Acronis Protected Workspace : sécurisez le maillon faible !

Les ordinateurs portables, de bureau et les postes de travail sont des outils essentiels, qui comportent néanmoins des risques de sécurité considérables. Les collaborateurs les utilisent partout, ce qui les expose à un large éventail de menaces.

Pour les fournisseurs de services managés (MSP), les terminaux sont à la fois les ressources les plus critiques et les plus vulnérables qu'ils sont amenés à protéger. Ce qui n'est pas simple, car les MSP utilisent souvent plusieurs outils pour assurer la sécurité des terminaux. Et lorsque ces outils ne sont pas intégrés nativement, les faire fonctionner ensemble peut être difficile et laisser des failles dans la protection.

De plus, la gestion de plusieurs outils implique de devoir gérer des interfaces disparates, ce qui accroît la complexité, introduit des risques et nécessite souvent des domaines d'expertises spécifiques. Au final, les infrastructures de sécurité des espaces de travail reposant sur de multiples outils augmentent les coûts opérationnels, induisent des inefficacités et réduisent la protection globale.

Les cybercriminels utilisent l'intelligence artificielle pour créer des variantes d'attaques quasiment infinies, chaque jour devenant dès lors un zero-day. Les enjeux sont de taille : les attaques réussies entraînent des interruptions d'activité, des pertes de productivité et des préjudices de réputation pour les MSP et leurs clients, sans parler des problèmes de conformité pour de nombreux secteurs.

Cybersécurité, protection des données et gestion des terminaux nativement intégrées pour les espaces de travail

Les défis de la protection des espaces de travail pour les MSP

De nombreuses organisations ne disposent pas des ressources nécessaires pour gérer la sécurité des espaces de travail et font donc appel à des MSP. Elles ont besoin de fournisseurs de services pour sécuriser tous les ordinateurs portables et de bureau, où qu'ils se trouvent, de façon à protéger les données sans compromettre la productivité.

La cadence et la dimension mondiale des opérations des entreprises rendent cette tâche difficile pour les fournisseurs de services. Le problème est en partie lié à la scalabilité. Les centaines, voire les milliers de terminaux à protéger constituent une surface d'attaque considérable pour les MSP. Un seul terminal compromis peut rendre possible une cyberattaque apte à paralyser les activités des clients.

Ceux-ci ont également souvent des collaborateurs qui utilisent des terminaux un peu partout et envoient des données à travers le monde. Le télétravail complique la protection des espaces de travail. La mobilité, les opérations mondiales et l'exigence de réponses rapides exposent les terminaux des collaborateurs aux cyberattaques. Dans des secteurs comme la santé et la finance, des espaces de travail mal sécurisés peuvent compromettre la conformité réglementaire.

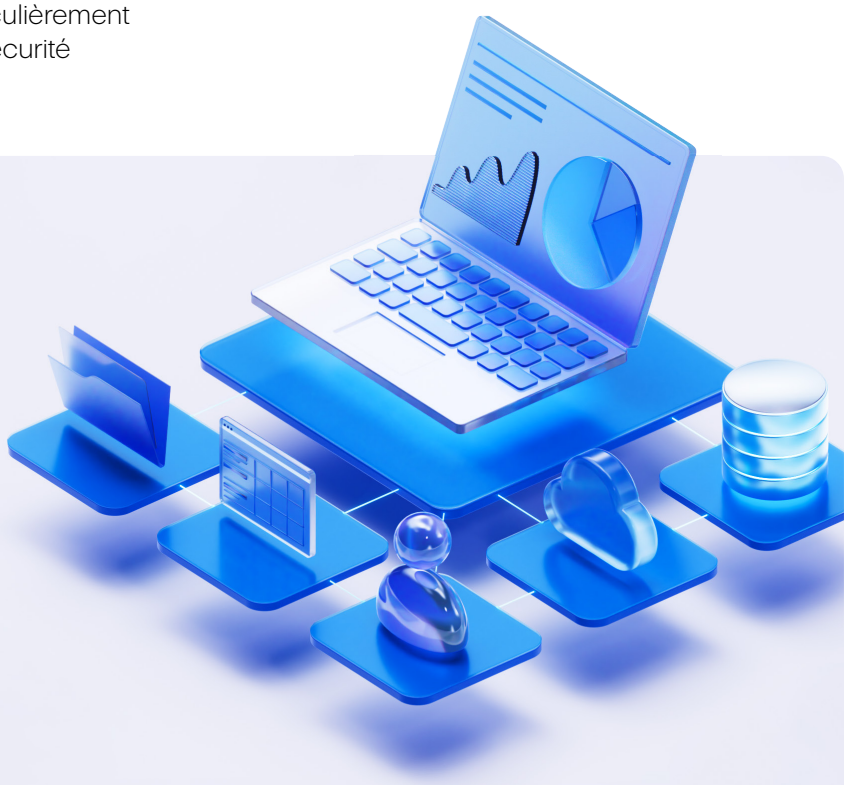
Le défi de la sécurité des espaces de travail pour les MSP

La protection des espaces de travail est particulièrement difficile pour les MSP, car les outils de cybersécurité des terminaux ne sont pas suffisamment efficaces pour répondre aux besoins des fournisseurs de services. Les outils fragmentés, avec une application antivirus, une autre application de sauvegarde et encore une autre de surveillance et de gestion à distance (RMM), rendent la protection des espaces de travail coûteuse et hasardeuse.

Chaque élément de protection nécessite une appli et une configuration uniques ; le nombre de combinaisons possibles tous terminaux confondus est pratiquement illimité. Et les MSP doivent disposer de personnel qualifié pour les gérer. Ils doivent embaucher plusieurs techniciens ou former des techniciens capables d'utiliser de nombreuses applications non intégrées, en espérant qu'ils ne commettent pas d'erreur.

