



QUANTIFYING THE VALUE OF Proactive Site Security

While trespassing may seem like a minor nuisance, failing to proactively address breaches exposes businesses to severe financial loss and compounding security risks; therefore, investing in intelligent deterrence measures is a critical strategy for long-term financial protection.

Virtually every enterprise—a critical infrastructure power plant, a sprawling logistics railyard, a commercial office building, or a retail footprint—faces a shared set of security challenges. Decision-makers must constantly balance how to secure physical spaces, mitigate liabilities, deploy guard forces effectively, and deter crime consistently. When successful, these efforts provide tremendous value,

preventing organizations from bleeding financially in the wake of a criminal incident.

The question is: **How do you quantify the financial impact of a non-event?** If an organization invests heavily in a sophisticated security ecosystem that successfully deters a trespasser, how does leadership accurately measure the losses that never occurred? How do you understand the ROI in this situation?

Historically, legacy security measures have struggled to truly prevent trespassing, leaving companies stuck in a costly, reactive cycle of responding to damages. To achieve true monetary and physical protection, businesses must transition to a proactive model rooted in intelligent site coverage.



This whitepaper provides a data-driven framework for security directors and executive leadership to calculate the true return on security investment. Specifically, we will explore:

- » **The true cost of trespassing incidents:** How minor trespassing incidents can slowly erode business revenue across industries.
- » **Escalating crime risk:** The direct correlation between unaddressed trespassing and future crime risks.
- » **The downfalls of legacy security:** Why traditional, reactive security models fail to deter modern threats.
- » **The proactive solution:** How to implement intelligent, measurable deterrence strategies that safeguard assets and actively defend the bottom line.

BUSINESSES FEEL THE IMMEDIATE IMPACTS OF TRESPASSING

Trespassing is unlawful or unpermitted entry onto another person or entity's property. Dark or poorly-lit, unstaffed, after-hours, and remote sites are all susceptible to trespassing, often causing unforeseen issues. Different industries have varying challenges when it comes to trespassing and damages.

According to the Federal Railroad Administration, **trespassing is the leading cause of rail-related deaths** in the United States with over 500 fatalities annually.

Construction and Infrastructure

Safety hazards can put individuals who trespass on construction sites at risk, and as a result, create expensive liabilities for the business. Unsecured equipment or materials, unfinished electrical work, uneven grounds, and



more pose risks to those who are unauthorized to be on a construction site. Trespassing incidents can also cause significant project delays by causing damage, vandalizing, stealing tools and materials, and tampering with expensive construction equipment.

Railroads and Transportation

According to the [Federal Railroad Administration](#), trespassing is the leading cause of rail-related deaths in the United States with over 500 fatalities annually. The number of trespassing incidents far outweighs the number of fatalities which means that there is an even higher potential for trespasser accidents

Trespassing also creates operational disruptions for railways. Cargo theft and other criminal incidents create delays in shipments that can impact the entire supply chain, leading to significant costs for businesses.

Retail, Commercial Real Estate, Logistics

Trespassing in retail and commercial spaces typically goes



Vandalism, burglary, and theft from parking lots, warehouses, loading docks, and other facilities **cost businesses \$45 billion in 2024 alone.**

hand-in-hand with property damage and theft. Vandalism, burglary, and theft from parking lots, warehouses, loading docks, and other facilities cost businesses [\\$45 billion in 2024](#) alone. According to a [study](#) released by the National Retail Federation (NRF) and Loss Prevention Research Council (LPRC) sponsored by Sensormatic, external shoplifting and merchandise theft incidents increased by 19% from 2023 to 2024.

INDUSTRY-WIDE PAIN POINTS

Across all industries, the pain points are consistent:

- » **Operational downtime:** The costs associated with operations halting are serious and significant. To maintain consistent revenue, operations must continue without interruption. Trespassing incidents are a major barrier in these instances. According to a [global macroeconomic study](#) by the World Bank, operational and logistical infrastructure halts account for over \$107 billion in annual losses.
- » **Cost of physical repairs:** Fencing, glass replacement, graffiti removal, equipment/machinery repair or replacement, and inventory damage or replacement can cost anywhere from tens of thousands, to hundreds of thousands, to millions of dollars in repairs. To replace a single [damaged HVAC unit](#) costs more than \$10,000. To [clean up graffiti](#), it costs \$300–\$1,000 or more per job. [Storefront widow replacement](#) costs \$800–\$1,500; big jobs can cost \$5,000–\$20,000.
- » **Insurance premiums:** Insurance premiums for businesses can skyrocket due to frequent incidents.

According to industry data, businesses can see a [5%–25%](#) increase after a single claim.

