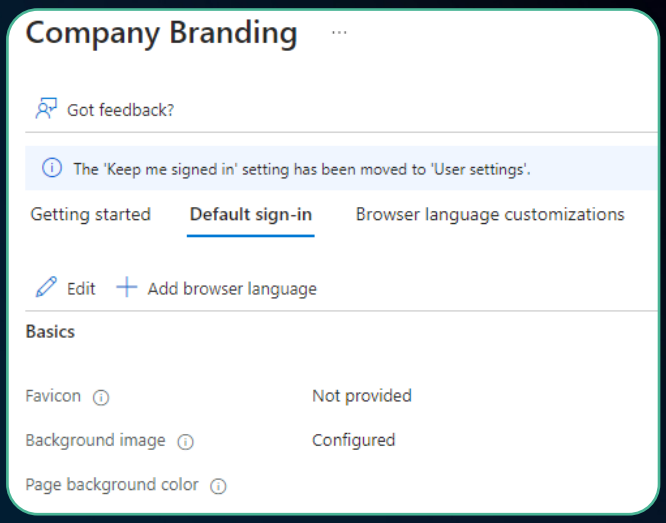


Graphique 7 Hornetsecurity Multi-Tenant Manager

En utilisant des modèles, nous pouvons maintenir notre solution personnalisée en regroupant les clients dans le modèle approprié et lorsque nous apportons des modifications au modèle, les clients de ce modèle sont automatiquement mis à jour. C'est la méthode utilisée pour déployer efficacement une configuration personnalisée.

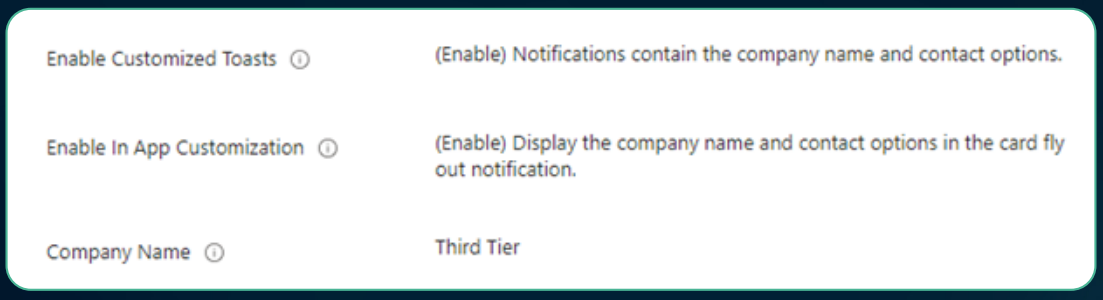
DÉPLOYER UNE PERSONNALISATION EFFICACEMENT

Mais vous devez également procéder à la personnalisation. Certains domaines de chaque environnement Microsoft 365 permettent une personnalisation qui aide à faire savoir au client qu'il opère dans son propre réseau, dans le respect des règles de conformité et de réglementation, et qu'il travaille en toute sécurité. Ce n'est pas tout à fait différent de ce qui se passe lorsque vous installez un serveur Microsoft et que vous y appliquez vos paramètres. C'est le déploiement personnalisé de ce serveur et la présence physique de la boîte qui ont permis au client de savoir qu'il en était propriétaire. Aujourd'hui, la présence physique est remplacée par la personnalisation.



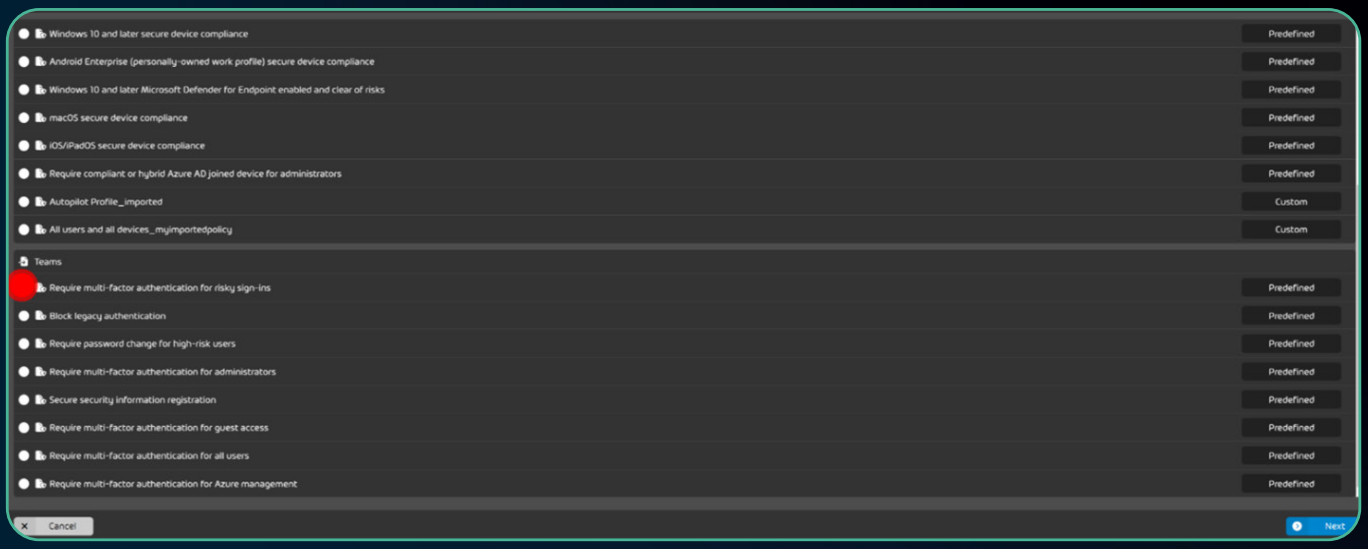
Graphique 8 Personnaliser avec l'image d'arrière-plan de l'authentification approuvée par l'entreprise

Nous ne disposons plus de ce serveur physique, mais avec un déploiement de Microsoft 365, la personnalisation peut comprendre des éléments tels que le logo de l'entreprise, le nom de l'entreprise, le nom et les coordonnées du support MSP, et la photo d'arrière-plan sur l'écran de connexion. Ces éléments aident les utilisateurs professionnels à comprendre qu'ils opèrent dans leur réseau d'entreprise. Pour le MSP, cela permet également de se différencier de ceux qui ne prennent pas le temps d'effectuer ces personnalisations.



Graphique 9 Personnaliser les pop-ups de notification avec le nom de l'entreprise et les informations de contact

La personnalisation peut également s'accompagner d'une certaine normalisation qui conviendra à un groupe de clients tenants. Vous avez peut-être un certain nombre de clients qui acceptent les paiements par carte de crédit et stockent ces données. Dans ce cas, ils auront tous besoin de votre politique de conformité PCI. La solution **365 Multi-Tenant Manager pour les MSPs** de Hornetsecurity vous permet d'appliquer cette politique au tenant approprié, selon les besoins. Comme indiqué ci-dessus, lorsque nous créons un modèle pour chaque type d'entreprise, nous faisons de même pour la conformité et les réglementations dont nos clients ont besoin et nous appliquons notre modèle de paramètres.



