vintra

WHITE PAPER

The AI (R)Evolution of Enterprise Security

Introduction

Guards, guns, and gates are the traditional holy grail of traditional physical security plans to protect a company's people, assets, and physical spaces. The beloved three G's used to be sufficient security measures in the enterprise world of yesteryear.

Today, the threats to enterprise workplace safety are more diverse, and have greater consequences both financially and in human form, than ever before. Workplace violence incidents, whether homicide or simple assault, are extremely costly to companies. The numbers, in fact, are astonishing:

- $121 billion in annual losses due to workplace assaults
- Lawsuits associated with workplace violence cost companies an average of $500,000 for out-of-court settlements
- Workplace catastrophes, such as active shooters on campus, have caused publicly-traded companies to lose close to 8% in shareholder value[1]

The reliance on security guards to roam the physical spaces, internally and externally, on a company's premises, is an outdated system rife with inefficiencies. The same can be said of the recent trend in security operations seeking to take advantage of camera networks and technology: central monitoring stations. Here, security operators observe a bank of video screens for hours on end and attempt to recommend actions or respond to alarms in real-time.

Security guards, by definition, are primarily a reactive force. It is only when they can physically see something, or be notified after the incident has happened, that an action can be taken in response. Nationally, there are over 15 million security guards employed in enterprise settings, accounting for $40 billion in wage spend. Let that sink in. In fact, there are more privately employed security guards around the world than police officers.

The typical central monitoring station is staffed by a handful of security operators watching anywhere from 2 - 5 screens at any point. Humans are not built for this kind of sustained focus that the job requires. After only 22 minutes of sustained video review, humans lose up to 95% of visual acuity and experience something akin to "video blindness".[2] One researcher did a study on how well security operators tasked with viewing monitors could detect a person carrying an umbrella on a busy street using differing amounts of monitors. The study found that observers

---

[1] *https://www.ravemobilesafety.com/blog/latest-workplace-violence-statistics*

[2] *http://www.cs.nott.ac.uk/~pszcmg/G64IDS/isd-dissertations-08/nxd07m.pdf*

viewing one, four, six and nine monitors had accuracy detection scores of 85%, 74%, 58% and 53% respectively in identifying the only person on a busy street holding an umbrella.[3]

THE SOLUTION?

Thanks to massive advances in computing power[4] and cutting-edge artificial intelligence (AI) that has blurred the line between fiction and reality, it is possible to implement systemic changes in a security team's operations and focus, reduce wage-spend on security guards, repurpose their time for higher-level work, and transform real-time monitoring into intelligent monitoring with a single cost-effective AI-powered video analytics solution.And what would the expected ROI look like for a solution such as this? Liberty Mutual Insurance estimates that for every $1 invested in workplace safety, $3 or more is saved.[5] In a study of 231 CFO's, it was found that for every $1 spent on improving or upgrading safety, they experienced savings of $4.41 on average. The savings were due to:

- Lower insurance premiums
- Improved productivity
- Reduced costs of training new employees
- Less workplace disruption[6]

Workplace violence is trending upward. In 2005, only 5% of businesses reported experiencing one incident of violence in the five years prior.[7] That number is now up to 27%. In this paper, we'll explore how AI can empower enterprises to better protect their people, assets, and physical spaces.

PROTECTING YOUR PEOPLE

Quality employees are the lifeblood of any successful enterprise. Safety and security go a long way towards retaining and attracting high-level persons in today's uber-competitive market. Catastrophic events, such as an active shooter on campus, are the easiest and most glaring examples for any exec thinking of improving their security system. If a solution saved one life, stopped one shooting, it would easily validate its cost. From 2005 - 2017 42% of active shooter incidents in the United States occurred in places of commerce.[8]

