



CRIME, NOT ART:

Preventing vandalism and crime on public transport

MAKE THE
WORLD SEE



Managing vandalism

Ensuring the safety of passengers using public transport is a top priority for all transport leaders.

Mostly, this focuses on reducing violent and aggressive behavior that threatens passengers and staff. However, managing vandalism and deterring anti-social behavior is just as important in providing a safe and pleasant environment.

Public transport operators want to deliver the best service and performance for passengers. Graffiti and vandalism give the opposite impression. It can make the public believe that the area is neglected.

Worse still, graffiti can lead to further crime. It can be an indicator of vulnerabilities that criminals may exploit to commit theft,

harm other passengers, and sabotage transport services. Plus, [research](#) has found that people become more disobedient in environments with high graffiti levels — trespassing, littering, and stealing all increase in these areas. Graffiti may also be used by street gangs to mark out territories with specific ‘tags’ or gang markings. Transport organizations may find themselves caught in the middle of a turf war, experiencing all of the crimes that often accompany this.

Graffiti can be an indicator of vulnerabilities that criminals may exploit to commit theft, harm other passengers, and sabotage transport services.

Widespread consequences

There is also the financial cost to consider. Destroyed equipment, smashed windows, and clearing graffiti all cost transport organizations money and resources that could be used to improve services.

In Europe, around €17 million per year, or up to 1% of operational costs are currently dedicated to cleaning up graffiti on trains alone. In the UK, Network Rail spends £3.5 million every year on clearing offensive graffiti. That doesn't include the cost of cleaning vandalism in stations, tunnels, bridges, viaducts, and more. Many operators are reporting that their costs are rising.

Costs are not just linked to graffiti clean-up, but also any damage caused through forced entry, spilled chemicals, and further vandalism and crime. There's also operational downtime and service disruptions, the costs of investigating vandalism, and increased measures to prevent further crime.

Downtime can be a significant issue along busy routes and during peak times. Many public transport operators adopt a zero-tolerance policy towards defaced vehicles, in order to prevent graffiti inciting further crime or negatively impacting passengers' perceptions. In one such case, graffiti impacted the delivery of new trains into service as they (as well as existing rolling stock) were defaced.

However, taking trains and buses out of service can leave operators short of rolling stock, struggling to meet their usual service levels, and inconveniencing passengers who regularly rely on the route. For example, a West Lothian evening bus service had to be canceled after windows were smashed on buses along the route.

The danger to passengers, staff, and vandals themselves, cannot be underestimated. Smashed windows, sprayed windscreens, or broken equipment will put passengers, staff, and drivers at risk (particularly if the vandalism occurs during transit). Trespassing also puts vandals at risk, especially when traversing railway tracks or climbing on bridges and walls to spray graffiti.

Finally, a loss of passenger trust in the reliability and security of transport services will impact an organization long after the vandalism occurred.



Current ways to protect assets

It is evident that public transport leaders must work hard to deter vandalism. Consequently, many public transport networks have become highly effective at protecting themselves from traditional vandalism tactics. Yet, tactics — and targets — are changing.

Protecting vehicles and trains in depots is quite straightforward. There are a variety of measures that can prevent intrusion and aid with investigations post-event. These include perimeter defenses like fence sensors, intrusion detection through buried detection sensors, and video surveillance with analytics.

However, an increasing number of operators are now reporting attacks that occur during operating service. This is a concerning trend across the globe that's putting staff and passengers at significant risk. Often, a gang of graffiti sprayers will board a train whilst in service, threaten staff and passengers, pull the emergency brake to stop the train, and then vandalize it. They are also becoming increasingly violent, assaulting any staff member or passenger who gets in their way — and destroying driver cabins and surveillance cameras.

These gangs are often very well organized and they often repeat their offenses (causing ongoing damages to public transport systems). They will research a potential target beforehand to understand its weak points, and they may steal keys and uniforms to gain access to a vehicle. Each gang member is given a specific role so the group can carry out the hit as quickly as possible. Often, they are linked to other crimes, including theft to fund graffiti spraying.

Combatting the rising prevalence of graffiti on public transport is top-of-mind for many public transport leaders. Indeed, when looking at future video analytics use cases in 2018, detecting graffiti was a top priority for 70% of public transport leaders.



