BeyondTrust

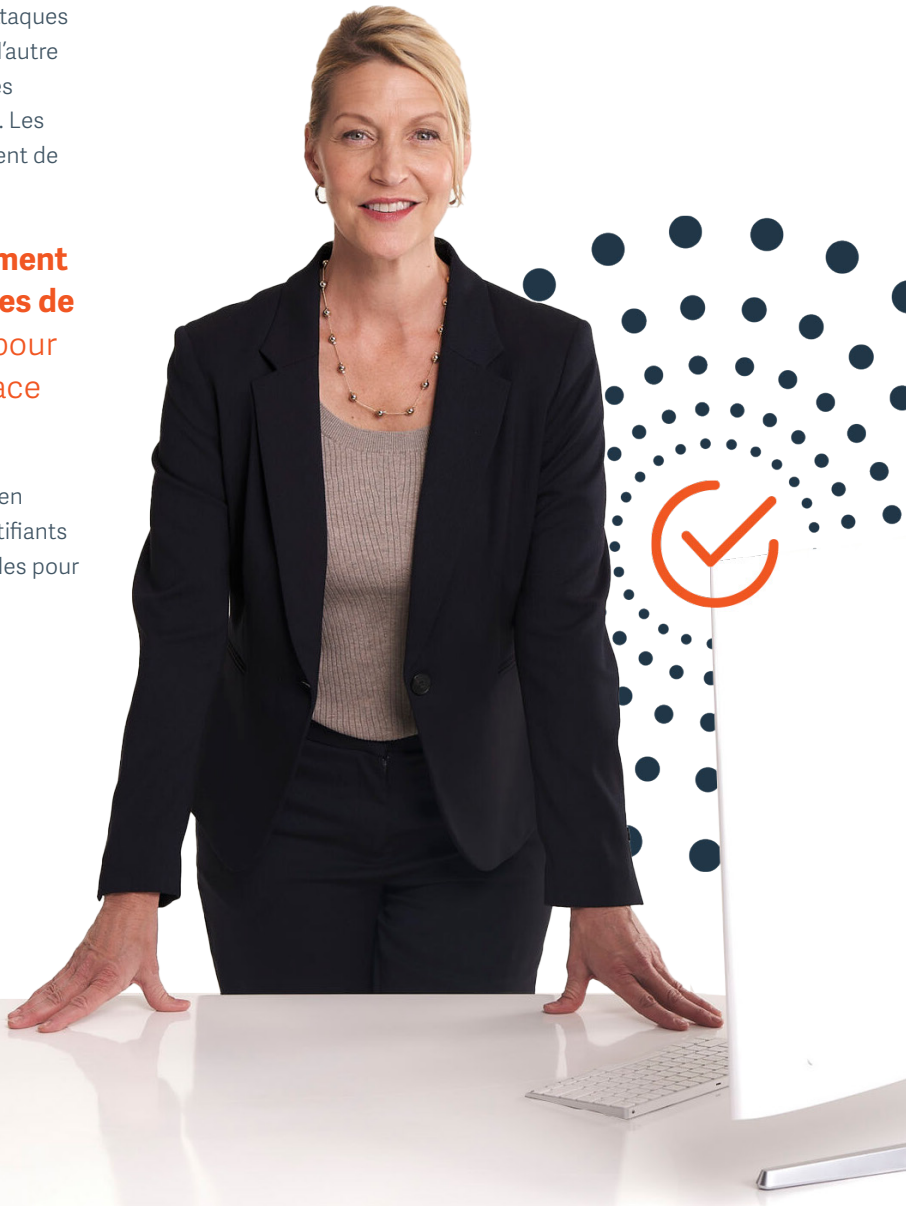
Répondre aux exigences en matière d'assurance avec le PAM

Checklist des assurances de cybersécurité

Face à l'afflux extrêmement rapide de cybermenaces et d'attaques de ransomware, les compagnies de cyber-assurance n'ont d'autre choix que d'augmenter nettement leurs tarifs et leurs primes ainsi que de refuser de couvrir les entreprises à haut risque. Les conditions de souscription à une cyber-assurance deviennent de plus en plus strictes.