- » **Time lost to reporting:** When incidents are frequent, businesses lose hours of productive time reviewing footage and filing police reports.

Intangible Value of Guarding Against Trespassers

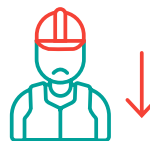
Not every value can be quantified in a number, but these soft factors influence overall perceived business value:

- » **Brand and reputation:** A security breach can destroy customer trust and loyalty across industries. One incident can have major impacts on your bottom line.
- » **Employee safety and morale:** [Employees who feel safe in their workplace](#) are more productive and less likely to quit. It is estimated that the quick service restaurant industry has an employee turnover rate of 144% every month, up from 135% in 2019, and a [quitting rate of 5.7%](#). Investing in an effective deterrence system can offset the high costs associated with employee turnover and training.
- » **Compliance costs:** In state and federal sectors, failing to prevent trespassing can result in major government fines. The value of deterrence is simply the cost of avoiding the fine.

TRESPASSERS



BRAND REPUTATION



EMPLOYEE SAFETY AND MORALE



COMPLIANCE COSTS



FROM IMMEDIATE IMPACT TO FUTURE RISK

While trespassing can seem like a victimless crime, it can act as a gateway to further, more serious crimes. What can look like a typical case of trespassing can actually be a type of reconnaissance mission to understand the site better in preparation for a future, higher risk incident—noting guard shifts, security gaps, and response times.

Broken Windows Theory

The [Broken Windows Theory](#) was developed by criminologists in the 1980s to describe the phenomenon that visible evidence of disorder in a neighborhood—like broken windows, graffiti, illegal dumping—encourages more crime and disorder. Unaddressed trespassing signals a soft target to future trespassers, leaving the door open for more insidious and costly future crimes.

Attractive Nuisance

[Attractive nuisances](#) are conditions on your property or site that draw trespassers. The biggest issue that arises with attractive nuisance is the liability that inevitably arises when someone gets hurt on your property, even if they were trespassing in the first place. Construction sites are common places for attractive nuisances—enticing machinery left unattended, surfaces to climb, man-made ditches, and dirt piles are all potential hazards for trespassers. Failing to secure sites against trespassers can leave businesses vulnerable to lawsuits and legal liabilities which can delay projects and be very costly in the long run.

Common Breach Vulnerabilities

The most common examples of security breaches are much less sophisticated than you might imagine. Trespassers often exploit the human factor of physical security to gain entrance to an unauthorized site. This could look like [tailgating](#): a trespasser follows an authorized person through a secure entrance before the door closes and locks to gain access to a site. They may also piggyback by entering with a group of authorized people, flying under the radar.

Trespassers may get more technical in their effort to gain access by picking cheap locks, using a stolen access card, or disabling outdated security systems. When there are no security safeguards in place, access to a site can be surprisingly simple for a determined trespasser or criminal. Repeat access breaches consist of poor badge-use enforcement, lack of visitor screening, lack of multi-factor access controls, insufficient security measures in the form of cameras, alarms, or deterrents, and distracted or untrained security personnel.

A single physical security breach can lead to a major data breach, operational outage or interruption, and significant damage to the reputation of a business. In 2011, burglars used sledgehammers to break into a [Vodafone exchange center](#) in the UK, proceeded to steal computer equipment and network hardware, and as a result, thousands lost their phone service immediately. In 2025, the infamous [Louvre heist](#) began with a physical security breach when a group of four men used a stolen mechanical lift to gain access to the Galerie d'Apollon through a balcony. They used a disc





cutter to access millions of dollars worth of jewels in a glass case. While the criminals have since been apprehended, the majority of the stolen items have not been recovered and likely never will be. These trespasses escalated into the exploitation of a security gap which caused irreparable consequences.



THE INEFFICIENCY OF LEGACY SECURITY MEASURES

The presence of CCTV cameras and other [legacy security measures](#) are nearly ubiquitous across industries and their effectiveness is waning, if not altogether ineffective. If someone is going to trespass, they're not worried about an outdated security system—they'll forge ahead to do what they want to do. Ineffective crime prevention has desensitized trespassers to consequences, and if there's no consequence or reaction, there's nothing keeping them from a criminal trespass.

The Limitations of Physical Guards

While physical guards will never become obsolete, there are [limitations](#) to a human-only security plan. The high labor costs, including base salaries, overtime, holiday pay, and expensive onboarding due to high employee turnover are difficult to keep up with as a business. Despite the significant financial investment that comes with physical security guards, businesses still face significant coverage gaps because human guards are prone to fatigue, distraction, and physical limitations that create blind spots.