Next-generation protection

In the face of such attacks, public transport operators must find more efficient strategies for dealing with new and repeat offenders.

This is where forward-thinking video surveillance strategies, coupled with advanced analytics and other connected devices can boost security, spot patterns, and deter vandalism. Indeed, [40%](#) of transport leaders are looking at connecting their video technologies with additional technologies like the Internet of Things by 2023 — and 23% intend to invest in an advanced technology platform to connect video to other systems.



Broadly, robust protection encompasses four areas:

-  Investing in the right technology to detect and reduce weaknesses and provide continuous feedback to improve security processes.
-  Incident reporting and evaluation that provides evidence for investigations and raises awareness of the severity of vandalism among law enforcement and local authorities.
-  Closer cooperation with local authorities and law enforcement to track recurring crimes, identify gang members, and improve the evidence presented to a court to convict vandals.
-  Wider collaboration across public transport organizations, Government, law enforcement, and even internationally, to exchange information on vandalism gangs, and promote gold-standard security practices.

When considering implementing next-generation security solutions, it's worth referring back to this list to understand how your chosen security technology meets each of these areas.

Five technologies to secure transport

Going a step further, here are some of the technologies that public transport leaders are currently using to protect their vehicles in depots and in transit.



01 AI-powered surveillance: your eyes on the ground

Vandals can target a wide range of different areas to graffiti, so an extensive surveillance system is needed to avoid any blind spots. However, that's easier said than done, especially on vehicles or trains that travel long distances and cannot always relay video footage back to control rooms.

Next-generation video surveillance cameras are able to process some footage at the edge, to reduce bandwidth requirements for sending video data back to a control room. Some automation can also be done through in-built analytics in the camera device itself or by using edge/IoT devices to run the analytics. Using edge/IoT solutions for running video analytics offers greater flexibility in the type of analytics that can be run, whereas in-camera analytics can be more cost-effective as there are fewer overheads required for the analytics compute power.

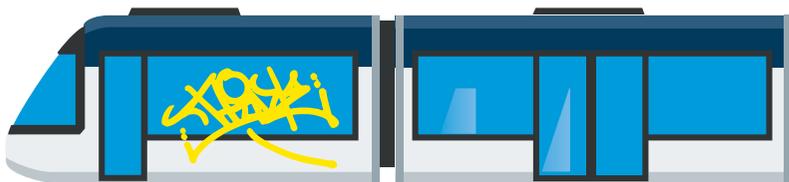
Object detection, thermal imaging, loitering detection, and audio analysis can all inform operators of suspicious behavior, left luggage,

known vandals, or sudden movement in a restricted area.

Likewise, operators can gather greater contextual data to understand what's happening on the ground in depots, stations, vehicles, and trains. Automatic number plate recognition (ANPR) can flag suspicious vehicles or unauthorized parking.

In fact, artificial intelligence (AI) applied to video analytics is now so advanced (thanks to deep learning) that it can detect and classify 'normal' behavior versus aggressive and threatening actions (behavior recognition).

Collectively, with these insights relayed back to operators, situational awareness and response times will improve. Additionally, all of these processes are done through automation, freeing up operators from constantly monitoring video feeds (which can cause video fatigue). Instead, their role becomes much more proactive and strategic.



Scan to watch webinar,
or use [this link](#).



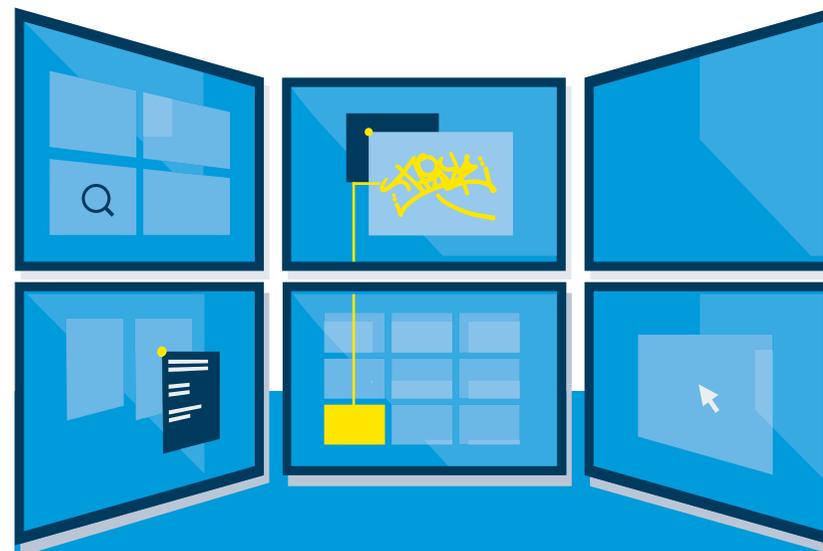
02 Deter and detect: get on the scene ASAP