La gestion de différents outils dans de multiples consoles entraîne des temps de réponse lents, épuise les techniciens et induit des erreurs. Le risque d'intégrations défaillantes peut également créer d'énormes failles de sécurité.

Les espaces de travail sont rarement « éteints », ce qui en fait une cible constante pour les cyberattaques. De plus, les collaborateurs des clients font souvent trop confiance à leurs terminaux, ce qui crée une couche de vulnérabilité supplémentaire. Les MSP ont besoin d'une solution de protection des espaces de travail qui offre des fonctionnalités de sécurité complètes et soit également facile à gérer.



« Dans de nombreuses organisations, une infrastructure de sécurité de l'espace de travail décousue entraîne une augmentation des coûts opérationnels et de la complexité, ainsi qu'une efficacité amoindrie de la sécurité. »

Gartner, 2025 Strategic Roadmap for Workplace Security

Acronis Protected Workspace fournit des services adaptés aux MSP

Acronis Protected Workspace inclut une série de services nativement intégrés qui permettent aux MSP d'assurer la protection des terminaux de leurs clients avec un risque minimal et une efficacité maximale. Ils sont disponibles par ressource ou par gigaoctet et incluent :

Services inclus dans Acronis Protected Workspace

Acronis Backup pour les postes de travail	Stocke et protège les données des ordinateurs portables, de bureau et des postes de travail des clients.
Acronis Advanced Backup pour les postes de travail	Étend les capacités de sauvegarde cloud pour assurer la protection des données des clients de manière proactive pour plus de 20 types de ressources, éliminant ainsi quasiment toutes les interruptions d'activité.
Acronis Endpoint Detection and Response (EDR)	Assure la surveillance active des terminaux, bloque les attaques avant qu'elles ne puissent causer des dommages et permet une restauration en un clic.
Acronis Extended Detection and Response (XDR)	Fournit une protection active et complète conçue pour prévenir, détecter, analyser, répondre aux incidents et restaurer rapidement les opérations.
Acronis Remote Monitoring and Management (RMM)	Des services d'administration et de surveillance supérieurs, avec une approche axée sur la sécurité. Automatisez tout et accélérez les opérations grâce à l'intelligence artificielle et à l'apprentissage automatique, associés à un puissant moteur de scripts. Découvrez et protégez les espaces de travail connectés avec Device Sense™.
Advanced Data Loss Prevention (DLP)	Empêche les fuites de données depuis les terminaux sans nécessiter de programme d'installation complexe ni de compétences particulières en termes de confidentialité.
Acronis Active Protection	Protège activement toutes les données des systèmes des clients, y compris les documents, les fichiers multimédias, les programmes, etc.
Antimalware Acronis	Protège de façon proactive et en temps réel les systèmes de vos clients contre les cyberattaques avancées grâce à des technologies de protection contre les virus, les malwares et les ransomwares reposant sur une analyse statique et comportementale assistée par l'intelligence artificielle.

Les MSP ont également la possibilité de choisir des packagings basés sur la solution, notamment :

Sauvegarde des postes de travail	Sécurité des terminaux + RMM	Ultimate Protection
Sauvegarde Acronis pour postes de travail avec 300 Go de stockage inclus	Acronis Active Protection	Package Sécurité et RMM
	Antimalware Acronis	Package Sauvegarde + stockage cloud
	Acronis EDR	Acronis Advanced Backup
	Acronis XDR	Acronis DLP
	Acronis RMM	

La puissance de la protection de l'espace de travail nativement intégrée

Les MSP ont besoin d'une méthode unifiée, efficace et rentable pour protéger, gérer et restaurer les espaces de travail. Acronis Protected Workspace fournit tous les services dont les MSP ont besoin pour assurer la protection des espaces de travail dans une solution unique, nativement intégrée : 1 agent, 1 licence et 1 console pour tout gérer. Cette approche simple mais puissante permet aux techniciens de gérer davantage d'espaces de travail avec une sécurité renforcée.

Acronis Protected Workspace offre également :

- **L'intégration native** de la sécurité des terminaux, de la gestion à distance et de la surveillance, ainsi que de la sauvegarde dans une console unique.
- **La protection de bout en bout :** anti-malware optimisé par l'intelligence artificielle, détection et réponse sur les terminaux (EDR), détection et réponse étendues (XDR), détection des ransomwares et analyse comportementale conformément au cadre de cybersécurité NIST.
- **L'efficacité opérationnelle :** résolution plus rapide des incidents, amélioration du service client et réduction des coûts de formation.
- **La flexibilité :** modèles de licence adaptés aux MSP avec possibilité de créer des packages de protection personnalisés.

« Acronis, notre plate-forme centrale, couvre tous les besoins. Son efficacité est inégalée : elle nous fait gagner du temps, réduit les coûts et limite les efforts de formation. Le fait d'avoir tout réuni en une seule console de gestion permet de gérer notre pile de manière cohérente et simplifiée. »

– Joshua Aaronson, cofondateur, Panda Technology

Acronis Protected Workspace fournit aux MSP les outils dont ils ont besoin pour assurer la sécurité des terminaux.

Avec Acronis Protected Workspace, les MSP peuvent relever le défi de la sécurisation des ordinateurs portables, des ordinateurs de bureau et des postes de travail sans devoir gérer une multitude d'applications de sécurité. Les fournisseurs de services peuvent se démarquer de la concurrence en proposant une protection plus efficace, des délais de réponse plus courts et un service client de meilleure qualité.

Acronis Protected Workspace vous intéresse ? CONTACTEZ-NOUS

Acronis

Pour en savoir plus, visitez www.acronis.com