Ambient.ai

THREAT DETECTION & RESPONSE

Automatically Detect Threats and Respond 10x Faster

Workplace violence is an ever looming issue. More than two million people face workplace violence annually. Those numbers are expected to rise at the same time as many employees are returning to office or considering a return to office. A recent report found that 88% of business and security leaders anticipate an increase in physical threats of all kinds to their enterprise organizations in 2022. At a time when workplace violence looms large, security and operations teams have few tools to help them detect and prevent threats.

Security cameras are foundational to physical security. Organizations with large areas to cover, a high-risk of theft, or where 24/7 guard services aren't feasible (e.g., schools), invest in security cameras to help protect people and assets. But on their own, the cameras do little to detect threats or help to prevent security incidents.

The challenge is that the cameras are reliant on human operators to interpret the surveillance footage, interpret the context of each specific situation, and apply their security awareness.

Even cameras equipped or connected with a video analytics system are prone to false alerts. As a result, security and operations teams are left reacting to security incidents.

A relatively large corporate campus with 300+ cameras produces 7,200 of video each day – making it impossible to have humans monitor the feeds in real-time. On top of that, humans simply aren't built for continuous monitoring. According to "Buyer beware," a study by T. Ainsworth, after 12 minutes of continuous monitoring an operator may miss up to 45% of screen activity. After 22 minutes, the miss rate can reach as high as 95%. In a few seconds, someone can sneak through a door that has been held open for too long, jump a fence, or walk out of a secure area with a laptop. It's unlikely that an operator would be able to spot these threat behaviors even if they are trained on a camera wall.

Brian Kellmann
Director of Security Engineering and Infrastructure at Impossible Foods

> Since our rollout with Ambient.ai, we have been able to enhance our threat detection capabilities and reduce false alarms by over 97% – representing a significant enhancement in overall security for the company.

