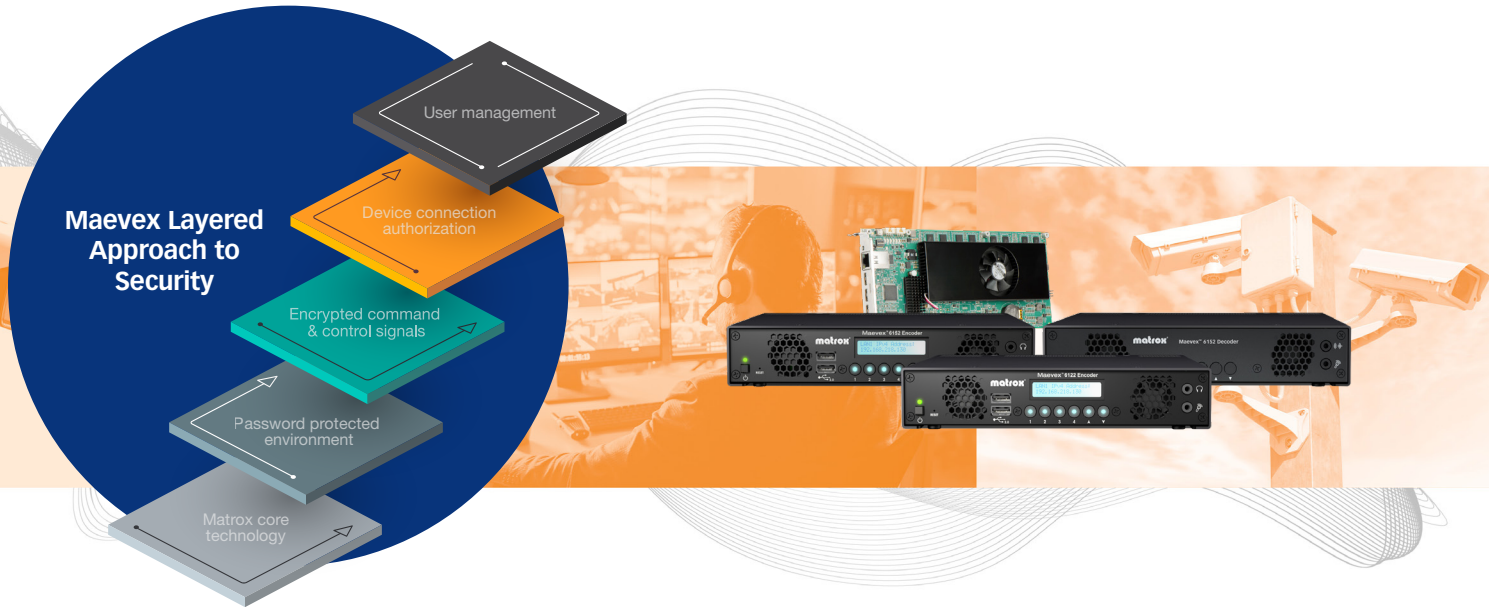


Enterprise-grade Security with Matrox MaeveX Series



Matrox MaeveX Series encoders and decoders are ideal for control rooms, real-time crime centers, and other mission critical environments. The devices employ a multi-layered security approach to protect confidential information and ensure continued operation of your surveillance and monitoring systems.

Encryption & Secure Communication

MaeveX Series supports industry-standard secure communication protocol and encryption, such as:

- **HTTPS:** Transmits commands over HTTPS, a secure communication protocol using TLS, which encrypts command and control signals exchanged between MaeveX devices and PowerStream Plus management application.
- **TLS:** Uses TLS, an industry-standard transport protocol, for secure and encrypted data transmission and communication.
- **IGMPv3:** Enables you to register trusted source devices in multicast.
- **SSH:** Supports Secure Shell (SSH) for encrypted network services, ensuring secure command execution and data exchange between devices over an IP network.
- **IPv6:** Implements Internet Protocol version 6 (IPv6) for enhanced network security and efficiency, supporting advanced features like IPsec for secure data transmission.
- **SRT Protocol with AES Encryption:** Provides secure, reliable transport of video streams with encryption for data security.

Authentication & Authorization

MaeveX Series prioritizes access control and user and device authentication to prevent unauthorized access:

- **Credential management:** Administrators can assign access rights to specific users for specific encoder and decoder devices.
- **Password protection:** MaeveX devices ensure security through password protection, allowing administrators to restrict access to authorized users only.
- **Microsoft Active Directory:** MaeveX devices are compatible with Microsoft Active Directory, enabling IT administrators to securely and efficiently handle user and group accounts.
- **Digital certificates:** Matrox digital certificates are pre-installed in each device for unique identification.
- **802.1x:** This IEEE standard prevents unauthorized devices from connecting to a local area network (LAN), enhancing network security by controlling access at the port level.
- **Disable protocols:** Users can deactivate SSH, UPnP, SNMP, and USB functionalities to prevent potential vulnerabilities associated with these protocols.
- **No CEC support on HDMI:** MaeveX devices exclude Consumer Electronics Control (CEC) on HDMI connections, mitigating risks associated with unauthorized control.



Monitoring & Updates

- **Firmware updates:** Perform firmware updates in a password-protected environment with the use of encrypted payloads and checksums to guarantee the use of Matrox coded firmware.
- **Vulnerability updates:** Regularly assess and update the system to address emerging security vulnerabilities, ensuring MaeveX remains safeguarded against the latest security threats and maintains operational integrity.
- **Syslog:** Forward audit logs to a central Syslog server to monitor and record device and user activity.

Why choose MaeveX for security?

Matrox MaeveX encoders and decoders maintain the security of your AV over IP systems in surveillance and monitoring environments. Embracing a multi-layered security approach, MaeveX protects your critical data from various threats. Rely on MaeveX to uphold the integrity and continuous operation of your crucial surveillance and monitoring systems.

To find out more, visit:

[Matrox MaeveX 6100 Series ▶](#)

[Matrox MaeveX 7100 Series ▶](#)

Contact Matrox Video

Montreal Headquarters: 1-800-361-4903 (North America), 514-822-6364 (Worldwide) | video@matrox.com

London Office: +44 (1895) 827300

Munich Office: +49 89 62170-444