---

[3] *http://www.securitysa.com/article.aspx?pklarticleid=3313*

[4] *https://blog.openai.com/ai-and-compute/*

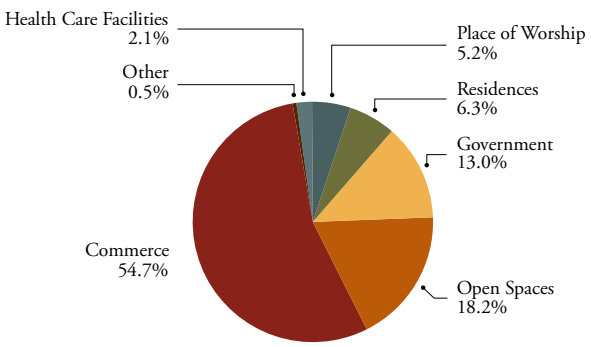
[5] *https://cdn2.hubspot.net/hubfs/3339889/Rave_Mobile_Safety_February2018/Docs/Healthcare%20Worplace%20Violence_Infographic.pdf?t=1528751363391*

[6] *https://www.hazardscout.com/wp-content/themes/eleven40-pro/home-page/sheets/docs/HazardScout_ROI_Safety.pd*

[7] *https://brandongaille.com/24-surprising-statistics-on-workplace-violence/*

[8] *https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics*

250 Active Shooter Incidents in U.S. from 2000-2017



IN 46%
OF ACTIVE SHOOTER SITUATIONS THE POLICE ARE UNABLE TO RESPOND WITHIN 10 MINUTES; AND 60% OF THE TIME THEY ARRIVE AFTER THE INCIDENT HAS ENDED.

Currently, not much is done to actively prevent an incident of this nature until the shooter has already opened fire inside the place of business. The security team notifies the police and does what it can to prevent as much physical harm as possible while awaiting law enforcement to respond. Unfortunately, in 46% of active shooter situations the police are unable to respond within 10 minutes; and 60% of the time they arrive after the incident has ended. While the security team cannot be expected to mitigate every outside factor which may lead to someone engaging in such conduct, AI-powered video analytics provide solutions to minimize the likelihood and risk of the shooter ever reaching their destination.

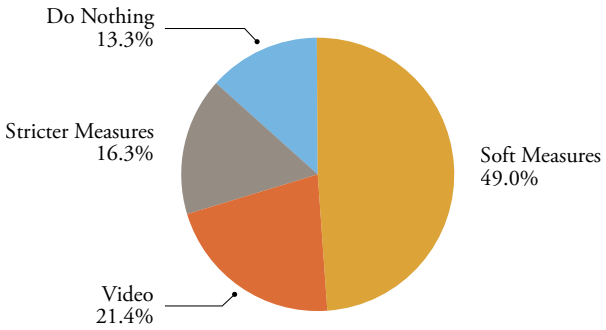
By deploying video analytics on any camera, the security team can be alerted the moment a weapon, concealed weapon, or anomalous activity is detected. Instead of the shooter reaching the lobby before being noticed with a gun in hand, cameras in the parking lot or on the exterior of the building could identify and recommend lock-down procedures to all departments and employees.

If the shooter was a former employee who was fired and made threats before leaving, that ex-employee's face can be added to an active watchlist within the solution. Or, as is often the case, the shooter may have previously made threats to the business or agency. Rather than merely creating paper BOLOs that are taped to the security guard's desk or wall, the watchlist is an alert, active, 24/7 safeguard against unwanted persons entering the premises.

TAILGATING: THE $150K PROBLEM

What may seem like a smaller problem, tailgating or piggybacking through entryways can actually lead to an array of larger safety concerns. In a survey done by IPVM, 61% of respondents said they either do nothing about tailgating or have soft measures in place to deter the activity.

How Do You Deal with Tailgating & Passback? [9]



In a 2015 survey done by Boon Edam Inc., more than 50% of enterprise security executives surveyed on the costs and risks associated with tailgating believed a security breach resulting from tailgating would cost the company anywhere from $150,000 to "too high [of a cost] to measure."[10]

In the same survey, only 15 percent of respondents said they were currently tracking tailgating incidents regularly. "While surveyors believe security breaches due to tailgating are on the rise and are deploying several strategies to combat tailgating, the big surprise is that roughly three quarters of respondents are not tracking tailgating occurrences, which could be a way to report on effectiveness or ROI and develop improvement strategies," results of the survey said.[11]

It could just be as simple as someone trying to be courteous and holding the door open for the person behind them. Or, passively granting a third-party vendor entrance without verifying credentials, but instead granting them access to the facility because of their uniform. The risks are obvious. From sabotaging equipment, stealing assets, planting a USB or chip to intercept data over wifi, to committing a violent crime, tailgating is not something security executives can take lightly.