Les solutions Privileged Access Management (PAM) de BeyondTrust apportent les bases de sécurité que les cyber-assureurs exigent pour réduire les risques et les responsabilités face aux cybermenaces internes et externes.

Nos produits réunissent les fonctions essentielles de mise en place du moindre privilège, de gestion des comptes et identifiants privilégiés et de sécurité des accès à distance, indispensables pour prétendre souscrire une assurance de cybersécurité.



Checklist des assurances de cybersécurité

Principaux critères d'éligibilité	En quoi le PAM peut être utile ?	La valeur ajoutée de BeyondTrust
Vos utilisateurs ont-ils des droits administrateurs locaux sur leurs ordinateurs fixes et portables ?	Il supprime tous les droits admins et n'élève les droits d'accès sur les applications que pour le contenu approprié et pendant une durée définie.	La suppression des droits admin est l'un des moyens les plus efficaces pour réduire la surface d'attaque et se défendre des menaces externes et internes. **BeyondTrust protège instantanément votre environnement et vous permet d'affiner vos règles au gré des comportements analysés.** En supprimant les droits admin et en élevant les applications, et non les utilisateurs, vous bénéficiez du moindre privilège dès le premier jour, sans impacter la productivité.
Pouvez-vous confirmer que les comptes humains et non humains observent systématiquement le principe de moindre privilège ?	Il met en place le principe du moindre privilège et le contrôle applicatif à tous les comptes et identités humains et non-humains sur tout type de endpoint.	La mise en place du moindre privilège réduit grandement la surface d'attaque. Cela protège les entreprises des menaces sans fichier et des attaques zero day. **Les solutions BeyondTrust vous aident à appliquer le principe de moindre privilège à tout votre écosystème IT, y compris les identités humaines et non-humaines.** Nos solutions vous aident à dimensionner correctement les privilèges et les permissions sur site et aussi dans le cloud.
Quelles sont les protections actives des accès à distance au réseau interne ?	Il établit l'accès par proxy au réseau interne, aux applications, aux actifs et gère toutes les connexions sortantes, sans VPN.	La gestion de toutes les sessions à distance privilégiées de fournisseurs et employés, y compris les identifiants de vaulting, permet un contrôle d'accès précis, quelle que soit l'origine de la session. **Avec BeyondTrust, la redirection de toutes les connexions via un chemin d'accès unique contribue à réduire la surface d'attaque tout en établissant une liste unique des endpoints autorisés pour chaque utilisateur.** L'expérience utilisateur est également améliorée puisqu'une seule interface donne accès à tous les endpoints.
Utilisez-vous des outils ou logiciels pour gérer les comptes privilégiés ?	Il découvre, gère, contrôle, surveille et audite toutes les activités des comptes privilégiés sur l'infrastructure IT.	Les solutions PAM sécurisent et gèrent tous les types de comptes privilégiés. **Les solutions BeyondTrust vous aident à découvrir, sécuriser, contrôler, surveiller, donner l'alerte et enregistrer les accès à tous les comptes privilégiés.** Avec BeyondTrust, vous bénéficiez aussi de l'analyse et du reporting des menaces privilégiées pour les besoins de cyber-assurance et de conformité.
Utilisez-vous l'authentification multifactorielle pour les accès à distance de l'extérieur du réseau par vos employés ou des tiers (ex. VPN, PC distant) ?	Il instaure l'authentification multifactorielle pour les accès à distance et permet l'intégration transparente des outils MFA de tiers.	L'authentification MFA établit une couche supplémentaire de sécurité qui garantit que l'accès n'est autorisé qu'à la bonne identité. **BeyondTrust inclut l'authentification multifactorielle native pour les accès à distance des employés et des tiers et permet l'intégration transparente des grandes solutions MFA, pour valoriser au mieux les investissements dans la technologie.**

