actuate

INFOSEC AND COMPLIANCE FACT SHEET

OVERVIEW

Actuate's threat detection AI solution makes organizations safer without implementation headaches. By using existing IT-approved security hardware and software, minimizing data retention, and leveraging world-class cybersecurity platforms, Actuate is compliant with IT and Privacy policies.

SOFTWARE ONLY

Actuate is a software-only solution that can be implemented in as little as 15 minutes, eliminating hardware procurement concerns.

USES EXISTING IT (INFORMATION TECHNOLOGY) ASSETS

No Actuate code touches the customer network: The AI platform integrates with the existing video management system (VMS) software and uses the VMS's integration APIs to pull video and send alerts. All communication occurs through already-implemented and already approved software channels.

MAXIMUM VMS SECURITY

Actuate communicates with the VMS using the highest level of security supported by each platform, including SSL and image encryption. In all cases Actuate uses unique authentication for each customer.

MINIMAL DATA RETENTION

The Actuate platform stores no video or images unless a weapon is detected: All other video received by the system is deleted immediately after being analyzed. When a threat is identified, images are stored only to support sending high-quality alerts.

NO PERSONALLY IDENTIFIABLE INFORMATION (PII)

Actuate stores no information of any kind about building occupants, except for images if a weapon is detected. Even when a weapon is detected, no data about an individual is tied to the stored images.

DETECTS THREATS NOT INDIVIDUALS

Actuate does not perform facial recognition or any other type of analysis of the humans present in a video feed: Actuate only looks for physical threats such as weapons. Many gun violence events are perpetrated by people who are authorized to be in a location, so facial recognition doesn't provide early warning, limiting its effectiveness.

WORLD-CLASS CLOUD HOSTING

Actuate uses Amazon Web Services (AWS), Microsoft and Azure to host its AI engine. AWS and Azure is trusted by global organizations because it has best in-class cybersecurity processes and teams, freeing IT from worrying about the security of the Actuate platform.

ORGANIZATION-SPECIFIC INFRASTRUCTURE

Actuate allocates a unique IP address and network gateway to each customer deployment, ensuring that customer data does not mix, and minimizing the cybersecurity impact of integration.