And what about badge access gates? That same bad actor could have swiped an employee's stolen badge-access card and made it through the trusty gates at the front door or other restricted areas of the facility. Without facial verification and live alerts pertaining to tailgating, the badge access security measure is toothless and far too easily overcome. Facial recognition used in watchlists, whitelists, blacklists, should be a crucial component to any modern day security solution and is a force multiplying feature of AI-powered offerings.

---

[9] *https://ipvm.com/reports/practical-solutions-to-piggybacking-and-tailgating*

[10] *https://www.securitymagazine.com/articles/86026-tailgating-a-common-courtesy-and-a-common-risk*

[11] *ibid*

DOMESTIC VIOLENCE IN THE WORKPLACE

Building on the concept of unwanted access to the physical space, a simple use-case scenario with major ripple-effects throughout the business is domestic violence that turns into workplace violence. In terms of productivity, domestic violence issues that bleed into the workplace cost companies $727 million in lost productivity.[12] Unfortunately, domestic violence is all too-common and measures must be put in place, augmented by AI, to inhibit more incidents from occurring.

What happens when an employee notifies security or HR about someone in their life whom they are worried may attempt to come to interact with them at work, and they do not wish that person to do so? Imagine there's an employee named Monica who has an abusive relationship with a man named Steve. Monica is a valued employee who has been with the company for many years. A month ago she went to HR and requested that her ex-boyfriend, Steve, not be allowed onto campus any longer. Steve used to regularly meet Monica in the main lobby to go to lunch together. HR should pass this request immediately to security. Maybe they do, but maybe they get delayed and forget to do it right away. Maybe Steve walks in that same day and is allowed into the facility by the security guard who he sees every time he comes to meet Monica. The security guard has no reason, yet, to suspect anything about Steve, because the guard hasn't heard from HR about the threat. Steve is allowed in, even says hello to the security guard and they talk about the weather for a moment. Steve then finds Monica and attacks her. Lawsuits abound.

Instead of relying on the HR person to talk to the security team, or for Monica to go directly to security and hope that the message is passed around to all relevant persons, Monica's potential assailant can be easily added to a watchlist within the AI-powered video analytics solution. Monica can provide a photo of Steve, Steve's photo can be uploaded to the security solution, and the moment Steve is identified by any of the company's existing cameras, security will be alerted and recommended an action. In this case, denial of entry and removal of Steve from the premises.

If Steve left a package in the lobby or near Monica's car or was detected loitering near a rear exit, or Monica was detected running to her car or leaving the office alone when she should be escorted, an AI-powered solution can be utilized to detect all of these events and immediately send an alert.

If the first line of defense in these situations is a security guard making visual contact with the suspect, and then checking them against a list that they hopefully have at their desk, it's already too late.

---

[12] *https://brandongaille.com/24-surprising-statistics-on-workplace-violence/*

CYBER SECURITY & ASSETS

15%
OF ALL CYBER ATTACKS HAVE A PHYSICAL COMPONENT TO THEM.

According to one study, the average organizational cost from a data breach in 2017 was $7.01 million.[13] 15% of all cyber attacks have a physical component to them. 15% of $7.01mill is $1.05mill and is enough to warrant special attention from CSOs and CTOs alike. Of course, there are stories of exotic and exciting methods used to gain physical access or proximity to a company's critical servers and information centers, but the primary ways a physical component is involved in a data breach is spectacularly mundane. And while AI-based solutions can take care of the enhanced methods deployed (like dropping a drone armed with a data grabbing device on a roof), converting the company's existing camera network, and its corresponding centralized monitoring station, into an AI-powered real-time monitoring tool, will cut out the 15%, saving the company millions in losses.