The Physical Security Bottleneck

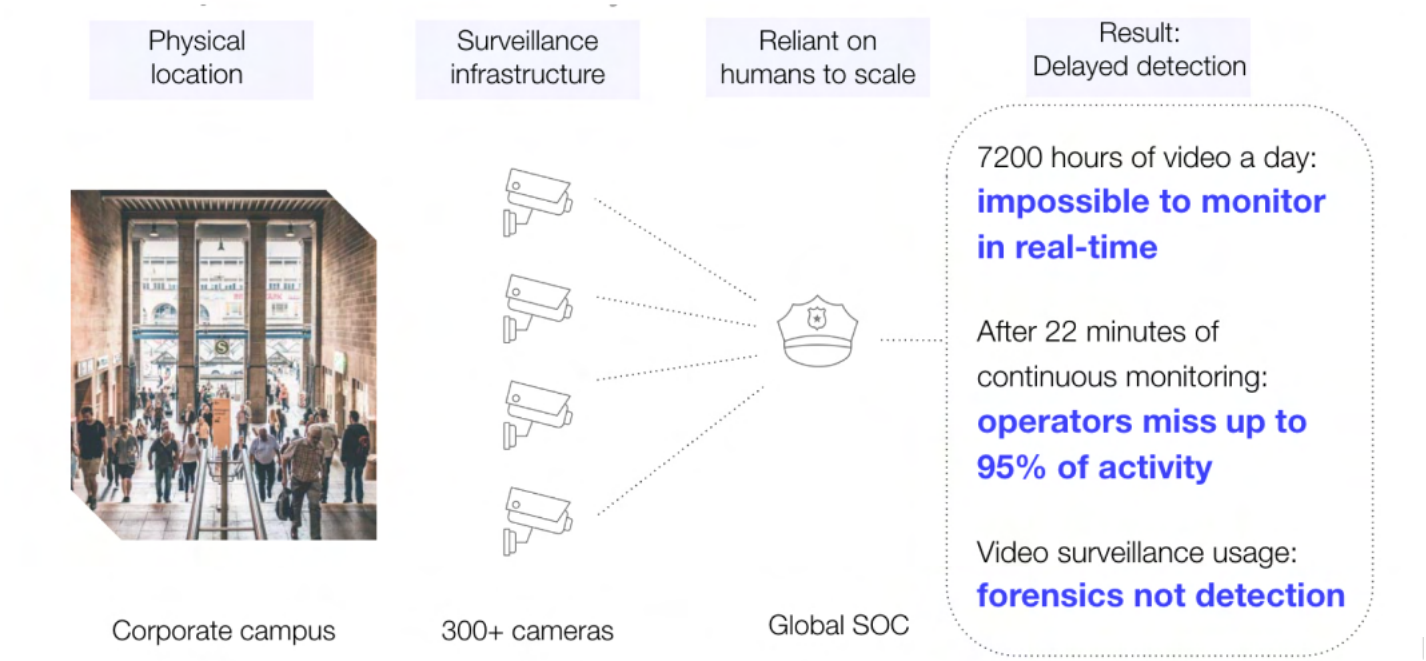

Figure above: At a relatively large corporate campus with 300 cameras, human operators are unable to effectively monitor surveillance feeds in real-time. As a result, security cameras become a forensic tool rather than a detection and prevention tool.

Ambient.ai removes this bottleneck by automating real-time threat detection and enabling security and operations teams to respond before incidents escalate. Ambient.ai leverages computer vision intelligence to apply advanced threat detection and security awareness to surveillance feeds. The Platform detects threats in real time, immediately alerts on threat behaviors, and enables security and operations teams to respond immediately with incident response workflows.

Introducing Automated Threat Detection & Response

Ambient.ai built upon innovations in AI and computer vision to achieve near human-level perception and combined that perception with contextual security awareness. The end result is computer vision intelligence, which is capable of recognizing not only movement, objects, and human-object-interaction but also security context and site-level intelligence.

By leveraging the existing security camera infrastructure, Ambient.ai's computer vision intelligence acts as the brain for security systems, detecting threat behaviors in real time and enabling security and operations teams to respond more effectively.

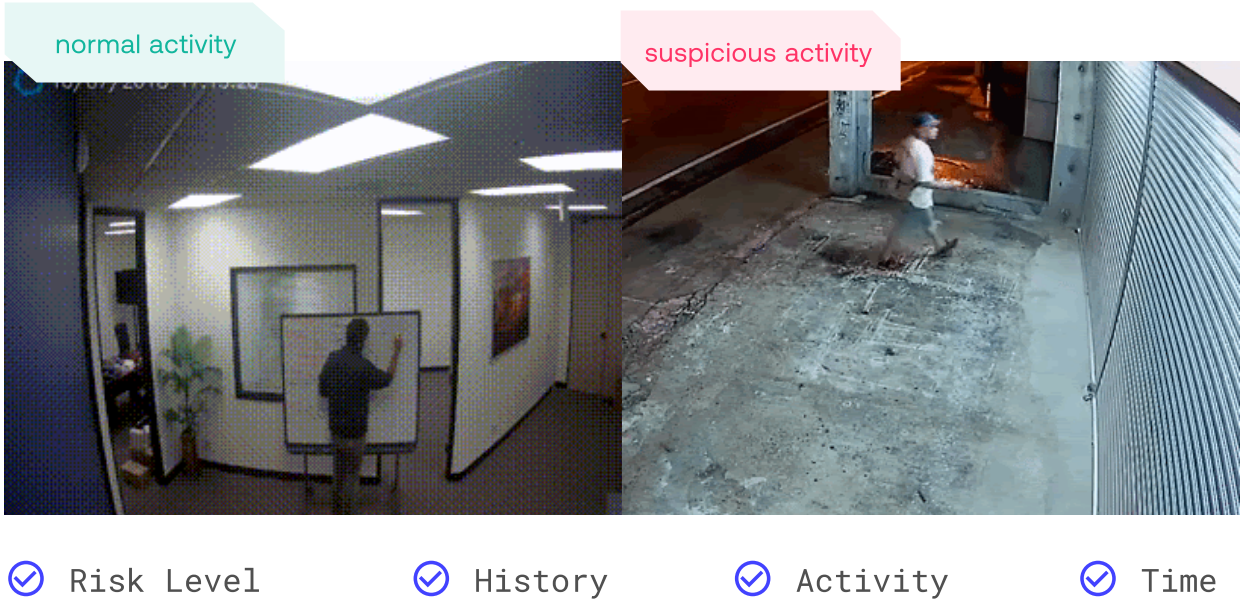

Figure above: By understanding the site level context around a behavior, computer vision intelligence can accurately discern what is a normal activity and what is a suspicious activity, even when the behaviors appear to be similar.

Automated threat detection

Ambient.ai automatically monitors and detects more than 150 unique threat behaviors – without use of facial recognition. With Ambient.ai's flexible context-graph models, new threat signatures are being added continuously and can be tailored to an organization's specific needs.

