Hardware and Software Security Features

IP Video, Digital Signage and Guest Experience Solutions

At Exterity, we strive to ensure our end-to-end IPTV solutions are secure, robust and reliable. This short guide details our hardware and software security features, and why they matter. To find out more about content security, check our content security guide.

What we offer	Why it's important
We are ISO 9001 compliant	Our engineering design and manufacturing workflows have been audited, ensuring the highest level of quality assurance. We manufacture our end-to-end solutions in the UK, meaning we have complete control over our production workflow.
Secure processors on all embedded platforms *(AvediaPlayer Media Players, AvediaStream Encoders and Gateways)*	Ensures physical security and robustness, and means these platforms will only run Exterity software, preventing the installation of malicious code. It also means we meet broadcasters' content protection requirements and can deliver premium channels securely across an IP network. Additionally, when distributed in the clear, data is not passed over open standard interfaces, which could be easily accessed and altered by third-party.
Only Exterity signed upgrades can be installed on our products *(AvediaPlayer Media Players, AvediaStream Encoders and Gateways)*	Guarantees that only verified and trusted firmware can be used to upgrade your Exterity products, meaning malicious code cannot be installed on your Exterity hardware.
We use security screws on our AvediaPlayer Media Players	As media players are frequently located in public spaces, we use special security screws on assembly. This means that specific tools are needed to fasten and unfasten our products. Standard tools won't work with them, making them resistant to tampering.

AvediaServer

AvediaPlayer
Media Player

AvediaStream
Gateway

What we offer	Why it's important
HTTPS-based user interface	Our web admin interfaces are secured by HTTPS, meaning that communication between the admin computer and the Exterity device is encrypted, preventing man-in-the-middle attacks.
HTTP proxy support	Means that only certain devices can access the internet and helps to ensure security of the internal network.
802.1x protocol *(AvediaPlayer 93-series Media Player)*	Protects networks from unauthorised access, as only certified devices will be able to function on the IP network.
SSH protocol	Provides secure authentication and protects the communications with strong encryption protocols. We do not support non-secure command line access.
Network firewall	Used to manage admin access and/or control access to ports on Exterity devices.
Single Sign On and Active Directory support *(AvediaServer, AvediaStream Origin Server, Transcoder and e5640 Encoder)*	Makes it easy for your users to access the system while maintaining your security policy through Active Directory integration. Single Sign On maintains this policy and enables access to the AvediaServer, reducing the risk of lost, forgotten or weak passwords.
User-based API access control *(AvediaServer, AvediaStream Origin Server, Transcoder and e5640 Encoder)*	Allows you to decide and control which users or groups of users can access specific capabilities on the server such as restricting access to system settings, creating and managing content, and more.
Password protection	All of our devices are password protected.
Penetration testing	Every time we release new software, we simulate a cyber attack to find weaknesses before attackers do.

Exterity Headquarters
t: +44 (0) 1383 828 250 w: www.exterity.com e: info@exterity.com