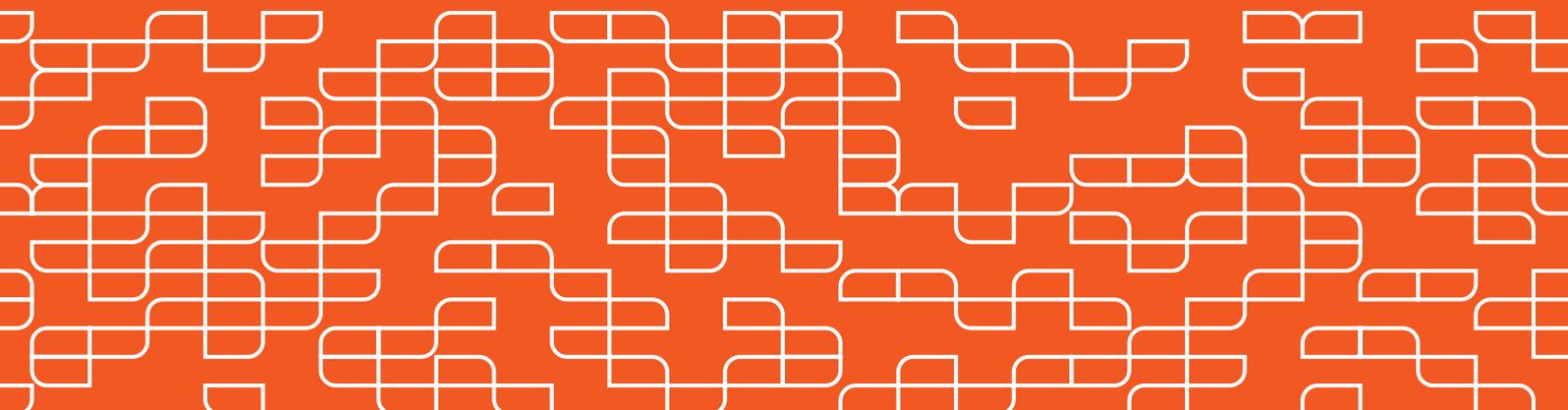


EMPOWERED PRIVILEGED ACCESS

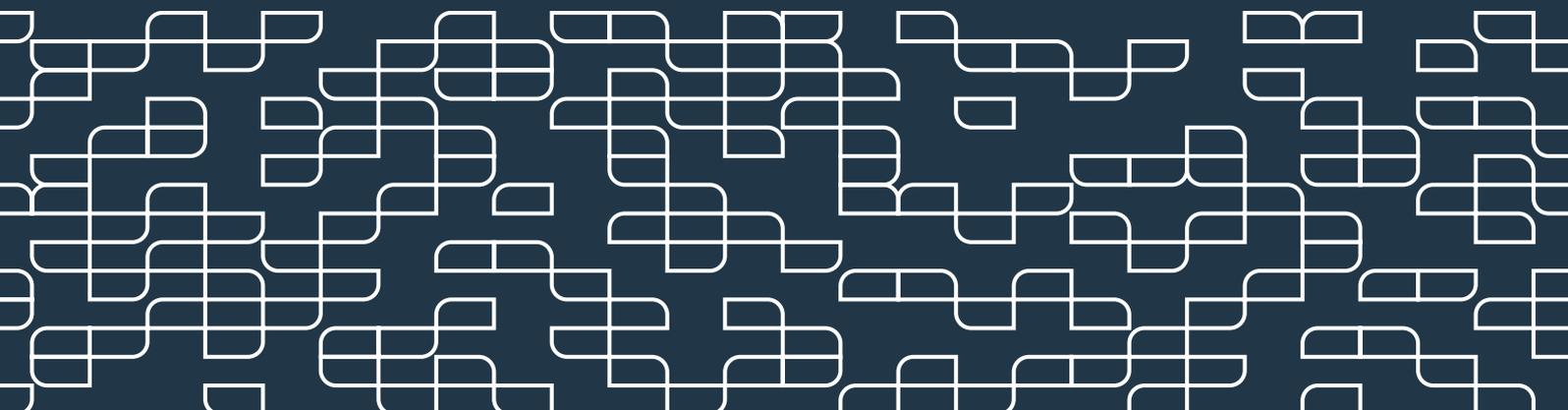
Protégez-vous des menaces liées aux identifiants volés, aux privilèges compromis et aux accès distants indésirables, tout en boostant la productivité des utilisateurs.