AI is advanced enough now that it can recognize graffiti. It can automatically alert operators to graffiti being sprayed or written inside and outside of a vehicle, as soon as the first paint or pen marks hit a surface. An alert, specific to when graffiti is being written, notifies operators and camera footage can be brought up for visual confirmation and to direct ground staff to the offender.

Alongside video surveillance, other sensors can alert operators to potential trespassing and vandalism. Intrusion panels, infrared barriers, LiDar (light detection and ranging), and motion detection can help to detect movement and activity, even in difficult weather or dark conditions. Using such technology in highly restricted and dangerous areas, like underground tunnels, can help to reduce risk to passengers and staff, and also prevent vandals from putting themselves in extreme danger.

Camera and device tampering analytics can also tell operators when a surveillance system is being sabotaged. Similarly, investing in these systems tends to reduce the total cost of ownership by automating the maintenance requirements for camera devices and video sources. The AI-based video quality monitoring system will spot degraded video sources automatically among thousands of cameras and generate periodic maintenance reports. Thereby reducing the time spent checking each individual video source manually. This at the same time also protects the investment that has been made for advance AI video analytics because in the end, the system can't detect what it can't see!

Ultimately, these alerts, when combined with video surveillance and analytics will ensure that on-the-ground security staff gets to a potential incident rapidly — to stop vandals and catch them red-handed, or to immediately investigate an event before physical evidence is lost.



AI can automatically alert operators to graffiti being sprayed or written inside and outside of a vehicle, as soon as the first paint or pen marks hit a surface.



03 Access control and intrusion detection: keep unauthorized people out

Access control technology will keep unwanted people out of depots, stations, and, in some cases, railway lines. Perimeter control and detection will detect if someone gains access to a site. Integration with video surveillance can then automatically pan cameras (or even dispatch video drones) to a potential entry point to track intruders (and direct security personnel to their location), gather evidence, or rule out false positives.

Meanwhile, access control systems will ensure only authorized personnel gain access to specific areas. This is particularly relevant for restricted areas like control rooms and offices. There are many different access control solutions to suit different staff and organization needs. In some cases, access cards will be suitable (rail station staff, for example, where it can double as an identity card for passengers). In others, mobile

credentials may suit (for engineers working along a route or railway line).

Whereas access control systems are mainly there for operational efficiency during operational hours, intrusion detection systems are considered as an access control system used during closing hours where operators can arm and disarm protected areas preventing and detecting break-in. Intrusion detection sensors like glass break sensors, seismic sensors, PIR sensors and magnetic contacts provide the first line of defense for a facility during closing hours. When combined with video you get immediate visual confirmation and situational awareness plus the option to automate access control command at the same time.