Between hourly wages, benefits, training, and liability insurance, guards are a long-term expense. On the high end, [armed security guards](#) can make more than \$100,000 annually, which is more than you can expect to pay for comprehensive, automated coverage by an AI-driven or automated security system.

Fixed, Legacy CCTV

Relying on outdated static camera systems introduces costly installation and maintenance infrastructure. Rather than deterring the crime to begin with, legacy CCTV systems only provide a look at the scene after the damage has been done.

Decades of criminological data confirm that stand-alone, passive CCTV fails to act as a primary crime deterrent. A comprehensive [40-year meta-analysis](#) published by the

On the high end, [armed security guards](#) can make more than **\$100,000 annually**, which is more than you can expect to pay for comprehensive, coverage by an AI-driven or automated security system.



College of Policing revealed that passive camera systems yield no statistically significant reduction in crime, functioning instead as a purely forensic, post-incident tool.

Static Floodlights

Static floodlights create exposure in specific areas, but lack the intelligence of dynamic spotlights which can make spotting and exposing a criminal a cinch. Static floodlights are too easy to avoid when you're a criminal who's cased the site beforehand.

Signage and Fencing

A "no trespassing" sign only does so much. For a determined trespasser, that will do close to nothing. They cover the bases for liability purposes, but signage does nothing to deter a criminal. Fencing is slightly more effective, but without intelligent perimeter security, a fence can be easily jumped, cut, or bypassed.

False Alarm Fatigue

Legacy security systems often trigger false alarms on property, resulting in alert fatigue among law enforcement and security personnel. This can mean that an actual alarm can be looked over or a response can be delayed, causing a security gap perfect for a trespasser to slip through.

CREATING PROACTIVE FRICTION AND DYNAMIC DETERRENCE

It's clear that now is the time in today's security landscape to move toward active resistance and away from passive recording. To really protect your sites from trespassing, damages, liabilities, and other costly incidents, there's a modern blueprint to follow across industries: intelligent, proactive resistance through dynamic deterrence.

What Does Dynamic Deterrence Look Like?

Dynamic [deterrence](#) is active, responsive, and psychological. It doesn't just sit there; it interacts with the intruder based on their specific actions. It uses technology to create the illusion



that a real human guard is watching them right at that exact moment. Dynamic deterrence employs features like AI talk down, dynamic spotlights, custom strobes, and thermal cameras, among others. Intelligent security systems will filter out unnecessary alerts to eliminate alert fatigue for security personnel. They'll also be able to understand behavior and context to differentiate between real threats and normal activity.

Combat Desensitization with Intelligent Deterrence

y implementing dynamic, personalized, and automated audio or visual warnings to potential intruders, you're eliminating the possibility of a trespasser ignoring a security warning from an outdated system. [AI talk down](#) calls out the intruder by their actions, their clothing, or what they're holding in their hands, and gives the sense that they are being watched by an actual human security guard in real-time.



Alleviating Team Fatigue

Intelligent deterrence filters out unnecessary noise for security teams, freeing up time and attention for more important tasks and operations. When personnel aren't attending to endless false alarms, there's more time to focus on strategic projects, and they're more prepared to act when a legitimate threat arises.

THE ROSI FRAMEWORK: MEASURING THE NON-EVENT

Quantifying the savings of a deterred crime requires shifting from traditional ROI metrics to return on security investment ([ROSI](#)). To calculate the financial losses that never occurred, executive leadership can utilize the following data-driven [framework](#):

$$\text{ROSI} = (\text{ALE} \times \text{Mitigation Rate}) - \text{Cost of Solution} / \text{Cost of Solution}$$

1 Calculate the Annualized Loss Expectancy (ALE)

Before you can measure what you saved, you must calculate your baseline financial exposure without intelligent deterrence.

Single loss expectancy (SLE): The total financial impact of a single trespassing incident (e.g., \$10,000 in stolen tools + \$15,000 in operational downtime delay = \$25,000).

Annual rate of occurrence (ARO): How many times a year this breach historically occurs (e.g., 4 times a year).

ALE = SLE x ARO: (In this scenario, \$25,000 x 4 = \$100,000 historical risk exposure).

2 Apply the Deterrence Mitigation Rate

Legacy systems like CCTV and fencing have a low mitigation rate because they are passive. Dynamic deterrence like AI talk down yields an average 85% to 95% reduction in successful intrusions by stopping them at the perimeter.

If your baseline ALE is \$100,000, and dynamic deterrence stops 90% of incidents, your Prevented Loss Value is \$90,000 annually.

3 Compare Against Solution Cost

If the intelligent security platform costs \$30,000 annually to deploy, your net savings is \$60,000. Your ROSI is 200%. This is how leadership accurately measures the losses that never occurred.





