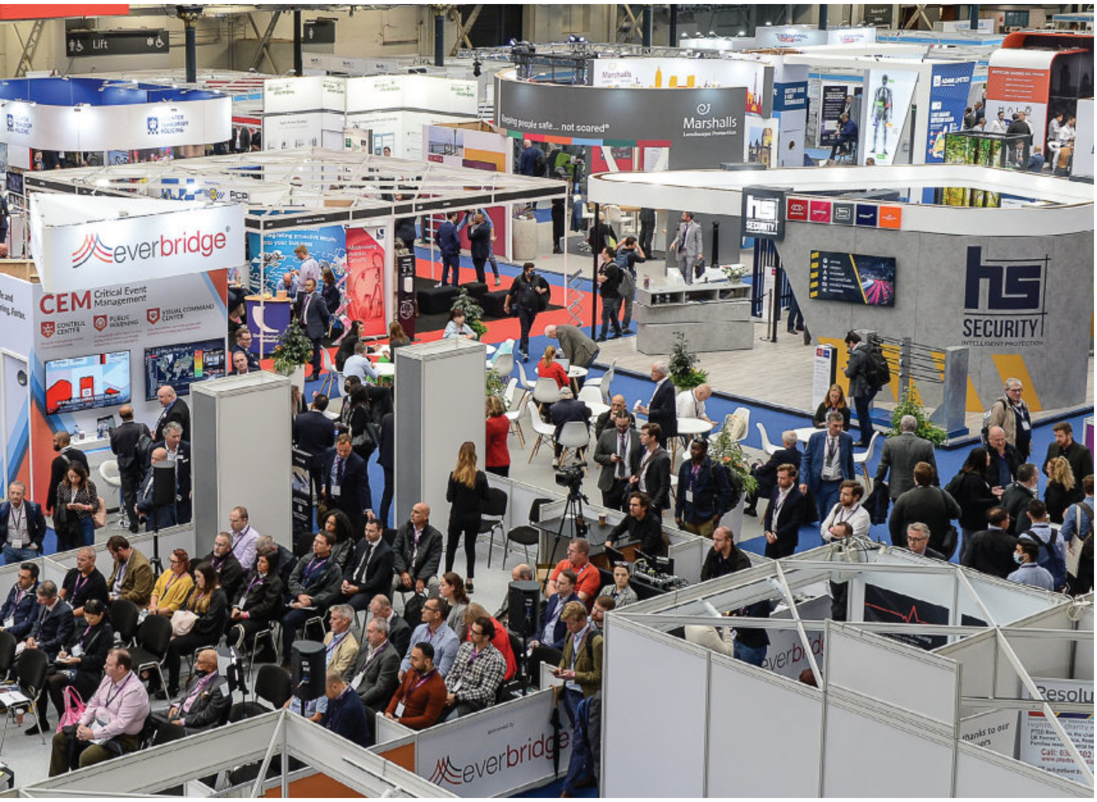

Image Credit: International Security Expo

worrying for industries most vulnerable to data breaches, such as banks and finance, healthcare, IT and tech centres.

To protect against such threats, 3M Privacy Solutions has developed Privacy Filters which prevents views from side lookers by blocking 60° on either side of a screen. The product has a breadth of range, and is usable on monitors up to 49". It has also been designed to be securely and effortlessly attached for ease of use and to prevent it being left behind. The product does not affect workflow as the image clarity remains crisp and clear.

Control the drone to control the threat

Drone and counter-drone technologies were a focus at the show. Martin Broomhead, UK general manager at D-Fend Solutions, discussed the D-Fend's counter-drone technology, which is based on a 'control the drone to control the threat' strategy and is ideal for sensitive scenarios.

Broomhead highlighted the wide-ranging nature of drone threats: smuggling contraband into prisons, disrupting events, posing dangers to planes and striking government buildings. Users can range from "misguided individuals wanting their YouTube moment", to state actors.

"They all use commercially available drones, from small, short-range drones, right through to the large drones capable of carrying a payload of more than 15 kilos and able to fly long distances. They are easily available and represent a clear and present threat."

Broomhead discussed some of the limitations of conventional counter-drone technologies, which can struggle in sensitive areas. Jamming solutions may affect legitimate communication signals, such as emergency services, and operators can regain control of the drone once the jamming ceases. Acoustic solutions are often ineffective in noisy environments, optical solutions mainly require line of sight and radar will struggle in a built-up environment and often result in false positives.

Counter-drone measures must focus on the risk: the most dangerous drones, and assess and prioritise detection and mitigation efforts.

"Security and law enforcement agencies want to know what the drone has done, the make and model, the origins of the pilot, and look at the recording the drone is making. The system needs to be able to do that. You can't just jam a drone and drop it out of the sky," said Broomhead.

He explained that D-Fend's EnforceAir solution detects, tracks and identifies drones and pilots without the pilot's knowledge. In this mode it is passive, with no transmission. When it detects a rogue drone, it transmits a signal that takes control without interfering with authorised drones and signals. The pilot loses control of operation, including video and telemetry information. The drone can then be reprogrammed and rerouted to a safe landing site, avoiding or minimising disruption and collateral damage.

The system enables fast and accurate detection and does not require a line of sight, so can operate in dense environments. It offers multiple deployment options and operational flexibility.

Broomhead said that the system is constantly evolving to stay ahead of the threat and is updated at least every three months, with 50% of the company's staff engaged in R&D.

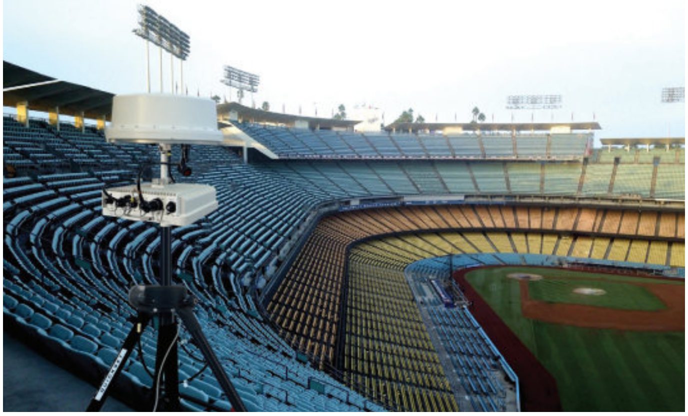

Image Credit: D-Fend Solutions