Graphique 10 Modèles de paramètres de Multi tenant Manager

GESTION DU TEMPS

La gestion du temps est la clé de l'efficacité des MSP. Pour rester efficace, nous devons

- Configurer le déploiement initial avec le nom de domaine et les entrées DNS
- Déployer notre configuration personnalisée de tenants
- Déployer les configurations de conformité et de réglementation aux bons tenants
- Configurer la personnalisation spécifique de l'entreprise et les expériences des utilisateurs

Le temps consacré à chaque tâche est important. Un MSP efficace devrait consacrer 10 % ou moins de son temps au déploiement des environnements et 90 % à la personnalisation, y compris aux exigences réglementaires et de conformité. Pourquoi une telle répartition ? Parce que le déploiement personnalisé concerne le MSP, tandis que la personnalisation sied au client. Un MSP devrait toujours s'efforcer de passer la majorité de son temps à travailler au profit du client.

N'oubliez pas que la réalité de vos clients est souvent très différente de la vôtre. Ils ne comprennent pas les détails technologiques comme vous le faites, et j'en ai eu un exemple classique dans mon entreprise à plusieurs reprises. Je passe trop de temps à identifier la solution la plus rentable pour répondre à un besoin professionnel, alors que je sais qu'une solution plus complète serait meilleure à long terme, même si elle est plus coûteuse. Lorsque j'ai fait le point avec le client, il m'a répondu sans ambages : « Je ne vous ai pas demandé de me faire économiser de l'argent, j'ai demandé la meilleure solution ». Vérifiez toujours vos hypothèses avant de poursuivre.

GESTION DU CHANGEMENT

La dernière chose que nous devons maîtriser dans notre tâche de personnalisation est la gestion des changements. Les outils devraient vous aider à suivre l'historique des modifications, mais ce sont vos procédures opérationnelles standards qui documentent les raisons de ces modifications. Presque toutes les modifications que vous apportez doivent s'appliquer à un groupe existant de clients qui ont déjà un modèle en commun. Assurez-vous simplement que vous n'appliquez pas moins de paramètres pour répondre aux besoins d'un seul client assigné au modèle. Une bonne règle à suivre est de ne jamais créer une politique basée sur l'exception. Si une exception est nécessaire pour un seul client, elle doit figurer dans son propre modèle. Cependant, un MSP efficace ne le fera presque jamais, mais s'efforcera plutôt d'amener tous les clients à une norme plus élevée.

RÉSUMÉ

En conclusion, la maîtrise du déploiement personnalisé, de la personnalisation ainsi que la gestion du changement est essentielle pour permettre aux MSP de laisser une meilleure empreinte sur le marché et d'apporter de la valeur à leurs clients. En déployant efficacement des configurations personnalisées et en maintenant des modèles standardisés, les MSP peuvent s'assurer que les besoins uniques de leurs clients sont satisfaits tout en maintenant l'efficacité opérationnelle. Une gestion efficace du temps, en privilégiant la personnalisation par rapport au déploiement, permet aux MSP de consacrer la majeure partie de leur temps à des tâches centrées sur le client, ce qui se traduit en fin de compte par une plus grande satisfaction du client et une proposition de valeur plus forte lorsque vous allez sur le marché.

HORNETSECURITY

CHAPITRE 5

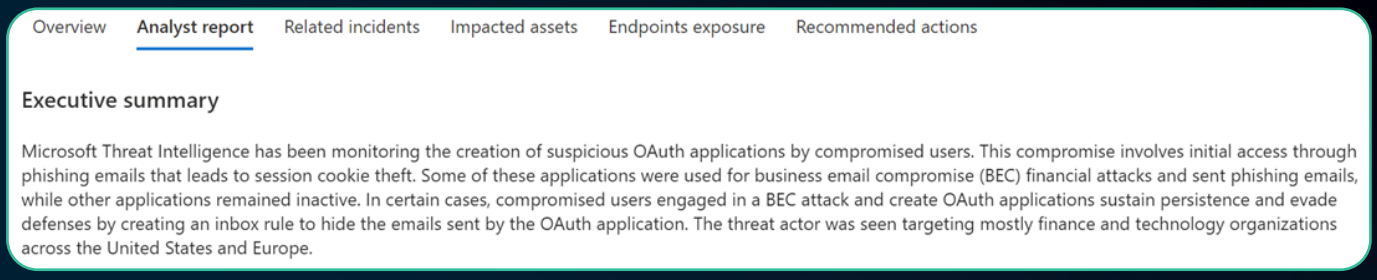
CYBERSÉCURITÉ

Il n'y a pas de sujet plus important aujourd'hui pour les MSP et leurs clients que la cybersécurité. La cybersécurité pourrait faire l'objet d'un ebook à part entière. De nombreux paramètres et une maintenance permanente sont nécessaires pour garder une longueur d'avance sur les cybercriminels et protéger les clients. Dans ce chapitre, nous nous intéresserons moins aux paramètres spécifiques qu'au maintien de notre efficacité et donc de notre rentabilité face à l'évolution rapide du paysage de la cybersécurité.

Lorsque nous réfléchissons à la manière de protéger les réseaux dont nous sommes responsables, nous devons utiliser l'ensemble de la boîte à outils.

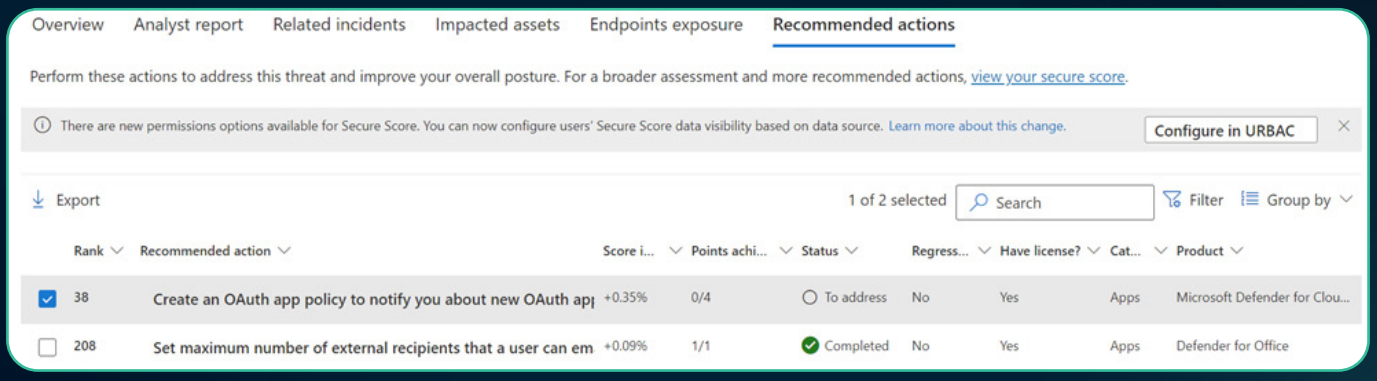
COMPRENDRE LES VULNÉRABILITÉS

Microsoft fournit des rapports d'analyse dans la zone d'analyse des menaces de Defender, offrant une panoplie d'informations produites par ses analystes de traitement sur le fonctionnement de menaces spécifiques. Ces rapports sont détaillés mais faciles à lire, commençant par un résumé et s'étendant sur le fonctionnement de la menace.