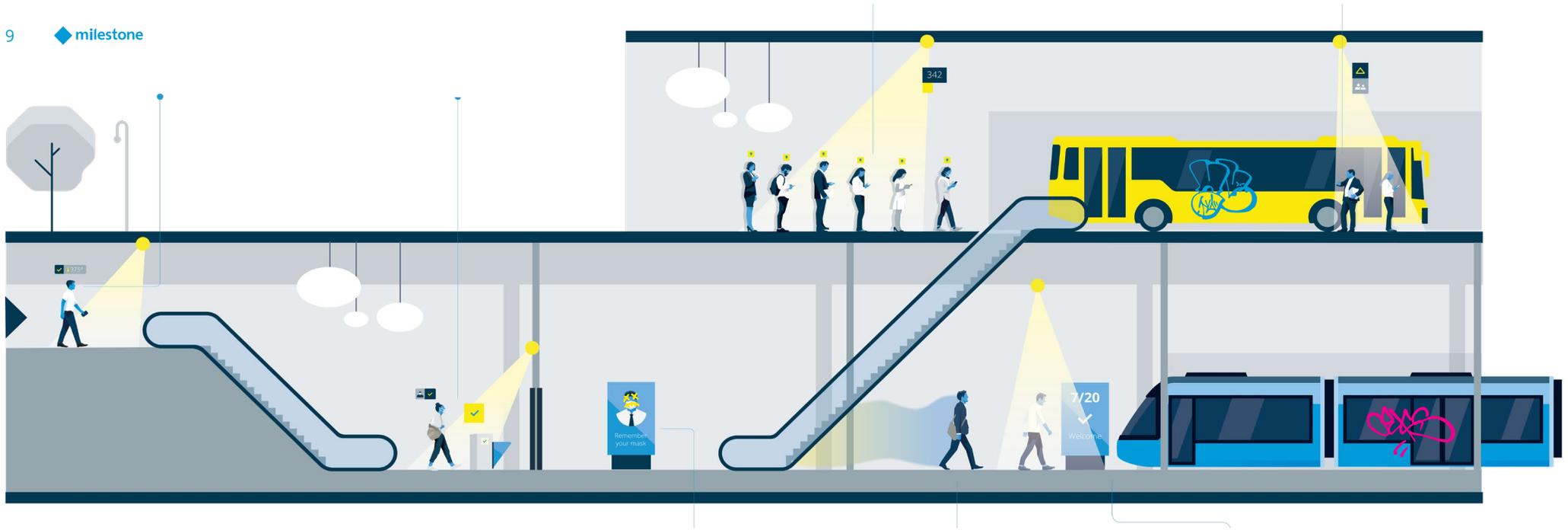
Scenario: During break-in the intrusion system detects a burglary. The video management

system offers the operator visual confirmation and situational awareness of the incident. At the same time the video management platform controls the doors closing and locking them in case a stolen badge was used.

Integration with video surveillance can also monitor tailgating to ensure nobody can access a site by following closely behind an authorized individual. Integrating visitor and contractor logs will help operators understand who should be near a vehicle and on-site (and where). Access control systems will ensure operation efficiency during operational hours, and outside of this, intrusion detection systems will protect areas and detect break-ins. Sensors that can detect glass breaking (like a window), seismic activity like digging under a perimeter, and infrared sensors that can detect a human moving around a site, are the first line of defense for a facility during closed

hours. When combined with video, it gives an immediate visual confirmation and situational awareness of an event unfolding — plus the option to automate access control commands at the same time.





04 A VMS: technology to consolidate information

The nature of public transport means that there are many different video, sensor, audio and other data feeds coming into a control room at any one time. There's video footage from sites, along routes and railways, body-worn camera footage from conductors and drivers, ANPR footage, plus sensor data from access and perimeter controls.

Furthermore, many public transport assets require large-scale surveillance solutions spread over a wide area. There are likely several different types of asset to be monitored simultaneously (stations, depots, warehouses, roads, railway lines, offices, storage buildings, and more). These will require different solutions on-site.

For operators to understand everything that's occurring, an intuitive video management system (VMS) is needed that consolidates and makes sense of incoming data. Automation can carry out much of the day-to-day monitoring of such feeds, giving operators more time to focus on only the events that need their attention and action. Alarms will alert operators to investigate footage that requires their input. Even announcements can be carried out automatically when a VMS integrates with digital signage and tannoy systems — when someone is acting suspiciously near a railway track, a warning of the dangers sounded through a tannoy could be enough to deter them.

Establishing incident patterns is central to long-term vandalism prevention. Moreover, data insights can inform security staffing, establish new processes, make the case for further technology investment, and other strategizing. Even the seasonality of graffiti-tagging can be investigated so security teams can pre-empt increases, reacting before graffiti occurs instead of afterward.

Of course, if such preventative measures fail to stop an act of vandalism from occurring, the VMS will provide valuable evidence for investigations, prosecution, and future deterrent measures.