WHERE TO GO FROM HERE: THE LVT SOLUTION

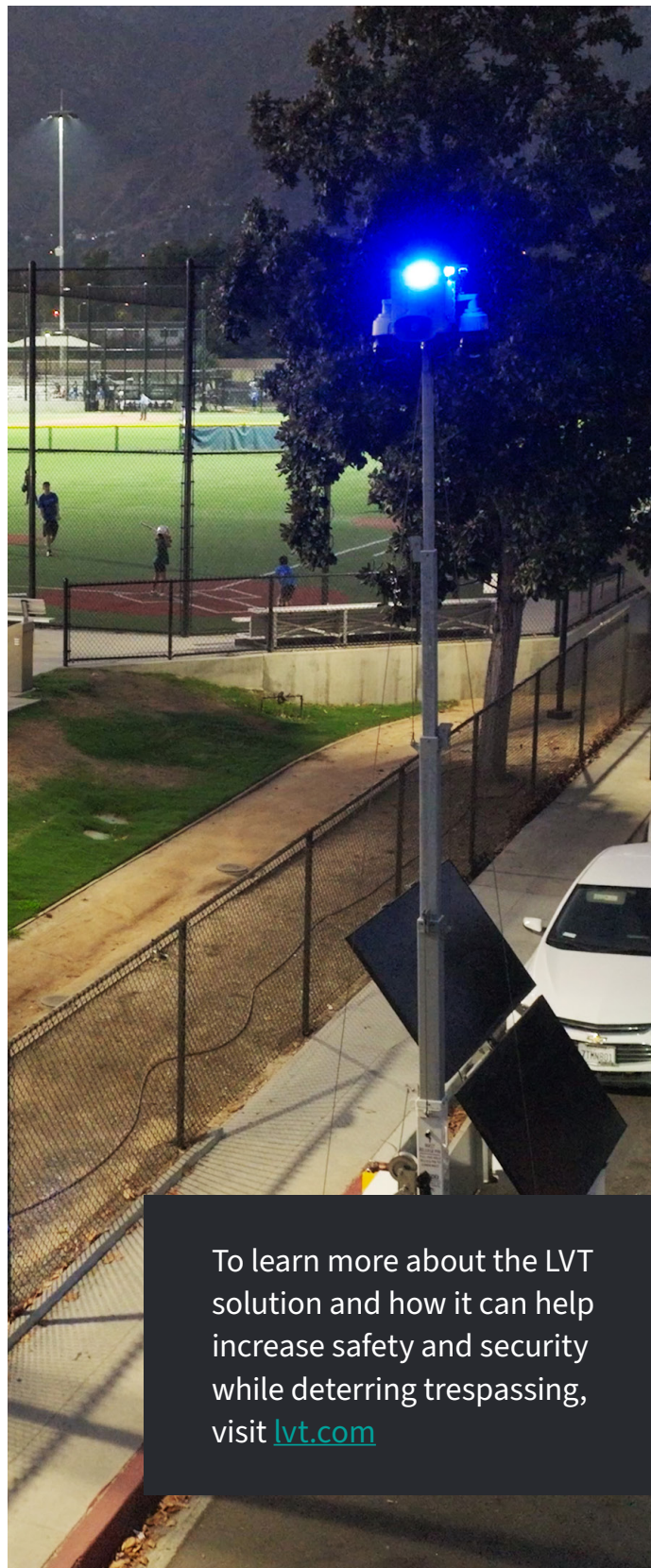
Intelligent deterrence is a profit-preserving tool and competitive advantage in today's security landscape, not a pointless cost for businesses. Rather than spend time and funds on repairing damage that has been done or on liabilities to take care of, security administrators will save on costs when implementing intelligent security solutions.

LVT provides an intelligent, proactive security solution to address trespassing across industries. With a combination of proprietary software and hardware, LVT goes beyond traditional security systems to actively deter crimes. It is a completely mobile, cloud-based security system that does not require external power or internet hookups, can be set up in minutes, and can be deployed anywhere in the world. With the deployment of LVT Units, businesses have seen:

43% reduction in trespassing incidents **70%** decrease in parking lot incidents

Improve criminal incidents and trespassing with personalized audio deterrence, automatically generating real-time verbal warnings. The LVT system engages bad actors the moment a security boundary or loitering timer is triggered. Because it requires zero human intervention, it reacts faster than traditional human responders, allowing security teams to focus on high-priority tasks. LVT's security solution provides 24/7 security at a cost-effective rate, and a fraction of the cost of physical security personnel.