In his article, "The Compelling Case for Unifying IT and Physical Security," Thomas L. Norman details story after story of data breaches involving a malicious actor physically involved in the process. One such incident is the Veteran Administration's (VA) data breach that put 26.5 million veterans personal information at risk, including their social security numbers. Was it a blackhat hacker group who gained access through a crack in the VA's cybersecurity? No, it was much more boring than that. A data analyst took material home from work, violating the VA's policy, and the material was then stolen from the analyst's home. A video analytics solution which allows customers to customize their analytics could be trained to detect when, for example, laptops containing sensitive information are removed from an office.

Additionally, disgruntled or careless employees account for many of the most well-known data breaches in recent memory. The NSA's data breach is believed to have happened because someone was able to gain access to areas where critical information was stored, and later simply walked out of the front door with a USB drive full of secrets.[14]

Some considerations for shoring up cybersecurity through a more robust physical security plan:

1. Maintain an exhaustive and continuously updated approved outside vendor list, verified through face identification. It is not enough to merely have a credential waved casually in a security guard's face in order to gain entrance into a company's facilities. The risks are too many and too varied, and the costs of incidents too high to not know who is gaining access to critical areas of your facility.

[13] *https://www.securityindustry.org/2017/11/20/the-compelling-case-for-unifying-it-and-physical-security/*
[14] *ibid*

2. Companies should have an exhaustive list of employees who are allowed inside areas that house sensitive information—be it a room, section of a facility, or a whole floor. As large corporations construct beautiful new buildings, in order to provide more enjoyable workspaces and public areas for customers and visitors to move about, the possibility of unwanted access is only heightened. If an employee is detected in an area they are not allowed into or trying to enter said area, doors should be locked, alerts sent out, and security guards deployed. Rather than stationing guards at every door and entry-point, leverage the cameras all-seeing power through video analytics.

3. Lastly, recently fired or disgruntled employees are routinely left with access to the buildings after they've been let go of or put on suspension. These individuals should not merely be expunged from the access lists but should have their faces added to a list of potential threats to safety. Brian Hill of Computer Forensic Services gave a talk at the 2017 Midmarket CIO Forum, where he said one of the major threats to cybersecurity is the employees themselves, whether they are terminated or resign, they can create backdoors for themselves to be taken advantage of later. Hill said, "In one major county in Minnesota, thousands of employees never had their credentials revoked when they resigned or were terminated. It was in the policy manual, but no one was actually doing it. This led to obvious, major, security risks."[15]

Just as many IT security professionals use behavioral analytics to identify suspicious online activity patterns on their networks,[16] an AI-powered video analytics solution can learn the normal behavior and movement patterns of employees. Does "Mike" normally try to access the server room at 5:49 PM on a Friday? In fact, has he ever accessed the floor that the server room is found located on? Or, is Mike the janitor and, in fact, accesses the server room once a day to empty a garbage can inside, which only takes an average of 30 seconds, but, today Mike was inside the server room for five full minutes? Security should and can be alerted.

Protecting against data breaches and IP theft is paramount to the long-term success of the modern enterprise. Data breaches not only cost the company in financial terms but in reputation and image. And some companies never recover. All of the above recommendations can be incorporated into a company's security operations through a comprehensive AI-powered video analytics solution integrated directly into the company's existing camera network and VMS.

---

[15] *https://www.techrepublic.com/article/6-common-enterprise-cybersecurity-threats-and-how-to-avoid-them/*

[16] *https://www.cio.com/article/3243281/leadership-management/end-user-security-risks-mitigating-insider-threats-to-enterprise-securit.html*

Conclusion

The data speaks for itself. As threats to enterprise security and safety continue to rise, and the consequences correlatively become more severe and costly, the time has arrived to rethink traditional security and to embrace the different ways AI can augment security. AI-powered video analytics will not only drastically improve security but can have a positive impact on employee morale and trust.

Do your employees and staff currently view the security team like a guardian angel or, rather, as an unresponsive, intrusive but necessary business function? If the security team is equipped with the tools necessary to respond to incidents quickly, using things like AI-powered post-event search, and can also proactively predict and meet employee needs, security then becomes a force for good rather than just simply existing as another necessary (and costly) line item on the yearly budget.

LEARN MORE AND REQUEST A DEMO AT

www.vintra.io

VINTRA, INC. \\ SAN JOSE, CA

408.610.8959 \\ INFO@VINTRA.IO

VINTRA.IO \\