The ever-expanding threat library detects threats in six categories:

1 High-Severity

High-severity threats are the most serious and often result in physical harm. Ambient.ai not only detects these threats in real-time, like brandishing a firearm or knife, but can also detect early warning signs, like unauthorized entry and crowd commotion – enabling faster response times and a greater chance of preventing incidents before they happen.

2 Alarm Reduction

Security and operations teams at large organizations are often overwhelmed by false alerts and nuisance alarms. More than 90% of alerts from physical access control systems (PACS) are false, leading to thousands of hours spent dispositioning alerts rather than responding to verified threats. By visually verifying PACS alerts, like door forced open and invalid badge read followed by tailgating, Ambient.ai eliminates the need to disposition false alerts. This capability is called Signals Intelligence.

3 Perimeter Control

Perimeter control is key to physical security. Ambient.ai detects security incidents and the precursors to security incidents at the perimeter, including person jumping fence, person loitering after hours, and unauthorized vehicle in secure area.

4 Health and Safety

Detecting health and safety incidents is important to ensuring that employees, students, and customers feel safe. Ambient.ai detects a wide range of behaviors that indicate health and safety risks, including person falling down, large crowd forming, and sudden egress.

5 IP and Asset Protection

Protecting IP and assets is critical to many organizations. Detecting IP and asset theft, however, is challenging. Many systems can't differentiate between normal activity and suspicious activity. In office environments, for example, it's normal for people to walk to-and-from locations with their laptops in hand. But if someone takes a laptop from a secure area that indicates a security threat. Ambient.ai understand the context in each situation and can accurately discern which is normal activity and which is a security threat that needs to be escalated.

6 Unauthorized Access

Physical access control systems (PACS) are important for preventing unauthorized access but are limited to alerting on a narrow subset of hardware-captured threats. If a door is forced open, the system will send an alert, but if an intruder instead enters through a window, a stand-alone PACS solution will not detect the intrusion. Ambient.ai detects unauthorized access even in cases when PACS wouldn't alert, including tailgating, entering through a propped door, or loitering outside of a secure door.

Intelligent Response

In physical security, every second matters. Ambient.ai is designed to automatically identify threats and enable security and operations teams to respond faster with response workflows.
These response workflows enable security and operations teams to respond 10X faster. Ambient.ai's response workflows ensure that every alert is actionable and enables security and operations teams to intervene before the incident escalates.