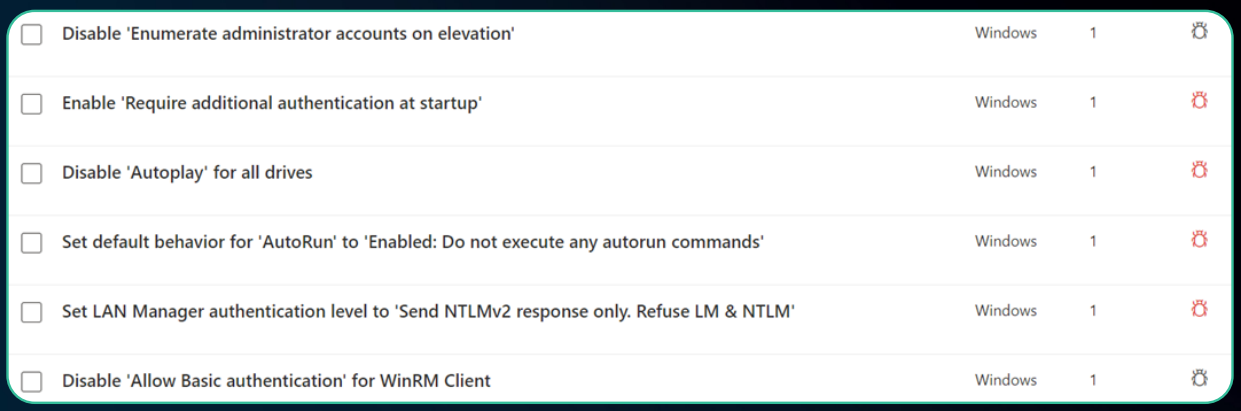
Graphique 11 Résumé exécutif débutant le rapport détaillé sur les menaces

Au fil des onglets, vous trouverez des informations supplémentaires sur l'impact de cette situation sur votre tenant et sur les mesures que vous pouvez prendre pour protéger votre réseau. En cliquant sur chaque tâche non terminée, vous accédez aux instructions de déploiement de la protection.



Graphique 12 Liste des mesures à prendre pour protéger votre réseau contre ce criminel

Le portail Microsoft Defender répertorie également les vulnérabilités qui ne sont pas liées à des menaces spécifiques. Ces vulnérabilités sont nombreuses. Nombre d'entre elles sont théoriquement possibles mais ne sont pas activement exploitées. Dans la liste des recommandations de sécurité (figure 3), les insectes rouges indiquent des exploits actifs, tandis que les gris indiquent des vulnérabilités potentielles. Ces exploits actifs n'ont peut-être pas encore ciblé votre réseau, mais ils sont utilisés contre d'autres personnes



Graphique 13 Recommandations de sécurité par exploit actif

En utilisant ces deux outils, le MSP efficace peut cibler ses activités de maintenance de la cybersécurité sur les vulnérabilités les plus susceptibles de constituer une menace pour ses clients.

Si l'on considère le nombre de vulnérabilités cybernétiques existantes et le nombre de criminels qui découvrent de nouveaux moyens de pénétrer dans les réseaux, on pourrait croire qu'il s'agit d'un de ces vastes problèmes que l'on aborde en haussant les épaules et en se disant que l'on n'y peut pas grand-chose. En d'autres termes, vous ne pourrez jamais faire face à la cybersécurité. Mais en utilisant les deux outils décrits ci-dessus, nous pouvons faire bouillir de l'eau pour une tasse de thé et nous atteler à la tâche de sécuriser les réseaux de nos clients.

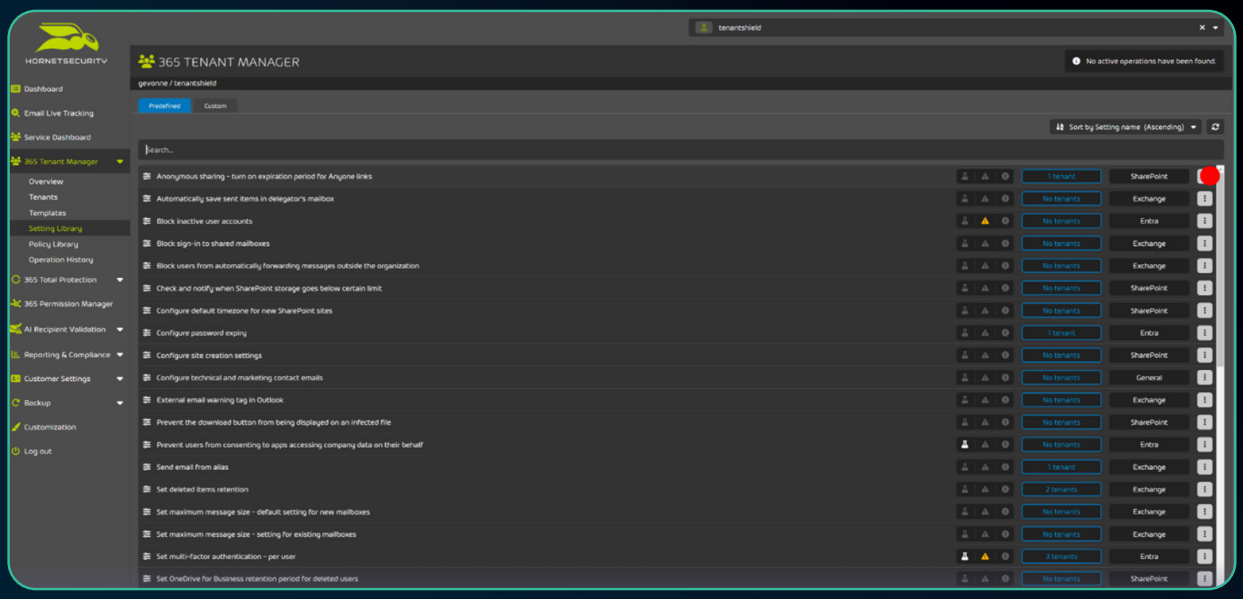
BASES DE RÉFÉRENCE

Les bases de référence sont un autre outil dont nous disposons pour nous aider à améliorer l'efficacité de la cybersécurité. Microsoft fournit des lignes de base de sécurité pour Windows, Edge, Windows 365, Defender for Endpoints et les applications Microsoft 365.

Graphique 14 Security baselines

Vous pouvez utiliser ces bases de référence, mais elles sont très strictes et peuvent représenter un défi pour de nombreuses entreprises. Nous vous suggérons plutôt d'évaluer les paramètres de la base de référence et de créer les vôtres. Une fois cette étape franchie, vous disposerez d'une norme que vous pourrez déployer sur l'ensemble des environnements.

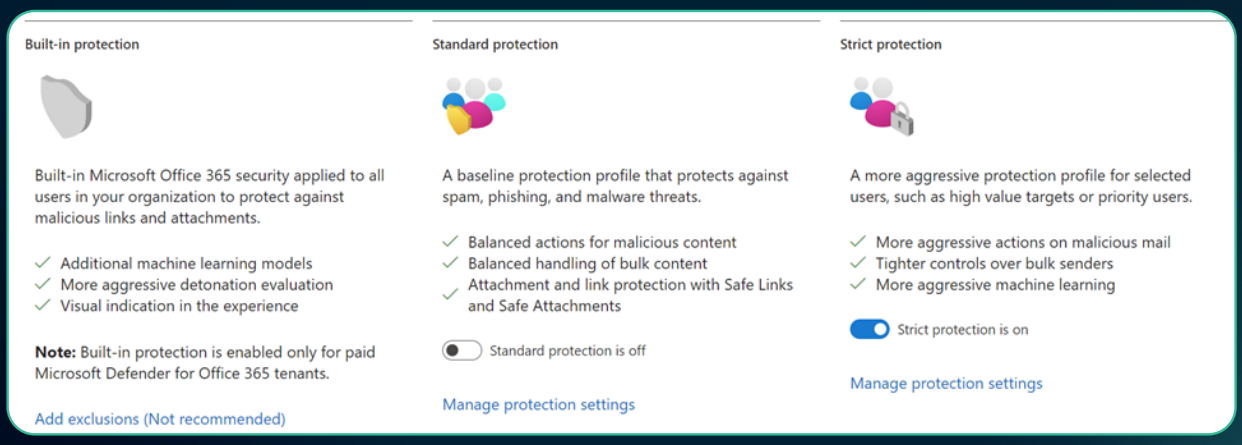
Pour ce faire, vous aurez besoin d'un outil tiers tel que **365 Multi-Tenant Manager pour les MSPs** de Hornetsecurity pour pouvoir affecter vos normes aux réseaux dont vous êtes responsable. La fonction de création de modèles est très utile à cet égard.