Les employés, tiers et autres insiders ayant des accès excessifs et superflus à vos systèmes et données sont un risque majeur pour votre sécurité.

BeyondTrust vous protège de ces menaces et facilite votre mise en conformité avec les réglementations en vigueur sans que cela n'impacte la productivité de votre organisation.



PLATEFORME PRIVILEGED ACCESS MANAGEMENT

La plateforme PAM de BeyondTrust est une solution intégrée offrant visibilité et contrôle sur tous les comptes et utilisateurs privilégiés. Facile d'utilisation et riche d'un grand nombre de fonctionnalités pour la sécurité des privilèges, la solution se déploie simplement et aide à réduire les risques de compromissions des privilèges.

Découverte • Analyse des menaces • Rapports & connecteurs • Gestion centralisée des politiques de sécurité



Gestion des sessions & des mots de passe privilégiés

Identifiez, gérez, auditez, et contrôlez tous les comptes privilégiés



Gestion des privilèges sur les endpoints

Supprimez les droits admin et privilèges excessifs des utilisateurs sur Windows, Mac, Unix, Linux, et dispositifs réseaux



Accès distants sécurisés

Sécurisez, gérez et auditez les accès privilégiés distants des tiers et insiders, et dépannez les systèmes à distance

Gestion des vulnérabilités

Identifiez, priorisez et corrigez les vulnérabilités, et accordez les privilèges en tenant compte des risques potentiels

Audit du changement

Auditez, générez des rapports et récupérez les changements sur l'ensemble des plateformes Microsoft Windows

Plus de 20 000 organisations utilisent BeyondTrust pour protéger leurs données et systèmes critiques tout en conservant leur productivité.

ServiceNow • MD Anderson Cancer Center • Business France • Verizon • Qualcomm • Roche Accor • Starbucks • Payboost (groupe Véolia Eau) • PayPal • Rolex • McKesson • Cegid

LA RÉALITÉ EN FACE

Les comptes et privilèges non gérés
sont sources de failles de données.

9/10

des vulnérabilités sont liées à
des droits admin excessifs¹

81%

des brèches débutent par des
mots de passe volés
et / ou faibles²

80%

des brèches résultent
d'utilisations inappropriées
ou malveillantes de comptes
à privilèges³

62%

des entreprises ne contrôlent
pas correctement leurs
accès privilégiés⁴

1: 2018 Microsoft Vulnerabilities Report, BeyondTrust

2: 2017 Data Breach Investigations Report[®], 10th Edition, Verizon

3: 2018 Forrester Wave: Privileged Identity Management

4: 2018 Privileged Access Threat Report, BeyondTrust

SOLUTIONS PRIVILEGED ACCESS MANAGEMENT



Gestion des sessions & des mots de passe à privilèges

- Découverte et enrôlement automatique
- Fonctionnalités avancées de contrôle et de gestion des sessions
- Analyses et rapports des menaces
- Déploiement clé en main



Gestion des privilèges sur les endpoints

- Fonctionnalités disponibles sur un large choix de plateformes (Windows, Mac, Unix, Linux) et de dispositifs réseaux
- Granularité du contrôle des applications et des commandes
- Mise en place du « least privilege » (principe du moindre privilège)
- Déploiement rapide



Accès à distance sécurisés

- Contrôle des accès des tiers et insiders
- Assistance à distance fiable et instantanée sur tout poste de travail, serveur ou appareil portable
- Protection des mots de passe et gestion des sessions intégrées
- Déploiement flexible et différentes options de licensing



Gestion des vulnérabilités

- Couverture complète
- Analyses et rapports détaillés
- Evaluation du risque dans son contexte



Audit du changement

- Audit en temps réel et restauration en environnement Windows
- Restauration et retour en arrière de l'Active Directory
- Console de gestion unique



BeyondTrust possède une expérience de plus de 30 ans dans la sécurité des privilèges. Plus de 20 000 entreprises dans le monde et un réseau solide de partenaires nous font confiance au quotidien.



CAS D'UTILISATION

*Protection des identifiants
et des mots de passe*

*Suppression des droits
admin et des privilèges
utilisateurs sur
les systèmes*

*Suppression des mots de
passe dans les applications*

*Contrôle de l'utilisation
des applications*

*Support des utilisateurs,
systèmes et appareils*

*Contrôle et gestion des
accès des tiers*

*Conformité et respect des
réglementations*



Visitez notre site web pour plus d'informations sur les solutions BeyondTrust

beyondtrust.com/fr