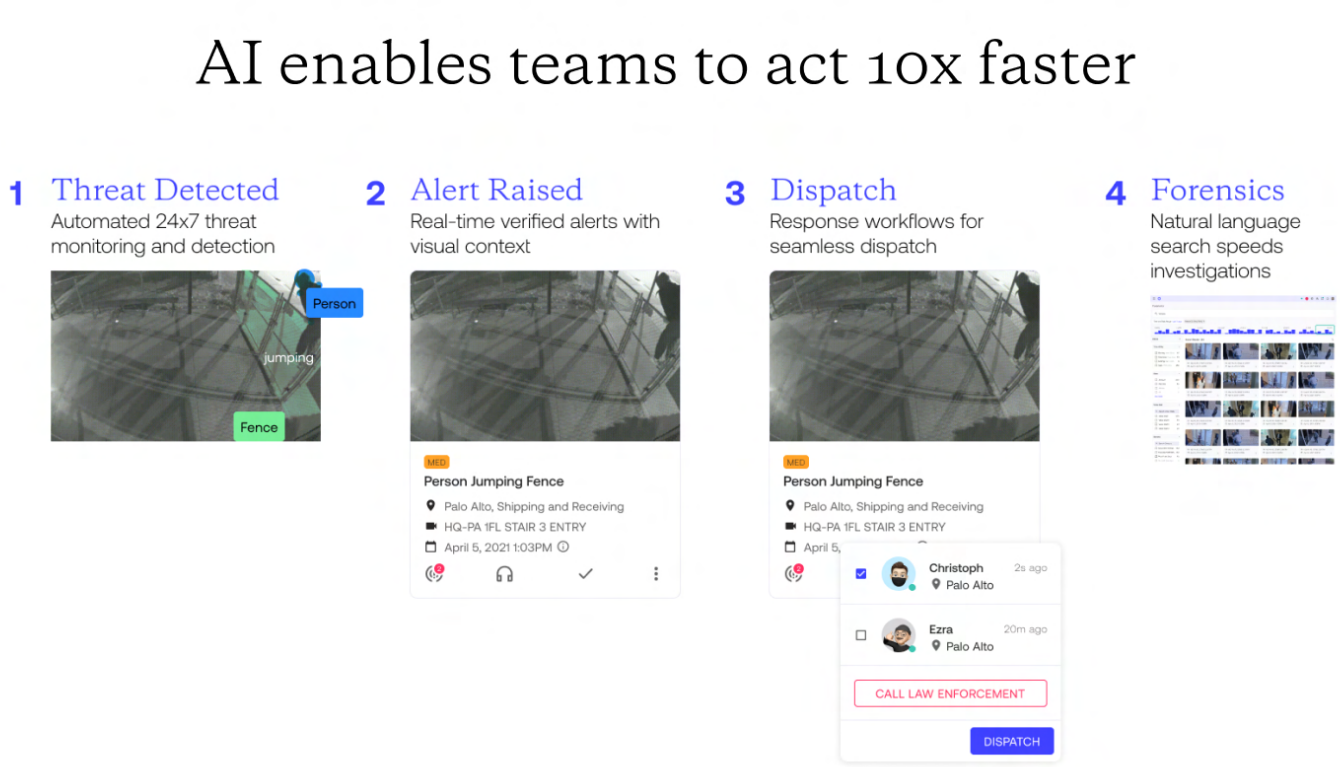

Figure above: Once a threat is detected, Ambient.ai immediately sets in motion a workflow that enables operators to respond 10X faster.

The workflows include enable security and operations teams to better respond to security incidents from:

1 Threat Detected

Ambient.ai leverages the existing security camera infrastructure to continuously monitor and detect more than 150 unique threat behaviors, including the precursors to security incidents – enabling security and operations teams to proactively respond to security threats.

2 Alert Raised

Once a threat is detected, a visual alert with the corresponding surveillance footage is sent to the appropriate team members. Alerts can be customized to fit the time and even severity of the threat. A fence jump during business hours might trigger an alert to the guard on duty while a door being forced open in the middle of the night might alert the guard and the head of security – and even local law enforcement.

3 Dispatch

Each alert includes integrated dispatching capabilities, allowing security and operations teams to respond faster with the visual context they need to assess the situation. Alerts can be accessed via desktop and mobile. Continuous updates ensure that responders know exactly what is happening as the incident evolves.

4 Forensics

Forensics applied to the video surveillance feeds enable security and operations teams to retrace each incident 20X faster. Natural language search ensures that security and operations teams can easily find the appropriate surveillance footage by searching by time, location, type of incident, and more.

The Impact of Adopting Automated Threat Detection & Response

The cost of reacting to security incidents rather than proactively intervening before they escalate is very high. The National Institute for Occupational Safety and Health estimates that workplace violence incidents cost employers more than $120 billion in business interruption, legal liability, and psychiatric care for affected workers – and that's only the beginning.

The pandemic has raised stress levels and brought new concerns to the forefront for many employees. In a March 2022 survey, the American Psychological Association reported that close to three in five (58%) adults labeled the pandemic as a daily stressor. Even after two years of modifying behaviors to reduce the risk of COVID-19, employees continue to report unusually high levels of stress. An incident of workplace violence will only exacerbate stress levels, making employees feel unsafe in returning to the office, damaging the reputation of the organization, and making hiring even more difficult than it already is.

While workplace violence is an increasingly serious threat, it isn't the only costly concern for organizations. US businesses lose up to $110 million a day due to employee-related crimes and Intellectual Property theft costs US business between $225 billion to $600 billion annually.

With automated threat detection and 10X greater response times, Ambient.ai enables security and operations teams to move from reacting to security incidents to proactively responding. In addition to hundreds of thousands of dollars in savings from automation and expert enablement, Ambient.ai gives security and operations teams the tools they need to intervene before security incidents escalate – providing them with the tools to prevent costly security incidents.

About Ambient.ai

Ambient.ai proactively monitors every single camera, correlates threats across cameras, and delivers site-level intelligence. It cross-correlates activities on surveillance streams with the data from other building endpoints, including PACS and other sensors, to automatically perform video verification and detect new previously undetected threats.

By adding contextual knowledge, Ambient.ai takes computer vision technology to the level of an autonomous system with near-human perception behind every single camera in the enterprise. The system that never gets tired and proactively alerts you of real threats to your security team 24x7x365.

To learn more about Ambient.ai visit our website at www.ambient.ai.