Graphique 15 Bibliothèque de paramètres du Multi-Tenant Manager de Hornetsecurity

SÉCURITÉ DE LA MESSAGERIE

Il est surprenant de constater qu'il n'existe pas de référence en matière de sécurité de la messagerie. Avec la montée en flèche de la compromission des courriels d'entreprise (BEC) en tant que vecteur d'infiltration des réseaux, on pourrait penser qu'il y en a une. Au lieu de cela, Microsoft s'est attaqué à ce problème avec des modèles prédéfinis de politique de sécurité du courrier électronique au sein même de Defender for Business.

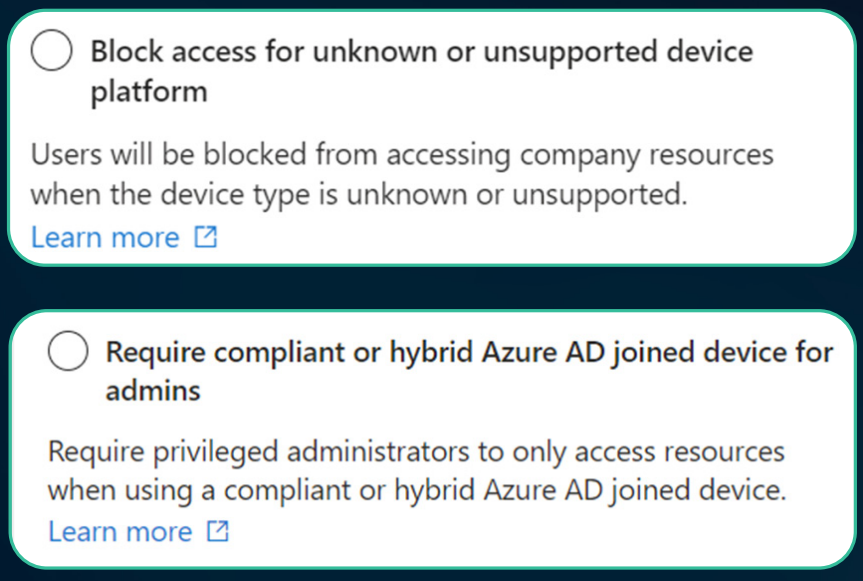


Graphique 16 Politiques de sécurité prédéfinies pour les emails

Il n'y a sans doute pas de mesure de cybersécurité plus importante à prendre qu'une solution complète pour le courrier électronique. Les criminels ont recours à l'hameçonnage, au spear phishing et à l'hameçonnage par QR code, ainsi qu'à d'autres moyens d'ingénierie sociale, pour faire le premier pas dans un réseau. Les entreprises doivent aujourd'hui gérer le courrier électronique avec une extrême prudence. La capacité d'usurper l'identité d'un utilisateur, de rédiger un contenu de qualité et convaincant et de faire passer des URL frauduleux pour des URL légitimes a atteint son apogée. La seule façon de lutter contre ce phénomène est de mettre en place un programme complet de sécurité du courrier électronique et de faire preuve d'une certaine tolérance à l'égard des faux positifs. L'utilisation des modèles fournis par Microsoft en combinaison avec la **365 Total Protection de Hornetsecurity** est le moyen d'y parvenir.

INTUNE ET LES POLITIQUES D'ACCÈS CONDITIONNEL

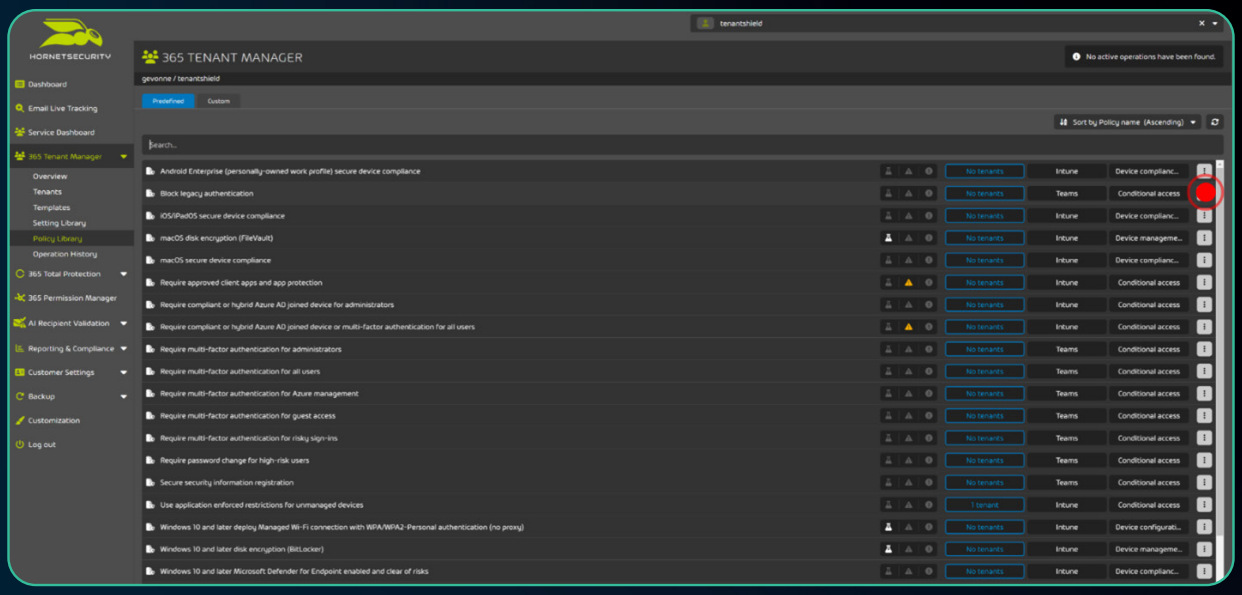
Intune, comme nous l'avons vu plus haut dans cet eBook, est un excellent outil de configuration. Il pousse vos configurations et applications vers les appareils de votre réseau, fournissant un contrôle fin sur les appareils connectés, ce qui est en soi une mesure de cybersécurité. Avec l'ajout des règles d'accès conditionnel d'Entra, nous pouvons limiter l'utilisation du réseau aux appareils qui y sont reliés ! Pouvez-vous imaginer un monde où les criminels décident de rejoindre votre domaine en utilisant l'ordinateur portable à partir duquel ils travaillent ? Nous pouvons exiger que cette situation survienne à l'aide d'une politique d'accès conditionnel, qui stipule que dès qu'ils obtiennent le contrôle de l'administration, ils doivent soit rejoindre le domaine, soit être bloqués. Vont-ils vraiment rejoindre votre domaine ? Une autre politique efficace limite l'accès aux plates-formes prises en charge. Par exemple, si vous n'utilisez pas Linux, Mac ou même d'anciennes versions de Windows OS dans votre réseau, bloquez-les. Nous voulons rendre la tâche des criminels aussi difficile que possible.



Graphique 17 Microsoft Entra conditional access rules

Les licences avancées de Microsoft 365 comprennent également des fonctions telles que les mesures « Risky User », « Risky sign-in » et « Risky Device » que vous pouvez également ajouter à vos politiques. Ces mesures peuvent être ajoutées à vos politiques afin de n'autoriser que les utilisateurs et les appareils sûrs et connus à utiliser le réseau.