Consolidating information can take two forms: real-time or via periodic reporting. With real-time dashboards, operators can quickly make decisions based on immediate insights and event notifications. For instance, an alert of graffiti being sprayed on a train can enable operators to apprehend the vandals before they are able to deface any more of the carriage.

Meanwhile, periodic reporting offers longer-term insights and trends that can help with planning security patrols and other defenses. Weekly status reports about events can also track the results of implementing different preventative measures.



05 Investigation: gather evidence and convict

As for investigating post-event, your VMS will simplify evidence tracking, collection, and documentation. Video and sensor data, along with visitor and contractor logs, and other key information, can be easily collected and shared with the relevant authorities. Camera tracking, object and vehicle recognition, heat mapping, video, and audio enhancement, and other video analytics can all assist in identifying vandals and license plates, for law enforcement to then track down and prosecute.



IN ACTION:

Utah Transport

The Utah Transit Authority (UTA) provides transport to 120,000 passengers a day through its fixed bus routes, commuter rail trains, light rail trains, paratransit buses, and vanpool services (rideshare). As part of the development of a new transit line, UTA wanted to improve its surveillance system to accommodate a 500-camera expansion and futureproof its system. It turned to Milestone XProtect® as a more flexible and efficient VMS compared to its old video system.

XProtect® married two critical components: a centralized system and a lot of diversity in its deployment. The open platform ensures UTA isn't tied to a single technology or vendor, allowing it to use best-in-breed solutions for each site and route.

After switching to XProtect®, improvements in video quality have made it easier to monitor and investigate events. Evidence Lock allows for the extension of the retention time for video recordings from selected cameras (to be used for further investigation and prosecution). Encrypted video footage has watermarks that prove the authenticity of footage for presentation in court. This has helped local police to follow up on vandalism and crimes and even recoup damages.

The system has also been used to prevent serious incidents. When a driver failed to report his truck stalled on a train track, the incident was observed in the VMS by a UTA technician who notified rail authorities. In that instance, Milestone helped avert a serious and potentially life-threatening accident.

Beyond Security

As well as the security aspect, intelligent video technologies can be leveraged for a number of value-added processes that'll benefit your wider organization.



Crowd management:

video analytics can detect if a crowd is suddenly forming either due to demand or potential anti-social behavior. With the former, people can be redirected to other areas to reduce bottlenecks and crowding in peak times. With the latter, tannoy and on-site staff can encourage groups to break apart.



Occupancy measurement:

cameras can measure occupancy continuously and evaluate levels in real-time to take appropriate actions. For instance, where a platform's safe capacity is about to be exceeded, passengers can be redirected to alternative locations using integrated digital signage. Where a location regularly exceeds safe capacities, decision-makers can be informed to then decide whether to expand an area.



Public health:

current social distancing and public health measures can be supported with video analytics that detects when people aren't wearing face coverings or are standing too close to others. Digital signage and tannoy can be used to remind people of public health requirements.



Smart parking management:

license plate recognition can allow vehicles to enter and exit a car park or loading bay. Tickets can be automatically issued and fares paid based on a vehicle's credentials. Parking can also be monitored and drivers directed to the nearest space (or redirected elsewhere when there are no spaces available). Management can get an overview of occupancy rates at different times to inform future parking strategies. Research shows that in 2022, intend to invest in smart parking video solutions.



Passenger monitoring:

video surveillance can detect passenger emergencies like someone falling over or being mugged. Staff can then respond quickly to any incidents. Passengers who need extra care (if in a wheelchair, for example) can also be detected and station staff alerted.



Cleaning support:

video analytics can monitor footfall and facility usage to determine optimum cleaning schedules. If somewhere suddenly has an increase in use, cleaning attendants can be informed to pay it an extra visit. Likewise, waste and contamination can be automatically detected and removed. This helps to contribute to a clean and pleasant travel experience.

The journey towards autonomous public transport

The future of public transport will soon be dominated by autonomous solutions. Self-driving buses and trains are a near-reality with trials ongoing across Europe, including in [Cambridge, UK](#), and [Hamburg, Germany](#). At the same time, stations and depots will be increasingly unmanned, and this can have significant safety and crime implications. Video analytics will be vital in protecting passengers and deterring vandalism at unmanned stations, depots, and vehicles.

