

How It Works

Detect Unexpected Activity

Customers configure certain cameras (or regions of interest) to be monitored, and set a schedule of when the Virtual Guard service should be active, or "armed." Using advanced AI analytics on the cameras, Verkada alerts our 24/7 monitoring agents when a person is detected in the scene. In addition, events from other Verkada devices can be configured as triggers for virtual guard review.

Review Events

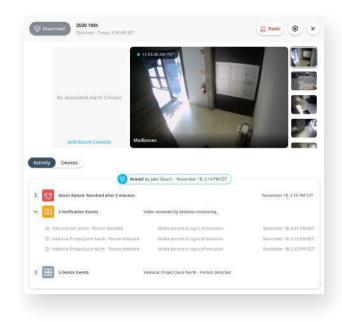
Verkada sends a secure video stream of the event to our U.S.-based monitoring agents for review. These trained security agents review the video in real time and determine if there is suspicious or threatening behavior.

Respond Appropriately

In the case of a visible emergency, agents will immediately contact first responders for dispatch to the site address and then contact the customer's call list.

If there is suspicious activity but no emergency, agents will attempt to call customer contacts first to determine the desired response, and only contact emergency services if no one can be reached.

If the agents cannot identify a threat, the event will be disregarded. All events are logged and available in Command for auditing and review.





Verkada Product Integrations

Our professional monitoring agents can review events triggered by other Verkada devices, including door controllers, environmental sensors, and wired/wireless intrusion sensors. Monitoring agents will review video from Verkada cameras that are linked with these devices in Command.



Use Cases

Verkada's Virtual Guard service offers 24/7 protection for customers across a diverse set of industries. Examples include:

- Restaurants and retail businesses detect and respond to suspicious activity in buildings and parking lots after closing.
- Retailers and restaurants detect, verify, and respond to suspicous activity, while reducing false alarms.
- Construction sites and car dealerships detect trespassers and respond with police dispatch
- Warehouses and storage facilities are alerted to unauthorized or unusual access after hours.

Limitations

The Virtual Guard service is designed for after-hours, event-based video monitoring. Monitoring agents will only review video clips from events designated as alarm triggers by customers in Command. Customers should not use Virtual Guard to monitor spaces with constant human activity, or any situations where a threat to people or property would not be self-evident from the video footage. A resolution of 75 pixels per foot is recommended for accurate person detection. Monitoring is provided by three fully redundant U.S.-based, UL-listed, TMA Five Diamond certified central stations.

Contact **sales@verkada.com** for help setting up Virtual Guard with your Verkada cameras.

Not yet a Verkada customer?

Contact **sales@verkada.com** to recieve a 30-day camera and Virtual Guard trial.

Emergency dispatch services are only available in the U.S. and Canada. See **www.verkada.com/alarms-availability** for more information.



Getting Started

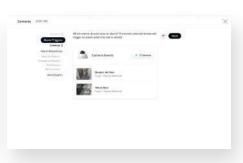
The Virtual Guard service is bundled into the Alarm License, and a free 30-day free trial is available to all customers with Verkada cameras. Organization administrators can click on the Alarms tab in Command to begin their free trial. Follow the steps below to set up Virtual Guard at one or more of your locations:



Start trial and select site to monitor.



Choose cameras and regions of interest to have monitored.



3

Select other devices to trigger video review (optional).



Enable video verification and choose your video review settings. Normal Security is recommended.



Enable Emergency Dispatch. You can put the site in Monitoring Test Mode if you want to receive a test call but not dispatch first responders.



5

Designate which individuals should be contacted by the monitoring agents after events are verified and in what order. You can also have individuals receive SMS or email alerts for verified events.



Virtual Guard is only enabled when the designated site is "Armed." You can manually arm and disarm the site via Command, or set an Arm schedule. Site should only be armed after hours or during periods where human activity in the selected cameras/regions is unexpected and represents a potential threat to people or property.