La gestion des politiques d'accès conditionnel (CA) à travers tous les tenants du client est vitale, mais le faire manuellement prend du temps, et une fois de plus, le 365 Multi-Tenant Manager pour les MSPs de Hornetsecurity vous aide en gérant la personnalisation et le déploiement des politiques de CA à l'échelle.

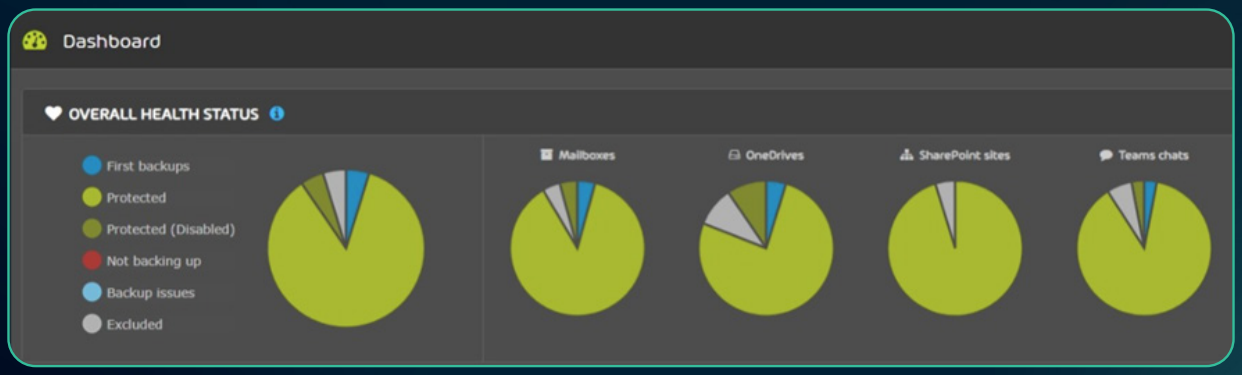


Graphique 18 Bibliothèque de politiques d'accès conditionnel dans Multi-Tenant Manager

AUTOPILOT, LIGHTHOUSE ET BACKUP

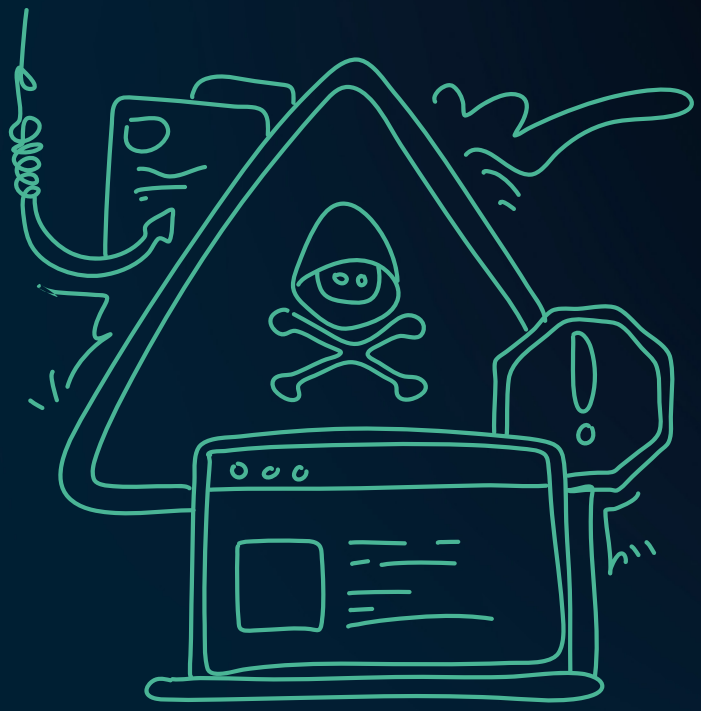
Outre les outils qui vous permettent de découvrir et de définir des configurations de sécurité, vous devez également penser à Autopilot, Lighthouse et à une solution de sauvegarde dans le cadre de votre stratégie de cybersécurité. Autopilot pour identifier avec certitude les appareils qui appartiennent à votre domaine et vous donner le contrôle de l'appareil dès sa sortie de l'emballage. Lighthouse pour gérer certains paramètres entre les clients, si vous n'utilisez pas un tiers pour cette fonction. Faites une sauvegarde pour assurer la continuité de l'activité, si tout le reste échoue.

Comme nous l'avons vu plus haut, c'est cet aspect de la continuité des activités qui semble avoir disparu de l'offre de nombreux MSP. Un tableau de bord facile à lire qui affiche l'état des sauvegardes pour tous vos tenants est un moyen efficace de surveiller l'état des sauvegardes.



Graphique 19 Tableau de bord de l'état des sauvegardes de Hornetsecurity Total Backup

Pour compléter le processus de continuité des activités, le MSP effectuera des tests de restauration au moins une fois par trimestre afin de déterminer si la sauvegarde peut être restaurée. La sauvegarde n'a pas d'importance si elle ne peut pas être restaurée avec succès. C'est un peu fou, mais il y a quelques truismes dans l'informatique. Les imprimantes et les sauvegardes échouent toujours. C'est une mauvaise idée de se désintéresser de l'un ou de l'autre.



La clé de la gestion de la cybersécurité pour vos clients est la visibilité. Avec un système adapté (tel que Microsoft Sentinel, que j'utilise avec tous mes clients), je sais en quelques minutes si quelqu'un a créé une nouvelle politique d'accès conditionnel, ou ajouté une nouvelle méthode MFA à son compte, ou a été victime d'une attaque de fatigue MFA (tellement d'invités que l'utilisateur final finit par accepter l'invite pour qu'elle s'arrête). Cette visibilité en temps quasi réel m'a permis de contenir de petits incidents avant qu'ils ne se transforment en brèches plus importantes.

RÉSUMÉ

Pour conclure ce chapitre sur la cybersécurité, il est essentiel de reconnaître que le paysage des cybermenaces est en constante évolution. Les professionnels de l'informatique des petites entreprises doivent faire preuve de vigilance et de proactivité dans leur approche de la cybersécurité. En exploitant les outils et les stratégies présentés dans ce chapitre, les professionnels de l'informatique peuvent protéger efficacement les réseaux et les données de leurs clients tout en restant efficaces et rentables. N'oubliez pas que la cybersécurité n'est pas un effort ponctuel, mais un processus permanent qui nécessite un apprentissage et une adaptation continus. Restez informé, préparez-vous et restez en sécurité.

HORNETSECURITY

CHAPITRE 6

GESTION DES FOURNISSEURS

Il y a plusieurs façons de décider comment gérer les fournisseurs dans votre MSP. Faut-il rechercher plusieurs fournisseurs de premier ordre ou choisir un seul fournisseur ? À première vue, le choix semble facile : il suffit de choisir entre un seul ou plusieurs fournisseurs. Mais ce n'est pas si simple. Si l'on garde à l'esprit que notre objectif est l'efficacité, de nombreux facteurs doivent être pris en considération. Nous devons trouver un équilibre entre l'efficacité et la fourniture d'une excellente solution à nos clients. Lorsque nous sommes confrontés à une décision complexe, il est préférable d'utiliser un processus de prise de décision tel qu'un tableau comparatif ou un SWOT. Dans ce chapitre, nous étudierons ces deux types de processus.