Without staff on-board or on-site, real-time analytics will need to immediately alert operators to any emergencies or crimes. For example, aggressive or suspicious behavior (like tailing a passenger through a concourse) can be flagged for operators to follow up. Emergencies like someone falling or fire and smoke detection can immediately inform the emergency services. Plus, crimes like anti-social behavior and vandalism can be automatically detected and the authorities alerted.

Detecting graffiti becomes all the more critical when you consider that it [may confuse](#) self-driving vehicle systems when it appears on something like a street sign. Such an event could cause the vehicle to malfunction or misread a sign and crash. That said, some predict that in the future, video footage from [self-driving vehicles](#) themselves will be used to detect graffiti on roads and in tunnels and direct local authorities to clean it up.

Extra considerations

Once a new technology is implemented, it's vital to keep it updated ready for the latest threats and crime trends. Simultaneously, most organizations will have a mix of new and existing technology to keep updated and working effectively.

However, this can be a challenge due to the complexity and scale of most public transport security systems (and, therefore, the cost that goes with it).

An open VMS is key in this situation. It allows you to make more choices in the technology used across your public transport network and can adapt to future needs and solutions. Open platforms can integrate with existing infrastructure as well.

It's worth noting that there are many fast-moving developments with the Internet of Things (IoT), AI, the cloud, edge computing, 5G, and other emerging technologies. Futureproofing your investment is critical because it ensures a long-term return on investment. It will also keep your security system updated against new kinds of crime and vandalism while offering the option to implement new cameras, sensors, and features.



How Milestone can help

Milestone offers a range of solutions adapted to different public transport requirements.

XProtect®

this market-leading VMS unites all the puzzle pieces for video surveillance together, combining video footage with sensor data, access control, visitor logs, and more. It then facilitates advanced video analytics like fire detection, vehicle recognition, and object classification to protect all assets in a public transport network. In one case, a municipality was able to reduce vandalism by 90% with XProtect®.

As well as on-premise, XProtect® is available as a cloud-based solution through AWS. This suits installations where scalability and elastic computing is a priority.

XProtect® Smart Client

Milestone's powerful, all-round desktop application for operators to detect and respond to events quickly, or find and export evidence material. Operators can track and understand everything occurring across a public transport network at-a-glance, resulting in greater situational awareness and contextual understanding of events. Alarms can be automatically triggered based on anomalies detected by cameras.

Milestone Smart Map

a map function embedded in the XProtect® Smart Client that visualizes the elements of a surveillance system with geographical, accurate, real-world imagery, audio and real-time alerts. This offers extra context and visual representation for operators to really grasp what's happening on the ground.

XProtect® Rapid Review

an intelligent AI video analytics solution that enables operators to quickly review and analyze forensic video content to find what they are looking for, fast.

MILESTONE INTERCONNECT™

Milestone Interconnect enables security teams to centrally monitor and connect multiple sites spread across a region. This makes it ideal for distributed installations where many different sites and risks need to be managed — like a train station, embankments, railway tracks, level crossings, and depots.

XProtect® Access

this allows teams to connect their access control system directly to XProtect® so all video and access systems are viewable and manageable from a single interface. This also provides visual verification of access control events and alerts.

Milestone Marketplace

find and compare different hardware, software, and solution service partners, verified by Milestone, to build the exact security solution your organization needs today — and tomorrow.



Go Beyond

To truly meet the needs and expectations of modern-day passengers, surveillance systems need to go beyond simply responding to an act of vandalism.

Instead, they need to proactively deter vandals, track and respond to graffiti gangs, and work with law enforcement on long-term prevention.

With next-generation video solutions, transport leaders can make it clear to vandals that their tags, dubs, and blockbusters are unwelcome on our roads and railways.





To discuss your organization's unique requirements in more detail and how Milestone can improve your security, contact:

Crime, not art: Preventing vandalism and crime on public transport



Scan to watch webinar,
or use [this link](#).

Milestone Systems A/S Headquarters
Banemarksvej 50 C
DK-2605 Brøndby
Denmark
Telephone: +45 88 300 300

Any questions?

Please reach out to us [here](#) if you have any questions or inquiries.



For more information visit:
milestonesys.com