BeyondTrust

GARANTIR LA SÉCURITÉ & LA CONFORMITÉ DE L'IOT / IIOT

GESTION INTÉGRÉE DES ACCÈS PRIVILÉGIÉS ET DES VULNÉRABILITÉS POUR TOUS LES DISPOSITIFS

Les périphériques IoT non identifiés ou mal gérés peuvent être sources d'importantes failles de sécurité, qui rendent les réseaux vulnérables face aux failles de sécurité, aux fuites de données, aux vols de propriété intellectuelle, aux attaques par déni de service et aux lacunes de conformité réglementaire. L'Internet des Objets non sécurisé étant de plus en plus exploité dans le cadre d'attaques d'ampleur toujours plus impressionnante, il n'a jamais été aussi important de sécuriser de manière proactive ces appareils. La solution BeyondTrust de sécurité de l'IoT / IIoT permet de scanner et découvrir tous les périphériques de ce type présents sur l'environnement, de les gérer par groupe pour une gestion des privilèges cohérente et d'analyser les vulnérabilités et les risques liés aux privilèges au sein d'une même solution.

Identification de tous les appareils IoT / IIoT
Identifiez tous les périphériques, vulnérabilités et failles de sécurité, y compris sur les mots de passe codés en dur et les comptes partagés.

Sécurité renforcée IoT / IIoT
Corrigez les vulnérabilités et étendez les bonnes pratiques de contrôle, de gestion et de sécurité des accès privilégiés à tous les périphériques.

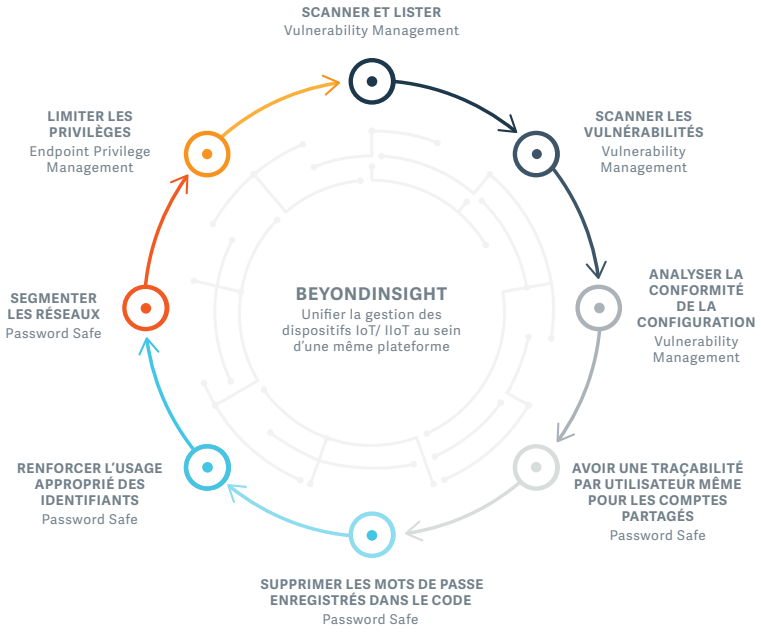
Gestion unifiée IoT / IIoT
Centralisez la gestion des privilèges, la gestion des vulnérabilités et la création de rapports portant sur l'IoT / IIoT au sein d'une plate-forme unique.

Caractéristiques et fonctionnalités

- **Découverte et inventaire :** effectuez un scan continu des périphériques IoT.
- **Analyse des vulnérabilités :** analysez les réseaux et les périphériques IoT, en fournissant des rapports permettant de hiérarchiser les risques.
- **Analyse de la conformité de la configuration :** effectuez une analyse permanente et renforcez la sécurité en continu, conformément aux directives du secteur et aux meilleures pratiques fournies par NIST, CIS et Microsoft.
- **Gestion des comptes partagés :** contrôlez et auditez l'accès aux comptes partagés. Gérez et faites pivoter les identifiants au sein de votre environnement.
- **Suppression des identifiants codés en dur :** contrôlez l'accès aux scripts, aux fichiers, au code, aux identifiants enregistrés dans les applications notamment en éliminant les mots de passe codés en dur dans les périphériques IoT.
- **Gestion des identifiants privilégiés :** éliminez les privilèges admin sur les endpoints, grâce à un simple process de workflow pour l'archivage et l'extraction, ainsi que la surveillance des sessions à privilèges.
- **Segmentation du réseau :** utilisez un serveur de rebond sécurisé avec une authentification forte, une autorisation d'accès évolutive et une surveillance des sessions. Délimitez clairement des frontières entre les systèmes de développement, de test et de production.
- **Gestion des privilèges :** accordez uniquement les autorisations requises aux périphériques. Surveillez les commandes indiquant un mouvement latéral et fournissez la traçabilité nécessaire pour les audits et forensics.

GARANTIR LA SÉCURITÉ & LA CONFORMITÉ IOT / IIOT

L'approche BeyondTrust en 8 étapes pour sécuriser les appareils IoT



Les solutions BeyondTrust pour la protection des appareils IoT/IIoT font partie de la plateforme BeyondTrust Privileged Access Management (PAM). Celle-ci inclut de nombreuses fonctionnalités pour les environnements sur site, virtuels et cloud. Les solutions BeyondTrust proposent :

- **Gestion des sessions & des mots de passe privilégiés**
- **Gestion des privilèges sur les endpoints**
- **Accès distants sécurisés**
- **Gestion des vulnérabilités**
- **Audit du changement**

BÉNÉFICES

- Sécurité renforcée : seuls les périphériques correctement configurés, sécurisés et autorisés sont disponibles et utilisés dans votre environnement - pas de shadow IT !
- Meilleure visibilité grâce à une évaluation continue des vulnérabilités et à des conseils de remédiation sur l'infrastructure dans les environnements IoT physiques, virtuels et cloud.
- Responsabilisation accrue en veillant à ce que tous les comptes soient correctement gérés et renouvellés dans l'environnement et que toutes les activités contrôlées soient associées à une identité unique.
- Réduction des risques en limitant l'accès des développeurs et des testeurs aux périphériques, en fermant les portes dérobées aux systèmes critiques et en limitant les mouvements latéraux.

BeyondTrust est le leader mondial du Privileged Access Management, offrant l'approche la plus complète du marché afin de réduire les risques de failles liées à l'exploitation des privilèges. Flexible, notre plateforme permet aux organisations de sécuriser les privilèges sur les endpoints, serveurs, réseaux et environnements cloud, DevOps etc. de façon évolutive pour faire face aux menaces en constante mutation et évolution. Plus de 20 000 clients dans le monde nous font confiance.

beyondtrust.com/fr

V2019_06_FRE