L'APPROCHE DE LA TABLE DE DÉCISION

Il y a de nombreuses années, avant que la cybersécurité ne devienne si complexe et que nos besoins en matière de défense ne soient si vastes, j'étais partisan du « meilleur de sa catégorie». À l'époque, ce choix signifiait que j'avais deux fournisseurs à gérer. Mais j'ai changé d'avis lorsque le paysage de la cybersécurité a évolué en raison du nombre de fournisseurs qui devraient être impliqués dans un ensemble de solutions «meilleures dans leur catégorie » aujourd'hui et des différences relativement mineures entre les solutions au fur et à mesure que les fournisseurs dans ce domaine sont arrivés à maturité.

FACTEUR	APPROCHE PAR FOURNISSEUR	APPROCHE „MEILLEUR DE SA CATÉGORIE"
Gestion de la compléxité	Simplifié	Complexe
Coût	Économies ?	Coûts plus élevés
Intégration	Sans faille	Défi
L'innovation	Limitée ?	Élevée
Immobilisation des fournisseurs	Élevé	Faible ?

Graphique 20 L'approche de la table de décision

Cette décision n'a pas été simple à prendre, car elle était synonyme de compromis. Les facteurs à prendre en compte étaient la complexité de la gestion, le coût, l'intégration, l'innovation et, de plus en plus, l'immobilisation des fournisseurs.

Avec l'approche « meilleur de sa catégorie », la complexité est toujours plus grande. Nous aurons plusieurs portails de gestion à consulter, plusieurs fournisseurs à payer, ce qui augmente les frais généraux de notre MSP, l'intégration est au mieux difficile et généralement impossible, et nous nous retrouvons de plus en plus souvent enfermés dans des contrats longs ou difficiles. En tant que MSP, il n'est jamais facile de changer de fournisseur, mais récemment, les fournisseurs ont rendu les choses encore plus difficiles avec des clauses contractuelles onéreuses.

Outre ces considérations importantes, nous devons également nous interroger sur l'espace entre les produits que nous avons choisis auprès de différents fournisseurs et sur les limites de cet espace. Le plus souvent, nous ne savons pas exactement où un fournisseur a choisi de mettre fin à son influence et où un autre l'a commencée. Il se peut que nous laissions involontairement un vide lorsque nous faisons appel à un trop grand nombre de fournisseurs.

L'APPROCHE SWOT

L'approche SWOT est une simple analyse des forces, des faiblesses, des opportunités et des menaces. C'est un outil utile pour de nombreuses tâches décisionnelles. L'utilisation de SWOT peut nous aider à visualiser les deux approches de la gestion des fournisseurs de cybersécurité.

SWOT D'UN FOURNISSEUR UNIQUE

- **Points forts :** gestion simplifiée, complexité réduite, expérience utilisateur cohérente, économies potentielles.
- **Faiblesses :** taille unique, verrouillage des fournisseurs, innovation limitée.
- **Opportunités :** rationalisation des opérations, assistance plus facile.
- **Menaces :** dépendance à l'égard d'un seul fournisseur, lacunes potentielles en matière de sécurité.

L'ANALYSE DES FORCES ET FAIBLESSES DE LA CONCURRENCE (SWOT)

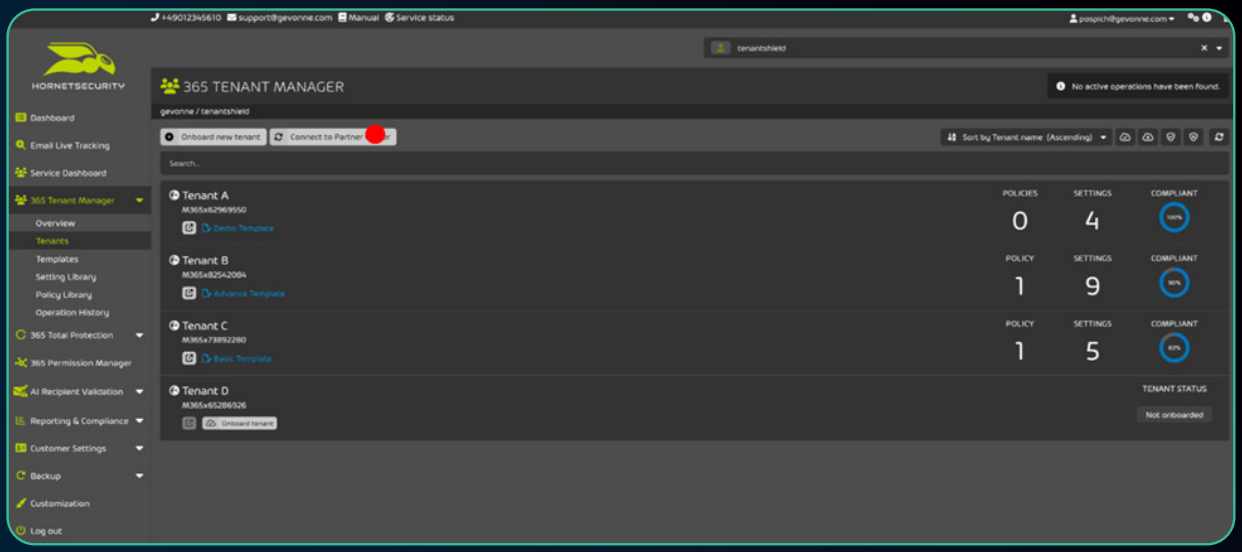
- **Points forts :** expertise spécialisée, flexibilité, réduction de la dépendance à l'égard d'un fournisseur.
- **Faiblesses :** gestion complexe, coûts plus élevés, difficultés d'intégration.
- **Opportunités :** accès aux technologies de pointe, solutions sur mesure.
- **Menaces :** complexité accrue, écarts inconnus entre les fournisseurs.

Un examen de la littérature sur l'utilisation des fournisseurs de MSP a révélé que jusqu'à 70 fournisseurs étaient en jeu pour les plus grands MSP et environ 7 pour le MSP moyen. Mais elle a également montré une tendance à la consolidation des fournisseurs. Cette tendance est probablement due en partie à la tendance générale à la consolidation sur le marché des fournisseurs en général, mais elle est aussi due en partie à une tendance à l'efficacité opérationnelle après avoir reconnu qu'en tant que MSP, vous ne pouvez tout simplement pas gérer de nombreux fournisseurs ni former votre personnel à un si grand nombre de solutions. La complexité croissante de la cybersécurité nous oblige à consolider nos efforts et à faire un choix.

Même si nous ne nous contenterons jamais d'un seul fournisseur, il peut être judicieux d'en adopter deux comme standard. Microsoft est l'un d'entre eux. Microsoft a de plus en plus investi dans la sécurité et a intégré ses produits de sécurité dans les suites Microsoft 365. Il est donc logique de les utiliser. Cependant, leur approche d'entreprise signifie qu'une grande partie est conçue pour des équipes de sécurité avec des spécialisations segmentées. Le MSP typique est de petite taille et est composé de généralistes de la sécurité qui doivent être familiarisés avec l'ensemble des aspects de la cybersécurité. Ce n'est pas le point fort de Microsoft. Un deuxième fournisseur est justifié pour combler ces lacunes. N'oubliez pas cependant qu'il est important de choisir une **suite d'outils de sécurité qui soit intégrée,** afin de minimiser les défis posés par des outils séparés.

GESTION MULTI-ENVIRONNEMENTS AVEC PLUSIEURS FOURNISSEURS

Un fournisseur comme Hornetsecurity peut aider à combler les lacunes de Microsoft. Par exemple, Microsoft ne propose pas de solution de sauvegarde complète pour Microsoft 365. Il y a de moins en moins de lacunes à combler pour les fournisseurs, mais l'une d'entre elles restera toujours la gestion multi-tenant.



