

Sécurité matérielle et logicielle

Solutions de vidéo sur IP, affichage dynamique et expérience client



Exterity fait tout son possible pour garantir la sécurité, la robustesse et la fiabilité de ses solutions complètes d'IPTV. Ce petit guide vous apprendra tout sur nos fonctionnalités de sécurité, tant logicielles que matérielles, ainsi que sur leur importance. Pour en savoir plus sur la sécurisation de contenu, consultez le [guide consacré à ce sujet](#).

Notre offre

Son importance

Conformité à la norme ISO 9001

Nous avons fait vérifier nos processus de conception technique et de fabrication afin de garantir le plus haut niveau d'assurance qualité. Le fait que nos solutions complètes soient fabriquées au Royaume-Uni nous permet de superviser intégralement notre processus de fabrication.

Des processeurs sécurisés sur toutes les plateformes intégrées

Permet de garantir la robustesse et la sécurité matérielles et signifie que ces plateformes ne prendront en charge que les logiciels Exterity, empêchant ainsi l'installation de codes malveillants.

(Média Players AvediaPlayer, Encodeurs et Passerelles AvediaStream)

Cela signifie également que nous répondons à l'ensemble des exigences des diffuseurs en matière de protection de contenu et sommes en mesure de diffuser des chaînes premium en toute sécurité par l'intermédiaire d'un réseau IP.

De plus, les données transmises en clair ne transitent pas par des interfaces en standard ouvert. Un tiers peut donc y accéder et les modifier facilement.

Seules des mises à jour approuvées par Exterity peuvent être installées sur nos produits

Garantit que vos produits Exterity sont mis à jour à l'aide de firmwares testés et approuvés. Ainsi, aucun code malveillant ne peut être installé sur vos appareils Exterity.

(Média Players AvediaPlayer, Encodeurs et Passerelles AvediaStream)



AvediaPlayer
Média Player



AvediaServer



Passerelle
AvediaStream

Notre offre

Son importance

Nos Média Players AvediaPlayer disposent de vis de sécurité

Nos média players étant souvent situés dans des espaces publics, nous utilisons des vis de sécurité spéciales lors de l'assemblage. Il est donc impossible d'ouvrir nos produits sans certains outils spécifiques (des outils normaux ne fonctionneront pas). Nos produits sont ainsi protégés contre toute tentative de sabotage.

Interface utilisateur HTTPS

Nos interfaces administration web sont protégées par un protocole de sécurité HTTPS, ce qui signifie que toutes les communications entre l'ordinateur administrateur et l'appareil Exterity sont chiffrées, empêchant ainsi toute attaque par le milieu.

Prise en charge du proxy HTTP

Seuls certains appareils peuvent accéder à internet. Permet de préserver l'intégrité du réseau interne.

Protocole 802.1x

(Média Player AvediaPlayer série 93)

Empêche tout accès non autorisé aux réseaux, le réseau IP n'acceptant que certains appareils certifiés.

Protocole SSH

Permet de s'authentifier en toute sécurité et protège les communications à l'aide de protocoles de chiffrement robustes. L'accès par lignes de commande non sécurisées n'est pas autorisé.

Pare-feu du réseau

Sert à gérer l'accès administrateur et/ou à contrôler les accès aux ports sur des appareils Exterity.

Authentification unique et assistance Active Directory

(AvediaServer, serveur Origine AvediaStream, transcodeur et encodeur e5640)

Facilite l'accès au système pour vos utilisateurs tout en conservant vos stratégies de sécurité à l'aide de l'intégration d'Active Directory. L'authentification unique permet de garder cette stratégie en place et autorise l'accès à AvediaServer. Les risques de mots de passe oubliés, perdus ou encore trop faibles sont donc réduits.

Contrôle d'accès API basé sur les utilisateurs

(AvediaServer, serveur Origine AvediaStream, transcodeur et encodeur e5640)

Vous permet de choisir et de contrôler les utilisateurs ou groupes d'utilisateurs qui peuvent accéder à certaines options du serveur, par exemple celles permettant de restreindre l'accès aux paramètres du système, de créer et gérer du contenu.

Protection par mot de passe

Tous nos appareils sont protégés par un mot de passe.

Analyse de vulnérabilité

Chaque fois que nous publions un nouveau logiciel, nous recherchons les vulnérabilités universellement connues.



Siège social
+44 (0) 1383 828 250

Australie
+61 (0) 2905 61199

Europe
+33 (0) 3 52 84 01 23

Arabie Saoudite
+966 (11) 834 3530

Singapour
+65 3157 9352

Afrique du Sud
+27 (0) 11 469 0465

Emirats Arabes Unis
+971 (4) 447 0604

Etats-Unis
+1 201 580 2130

e: info@exterity.com

w: www.exterity.com



© 2021 Exterity Ltd. Tous droits réservés. Le logo d'Exterity, ArtioGuest, ArtioPortal, ArtioSign, AvediaPlayer, AvediaServer et AvediaStream sont des marques déposées ou enregistrées au nom d'Exterity Ltd. Les informations et spécifications sont sujettes des changements sans aucune préavis. Exterity vérifie que toutes les informations du document sont à jour mais n'accepte aucune responsabilité pour toute erreur ou omission.