Checklist des assurances de cybersécurité

Principaux critères d'éligibilité	En quoi le PAM peut être utile ?	La valeur ajoutée de BeyondTrust
Utilisez-vous des systèmes d'exploitation ou plateformes sans support ? Si oui, quels contrôles compensatoires appliquez-vous ?	Il restreint les privilèges au minimum nécessaire pour limiter les risques d'utilisation abusive des systèmes ou plateformes.	**Les solutions BeyondTrust vous aident à appliquer le principe de moindre privilège aux utilisateurs humains et non-humains, limitant les utilisations abusives ou compromissions de tout système.** Nos solutions permettent aussi l'accès par proxy et la segmentation ou microsegmentation pour isoler les plateformes à risque ou sans support des autres actifs réseau afin de contenir la propagation en cas de compromission. La rotation des identifiants privilégiés et la surveillance de session protègent les actifs critiques par le contrôle et la surveillance de toute activité privilégiée.
Avez-vous recherché les Indicateurs de compromission (IoC) dans votre environnement ?	Il capture toutes les données des sessions privilégiées, y compris journaux de frappe, enregistrement d'écran, commandes tapées/exécutées, de façon à identifier les compromissions et le chemin suivi en interne par l'agresseur.	**Les solutions BeyondTrust peuvent vous aider à acquérir une vue centralisée de tous les actifs, comptes et utilisateurs dans votre environnement. Les informations sont corrélées aux normes comportementales attendues, elles permettent d'identifier les changements et de signaler les anomalies pouvant indiquer la présence de menaces critique.** Nos solutions permettent aussi d'identifier des Indicateurs de compromission pouvant indiquer une progression latérale ou une élévation de privilège inappropriée, liée à des commandes ou à un comportement inhabituel d'un utilisateur, tandis que la surveillance de l'intégrité des fichiers permet d'identifier tout changement suspect dans les systèmes Unix/Linux.
Si vous en avez trouvé, les avez-vous corrigés ?	Il procède à la rotation des identifiants compromis pour bloquer l'accès et empêcher que les mots de passe puissent être réutilisés. Les droits d'accès privilégiés peuvent être limités ou supprimés pour réduire les risques de progression latérale et d'exécution de malware.	**BeyondTrust propose plusieurs mécanismes pour prévenir les compromissions de données et les corriger le cas échéant.** Nos solutions déclenchent des alertes en cas d'activité anormale pour éviter l'utilisation abusive ou le vol d'identifiants privilégiés. Une rotation des identifiants est possible également pour bloquer les attaques ou dès qu'un identifiant a été compromis. Les droits admin des utilisateurs peuvent être réduits pour limiter la progression sur le réseau ou l'exécution de malware.
Décrivez toutes les mesures prises pour détecter et prévenir les attaques de ransomware.	Il empêche l'introduction et la progression des ransomwares et malwares par une sécurité robuste des accès distants, par l'intégration et la gestion des identifiants privilégiés et par la mise en place du moindre privilège et du contrôle applicatif.	**Les solutions BeyondTrust apportent une couverture complète de tous les scénarios impliquant des ransomwares, malwares et autres cybermenace.** Nos solutions empêchent tout ransomware, malware ou opérateur humain de progresser latéralement et d'élever les privilèges pour perpétrer une attaque. Les cybercriminels sont bloqués au point de compromission initial.

Souscrivez à une assurance cybersécurité et réduisez vos risques grâce aux solutions PAM de BeyondTrust.

Les compagnies d'assurance cybersécurité reconnaissent que les contrôles de sécurité des accès privilégiés constituent la base de la sécurité dans toute entreprise, qu'ils permettent de bloquer les cyberattaques et qu'ils limitent grandement les dégâts potentiels d'une compromission. Privileged Access Management de BeyondTrust peut vous aider à remplir les critères d'éligibilité à une cyber-assurance et à obtenir les meilleurs tarifs, tout en réduisant vos risques de cybersécurité.

Pour en savoir plus
beyondtrust.com/solutions/cyber-insurance

BeyondTrust

BeyondTrust est le leader mondial de la gestion des accès privilégiés (PAM), permettant aux organisations de sécuriser et de gérer l'ensemble de leur univers de privilèges. Nos produits et notre plateforme intégrés offrent la solution PAM la plus avancée du secteur, permettant aux entreprises de réduire rapidement leur surface d'attaque dans des environnements traditionnels, cloud et hybrides.

beyondtrust.com/fr