Graphique 21 Intégration des locataires dans le Multi-Tenant Manager de Hornetsecurity

Bien que Microsoft ait récemment commencé à ajouter la gestion multi-tenant à certains de ses produits, comme Defender XDR, elle a imposé des limites qui semblent arbitraires jusqu'à ce que l'on prenne en compte son point de vue. N'oubliant pas que Microsoft conçoit des solutions pour les entreprises, la société a limité à 50 le nombre d'environnements sur le portail multi-tenants de Defender. Cela peut sembler logique si vous êtes une entreprise avec plusieurs tenants dans votre société. Nombre d'entre elles en ont pour différentes lignes d'activité ou à la suite d'acquisitions. Mais pour un MSP, 50 tenants, ce n'est pas beaucoup. Certains de nos clients ont également plusieurs tenants qu'ils ont acquis par le biais d'une acquisition. Dans mon MSP de 7 personnes, nous nous occupons de 80 clients, ce qui dépasse déjà la limite de 50 tenants qu'offre la solution multi-tenants de Defenders. Ainsi, bien que nous préférions utiliser Defender XDR comme solution de sécurité, nous avons besoin d'un autre système de gestion, car la recommandation de Microsoft de donner la priorité à certains clients plutôt qu'à d'autres est inacceptable. Dans un souci d'efficacité et pour apporter des niveaux de service égaux aux tenants gérés, nous avons besoin d'une autre solution comme **365 Multi-Tenant Manager pour les MSPs de Hornetsecurity.**

AUTRES CONSIDÉRATIONS

La simplification de la gestion des fournisseurs permet au MSP de se concentrer sur la fourniture de services de plus haut niveau, tels que les missions virtuelles du directeur des systèmes d'information (CIO) ou du directeur de la sécurité des systèmes d'information (CISO). Ce changement permet aux MSP de fournir des conseils stratégiques, d'aligner les initiatives de cybersécurité sur les objectifs de l'entreprise et d'obtenir un avantage concurrentiel. Les clients apprécient davantage les services visibles, et les résultats tangibles tels que l'amélioration de la posture de sécurité, de la conformité et des réglementations, et la réduction des risques conduisent à une plus grande satisfaction et à une plus grande fidélité de la part des clients. Monter dans l'échelle du professionnalisme en matière de cybersécurité signifie des profits plus élevés, des flux de revenus plus importants et des engagements plus précieux avec les clients. En se concentrant sur les services stratégiques, les MSP peuvent atteindre une croissance commerciale durable et capitaliser sur les tendances de l'industrie qui exigent des services de plus haut niveau.

RÉSUMÉ

En conclusion, la gestion des fournisseurs dans un environnement MSP exige un équilibre délicat entre l'efficacité et la fourniture de solutions de haute qualité aux clients. La décision entre un fournisseur unique et une approche « best-of-breed » n'est pas simple et implique la prise en compte de facteurs tels que la complexité de la gestion, le coût, l'intégration, l'innovation et l'immobilisation des fournisseurs. Si l'approche d'un fournisseur unique offre une gestion simplifiée et des économies potentielles, elle peut conduire à un verrouillage des fournisseurs et à une innovation limitée. D'autre part, une approche « meilleur de sa catégorie » offre une expertise spécialisée et de la flexibilité, mais s'accompagne d'une complexité de gestion et de coûts plus élevés. En fin de compte, le choix dépend des besoins et des objectifs spécifiques du MSP, et un processus de prise de décision réfléchi, tel que l'utilisation d'une table de décision ou d'une analyse SWOT, peut aider à faire le meilleur choix. En gérant efficacement les relations avec les fournisseurs, les MSP peuvent se concentrer sur la fourniture de services de haut niveau et sur une croissance durable de leur activité.

Ces éléments, souvent négligés, représentent une valeur significative pour le client et le MSP, soulignant les avantages d'une gestion efficace des relations avec les fournisseurs.

HORNETSECURITY

CHAPITRE 7

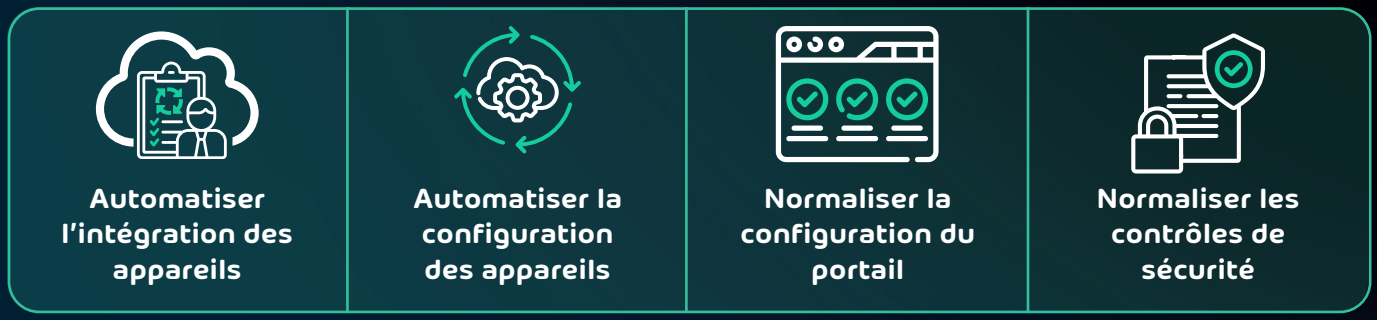
CONCLUSION

Dans cet eBook, nous avons couvert 5 facteurs importants qui conduisent à une opération MSP efficace : L'intégration, le suivi et la maintenance, la personnalisation, la gestion de la cybersécurité et la gestion des fournisseurs. Nous avons examiné ces principaux domaines d'activité des MSP et nous avons souligné les domaines dans lesquels des gains d'efficacité peuvent être réalisés et suggéré des moyens de les obtenir.

Voici ce que nous avons appris.

INTÉGRATION EFFICACE

Pour que l'intégration soit efficace, il faut accomplir les quatre tâches suivantes :



Graphique 22 Intégration efficace

L'utilisation d'outils inclus et tiers pour minimiser le temps nécessaire à l'accomplissement de ces tâches est essentielle, mais elle doit être équilibrée avec les attentes en matière de service au client et l'offre d'une expérience agréable au client. La recherche de cet équilibre portera ses fruits tout au long de la relation avec le client. Dans notre discussion, nous avons mis en évidence les différences entre les points de vue du client et du MSP. Sachez que ces différences n'existent pas seulement dans cette phase de la relation avec le client, mais dans tous ses aspects.

SUIVI ET MAINTENANCE

Nous avons exploré les aspects de l'efficacité des MSP dans les activités de surveillance et de maintenance. Nous avons abordé l'importance de la maintenance proactive, le rôle de la surveillance automatisée, l'importance de la procédure de réponse aux incidents et de la planification de la reprise après sinistre, ainsi que la nécessité de trouver un équilibre entre l'efficacité et l'expertise humaine. Il existe un réel besoin d'automatisation dans ce domaine, mais nous ne devons pas pour autant perdre de vue la relation avec le client.

Là encore, nous avons la possibilité d'automatiser et de satisfaire le client en même temps. Une grande partie du travail de routine d'un MSP est invisible pour le client. Le personnel de votre service d'assistance est donc votre porte d'entrée et un élément clé de la façon dont le client percevra vos services. Il est essentiel d'être aimable et efficace. En mettant en œuvre des procédures et des plans efficaces, les MSP peuvent améliorer leurs performances, réduire le stress et atteindre une plus grande rentabilité.