Now is the time to audit existing security systems and see where security gaps exist—don't wait for the next big disaster. Dynamic deterrence stops the cycle of crime by enhancing site security with improved response times and less unwanted behavior, reduces trespassing and loitering that could result in criminal activity, and offloads initial deterrence, overcoming desensitization so teams can focus on what matters most.



To learn more about the LVT solution and how it can help increase safety and security while deterring trespassing, visit lvt.com



SOURCES

- Amarok. (2023, June 14). Commercial property insurance after theft. Amarok Blog. amarok.com/blog/commercial-property-insurance-after-theft/
- Association for Financial Professionals. (2023). How to calculate your return on security investments: FP&A's role. Financial Professionals Resource Hub. afponline.org/ideas-inspiration/topics/articles/Details/how-to-calculate-your-return-on-security-investments-fp-a-s-role
- Atlas AC Repair. (2024, May 24). Commercial HVAC cost. Atlas AC Repair. atlasacrepair.com/cost/commercial-hvac-cost/
- BBC News. (2011, March 4). The technology protecting banks from physical breaches. BBC News. bbc.com/news/technology-12595681
- BBC News. (2024, August 28). The massive cost of retail crime. bbc.com/news/articles/cr5zm7n8ngpo
- Best Offer Glass. (2023, April 11). Storefront window replacement costs business guide. Best Offer Glass. bestofferglass.com/storefront-window-replacement-costs-business-guide/
- European Union Agency for Cybersecurity (ENISA). (2007). Return on security investment [Report]. enisa.europa.eu/sites/default/files/publications/Return%20On%20Security%20Investment.pdf
- Federal Railroad Administration. (n.d.). Trespass prevention. U.S. Department of Transportation. railroads.dot.gov/railroad-safety/divisions/crossing-safety-and-trespass-prevention/trespass-prevention
- Insurica. (2021, October 12). Construction sites and attractive nuisances. Insurica Blog. insurica.com/blog/construction-sites-and-attractive-nuisances/
- L.A. Darling. (2023, February 8). The human and economic cost of retail shrink. L.A. Darling Blog. ladarling.com/blog/human-economic-cost-retail-shrink/
- LiveView Technologies (LVT). (2023). Quick-service restaurants on the front lines of workplace violence [White paper]. LiveView Technologies. lvt.com/resources/quick-service-restaurants-front-lines-workplace-violence
- LiveView Technologies (LVT). (2024a). AI talk-down features for proactive defense. LiveView Technologies. lvt.com/features/ai-talk-down
- LiveView Technologies (LVT). (2024b). Crime deterrence and security automation. LiveView Technologies. lvt.com/crime-deterrence
- LiveView Technologies (LVT). (2024c, March 18). High costs, low coverage: How agentic AI is rewriting the security budget. LiveView Technologies Blog. lvt.com/blog/high-costs-low-coverage-how-agentic-ai-is-rewriting-the-security-budget
- Merriam-Webster. (n.d.). Trespass. In Merriam-Webster.com dictionary. Retrieved June 5, 2026, from merriam-webster.com/dictionary/trespass
- MW Group. (2022). Case studies: Physical security breaches. MW Group. mwgroup.io/case-studies/physical-security-breaches/
- National Retail Federation (NRF). (2025). The impact of retail theft and violence. National Retail Federation Research. nrf.com/research/the-impact-of-retail-theft-violence-2025
- Netwrix, & SANS Institute. (2018). How to calculate return on security investment: The quantitative risk analysis formula [White paper]. SANS Institute
- Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1), 135–159. doi.org/10.1111/1745-9133.12419
- Psychology Today. (n.d.). Broken windows theory. Psychology Today Basics. Retrieved June 5, 2026, from psychologytoday.com/us/basics/broken-windows-theory
- Salazar, M. (2021, August 23). What it's really like to work in the restaurant industry right now, according to fast food statistics. Business Insider. businessinsider.com/what-its-like-to-work-restaurant-industry-fast-food-statistics-2021-8
- SSilbar Security. (2023, November 2). How much do security guards cost? Silbar Security Blog. silbarsecurity.com/blog/how-much-do-security-guards-cost/
- Speedy K's. (2022, November 15). What is the average cost for professional graffiti removal? Speedy K's. speedyks.com/what-is-the-average-cost-for-professional-graffiti-removal/
- Talius. (2023, September 5). The hidden costs of property damage for businesses. Talius Blog. talius.com/post-3/
- World Bank. (2021). Economic and human impacts of global retail security and loss prevention [Research publication]. World Bank Open Knowledge Repository. openknowledge.worldbank.org/entities/publication/2ae571bf-8bcd-5025-b88c-971eab58cb39