101 on Asset Tracking Technology (or "Content Surveillance")

Jul 2, 2019

What is Content Surveillance? When should you use it, and when shouldn’t you use it?

The real power of the business and physical security solutions that we develop lies in how they integrate together. Possibly the best example of this is the content surveillance system available in our AssetTracer smart lockers for asset tracking. It connects physical asset lockers with centralized management software and our other real-time security systems. Whole new workflows are possible when these tools are integrated together.

But while content surveillance is a powerful tool, it’s not necessarily the right solution for every business. Here we’ll cover what content surveillance actually is. And discuss the situations where it’s valuable, and other situations where standard smart lockers might be a more appropriate choice.

What Is Content Surveillance?

Content surveillance systems verify that the correct assets are placed in lockers, and can also provide data on their condition. This surveillance gathering can be done over either wired or wireless connections.

Most electronic devices that charge with a USB-type port can identify themselves when plugged in inside a locker. This way they're both recharged at rest and their status automatically verified.

Alternatively, a wireless tag and reader system can be used. Wireless tags are attached to or embedded in assets, and the readers are mounted inside the locker cabinets. The readers can even be configured to detect multiple tagged assets within carrying cases. Integrating smart lockers with real-time location services (RTLS) elsewhere in a facility provides live data on where, when, and how those assets are used.

The goal of any content surveillance is to provide better insight on the asset and its use. By logging transactions, a smart locker system is already a source for business intelligence. But adding content surveillance turns assets themselves into information sources.

When You Need It

Any organization using asset lockers obviously cares about security. They have assets whose loss would be damaging financially or operationally. But for some businesses that's their only concern: the security of the asset itself.

Businesses that benefit from content surveillance tend to care just as much, if not more, about *how* their assets are used, and by whom.

Using a content surveillance system lets you build workflows around the real-time availability of different assets. You can restrict access based on the specific staff member signing the asset out, by time of day, or by other criteria. For example, if you need to provision rugged laptops for heavy-duty field use, you may want to rotate sign outs to distribute wear and tear. With a content surveillance system, your smart locker system can verify which laptop is in which locker, and how many hours of use each has received. Then the system will only unlock the laptop with the least use.

That’s just one example. A whole range of workflows can be improved:

Smart lockers can always track who signs an asset in or out. But without content surveillance, they can’t verify what is actually taken or returned from the locker, if anything is returned at all. A disgruntled employee could sign a laptop back in at the locker terminal, but then just keep it with them when they walk out the door on their last day.

If assets are particularly sensitive, expensive, or regulated, a content surveillance system can confirm in real-time whether they’ve actually been returned. And instantly notify supervisors if they’re not, for time-sensitive response. Without that automated verification it may not be until next shift, or even days later that a mission-critical device is found missing.

As we mentioned up top, content surveillance systems can detect multiple items in hardened carrying cases. Some organizations want—or need—to ensure that individual components are returned, like medication or controlled substances or government-regulated materials.

Content surveillance can notify EMTs if life-saving medications are missing from a kit bag *before* they go on a call. Or notify supervisors if a regulated substance is missing upon return.

Compliance Reporting

Some of those regulated materials probably need to be accounted for in compliance reports. These reports are easily and automatically compiled by smart locker management apps, in real-time as asset transactions occur.

Or as we talked about in a previous smart lockers article, alternate forms of content surveillance, like scales for weight checks, can measure and verify assets upon return. For law enforcement agencies who need to verify whether OC (pepper) spray cans have been used by checking their weight, this automates an important compliance task.

If IT teams need to be notified of break-fix issues as soon as laptops, tablets, or other assets return from the field, you can turn smart lockers into a service tool for them.

When a staff member returns an asset, the touchscreen interface on the smart locker can prompt them to log any issues encountered. For laptops, for example, it could be anything from a crashing application to an entirely dead device. That logging triggers an email alert to the IT team and unlocks a designated ‘Service’ locker. The content surveillance system then ensures that the specific device that user signed out is the one placed in the Service locker.

This general workflow—a staff-entered code triggering a specific locker opening—can be used for other assets that need attention. Like supply kits that need restocking, firearms that need maintenance, or delicate instruments that need cleaning.

When You Don’t Need Content Surveillance

Content surveillance is powerful, but only for certain workflows. So not every organization needs it. If your organization’s primary concern is mitigating the costs of lost or stolen assets, standard smart lockers will meet your needs perfectly fine.

Or if keeping staff accountable for their transactions is important, even if the value of the assets is low, then standard smart lockers again should be sufficient. Even without content surveillance, standard smart lockers still provide useful data through their reporting features, like those available in our RTNHub management app. For complying with some industry regulations, this level of reporting is sufficient.

It’s All Customizable

Content surveillance is a powerful and very flexible tool. While some businesses clearly either do or don’t need it, many fall in a gray area in between. Others know they need it, but aren’t sure how to implement it. Speaking with an expert security consultant may be the best way to determine what works best for your organization.

https://www.realtimenetworks.com/blog/101-on-asset-tracking-technology-or-content-surveillance