PERSONNALISATION

La maîtrise de la personnalisation et de la gestion du changement est cruciale pour les MSP afin de se différencier sur le marché et d'apporter de la valeur à leurs clients. En déployant efficacement des configurations personnalisées et en maintenant des modèles standardisés, les MSP peuvent s'assurer que les besoins uniques de leurs clients sont satisfaits tout en maintenant l'efficacité opérationnelle. Une gestion efficace du temps, en mettant l'accent sur la personnalisation plutôt que sur le déploiement, permet aux MSP de consacrer la majeure partie de leur temps à des tâches centrées sur le client, ce qui se traduit en fin de compte par une plus grande satisfaction du client et une présence plus forte sur le marché. En outre, la maîtrise de l'efficacité dans ce domaine pourrait permettre au MSP de commencer à se spécialiser dans des secteurs verticaux particuliers ou dans des exigences réglementaires, ce qui augmenterait encore l'efficacité et la rentabilité.

GESTION DE LA CYBERSÉCURITÉ

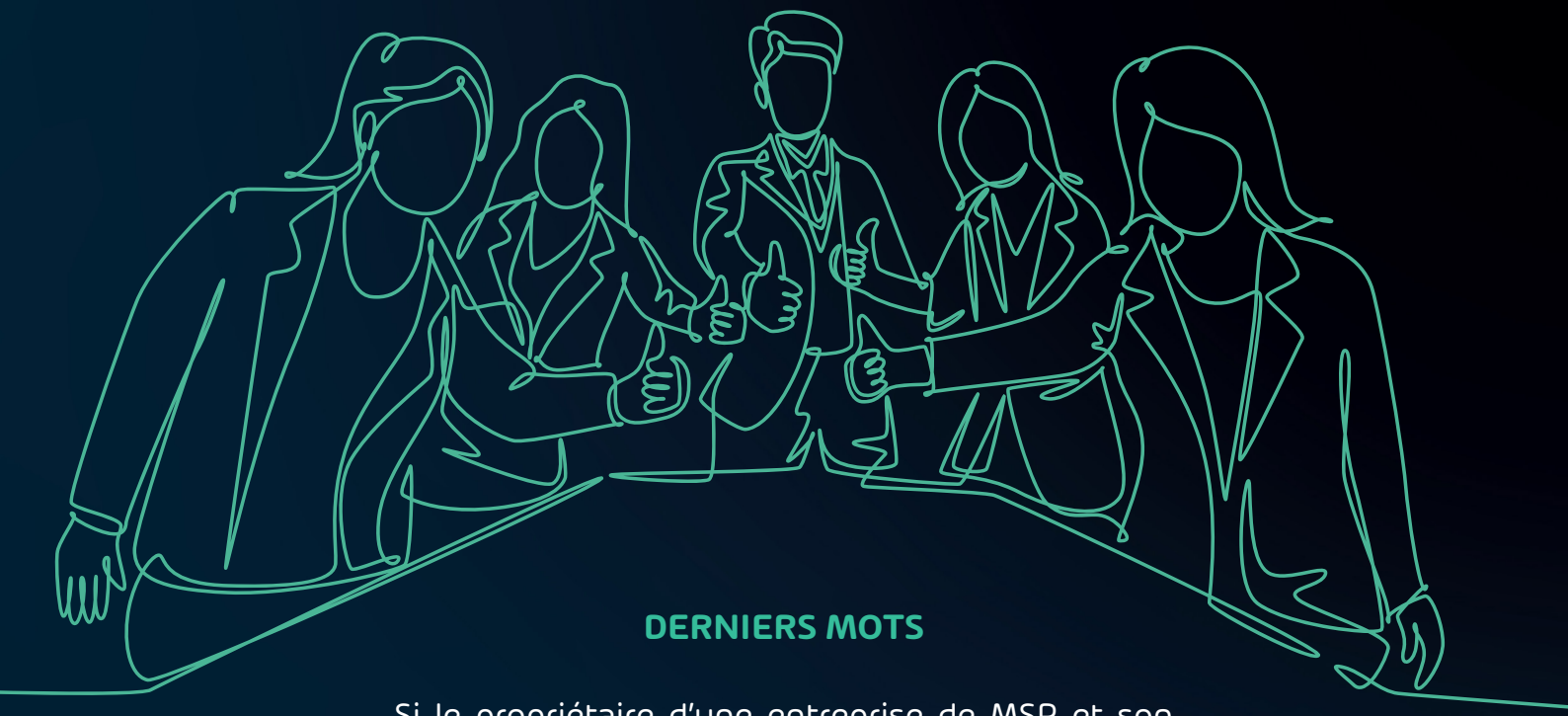
Il est essentiel de reconnaître que le paysage des cybermenaces est en constante évolution. Les professionnels de l'informatique axés sur les petites entreprises doivent rester vigilants et proactifs dans leur approche de la cybersécurité. En tirant le meilleur parti des outils et des stratégies présentés dans ce chapitre, les professionnels de l'informatique peuvent efficacement protéger les réseaux et les données de leurs clients tout en restant efficaces et rentables.

N'oubliez pas que la cybersécurité n'implique pas un effort ponctuel, mais un processus permanent qui nécessite un apprentissage et une adaptation continus. Ainsi, la gestion de la cybersécurité n'est pas si différente de la surveillance et de la maintenance en termes d'efficacité, et elle alimentera de nouvelles normes. Elle exige que le MSP dispose d'un personnel plus qualifié pour rester informé, préparé et sécurisé.

GESTION DES FOURNISSEURS

Avec l'évolution rapide du paysage commercial auquel les MSP sont soumis, beaucoup ont été confrontés à une prolifération des fournisseurs, car ils ont ajouté des fournisseurs pour essayer de suivre le rythme du changement. Réévaluer ces décisions dans un souci d'efficacité est une tâche importante et deux méthodes, SWOT et un tableau comparatif, ont été suggérées pour aider à cette analyse.

La simplification de la gestion des fournisseurs permet au MSP de se concentrer sur la fourniture de services de plus haut niveau, tels que les engagements de DSI ou de RSSI virtuels. Ce changement permet aux MSP de fournir des conseils stratégiques, d'aligner les initiatives de cybersécurité sur les objectifs de l'entreprise et d'offrir un avantage concurrentiel. Les clients apprécient davantage les services visibles, et les résultats tangibles tels que l'amélioration de la sécurité, la conformité aux réglementations et la réduction des risques conduisent à une plus grande satisfaction et à une plus grande fidélité de la part des clients. Monter dans l'échelle du professionnalisme en matière de cybersécurité signifie des profits plus élevés, des flux de revenus plus importants et des engagements plus précieux avec les clients. En se concentrant sur les services stratégiques, les MSP peuvent atteindre une croissance commerciale durable et capitaliser sur les tendances de l'industrie qui exigent des services de plus haut niveau.



DERNIERS MOTS

Si le propriétaire d'une entreprise de MSP et son personnel technique peuvent apprendre à maîtriser les cinq domaines que nous avons explorés, le succès ne pourra que suivre. Le MSP joue un rôle très important dans la réussite de toutes les entreprises, dans toutes les économies du monde. Peu d'entreprises sont assez grandes pour employer leur propre service informatique avec l'étendue des compétences que le MSP peut leur apporter. L'énormité du marché qu'un MSP efficace peut desservir rend l'opportunité presque illimitée. Lorsqu'un MSP réussit, tout le monde y gagne, et c'est l'efficacité qui est à l'origine de ce succès.