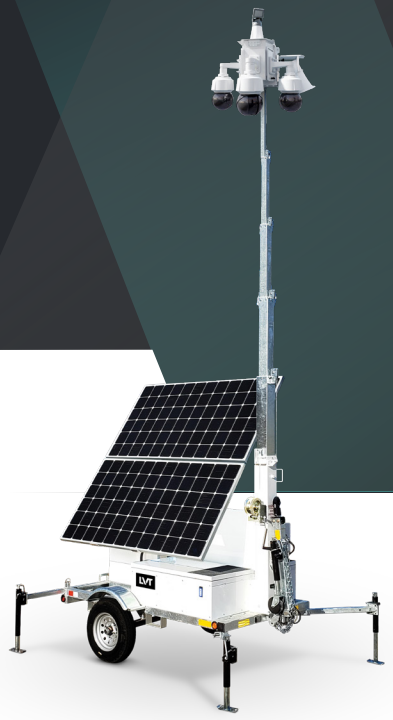
SECURE BY DESIGN



At LVT, we believe that cutting-edge security technology doesn't have to come at the expense of your privacy. Our mission is to make the world safer and more secure—and that includes data security and privacy.

LVT HAS A SOC 2 TYPE 2 REPORT

» SOC 2 Type 2 is a third-party audit report that assesses the design and effectiveness of an organization's security controls. SOC 2 independently validates a mature and reliable security position. LVT undergoes a SOC 2 Type 2 audit annually, conducted by a certified independent third-party auditor, which verifies that our controls are not only designed appropriately, but are consistently operating effectively over time.

WHAT MAKES LVT CYBERSECURITY DIFFERENT?

» **Secure edge-to-cloud communication:** LVT utilizes secure, private cellular networks for communication between the hardware units and the cloud platform. The edge device units are encrypted and securely overwrite previous data after decommissioning, ensuring data privacy at the source.

» **Security in the software development lifecycle (SDLC):** Security is built-in. Our dedicated InfoSec team ensures that security is integrated into our SDLC, including mandatory peer code reviews, secure code training for developers, a bug bounty program, and annual, independent penetration testing against our web application and mobile security unit.

» **Security risk management:** LVT maintains a comprehensive security risk management process that includes participation from executive leadership.

» **Personnel security and vetting:** All employees and contractors undergo a rigid background check prior to being granted access to customer data.

» **Access governance and control:** With LVT, you control which features and data your people have access to. Customers can use single sign-on (SSO) with multi-factor authentication (MFA) to further control and secure access to their environments.

» **User access reviews:** We manage internal access, reviewing employee access to customer environments on a quarterly basis.

» **Encryption in-transit and at-rest**: Data is encrypted in transit using strong protocols like TLS 1.2+ and at rest using industry-standard AES-256 encryption. Customer passwords are also securely hashed and salted.