

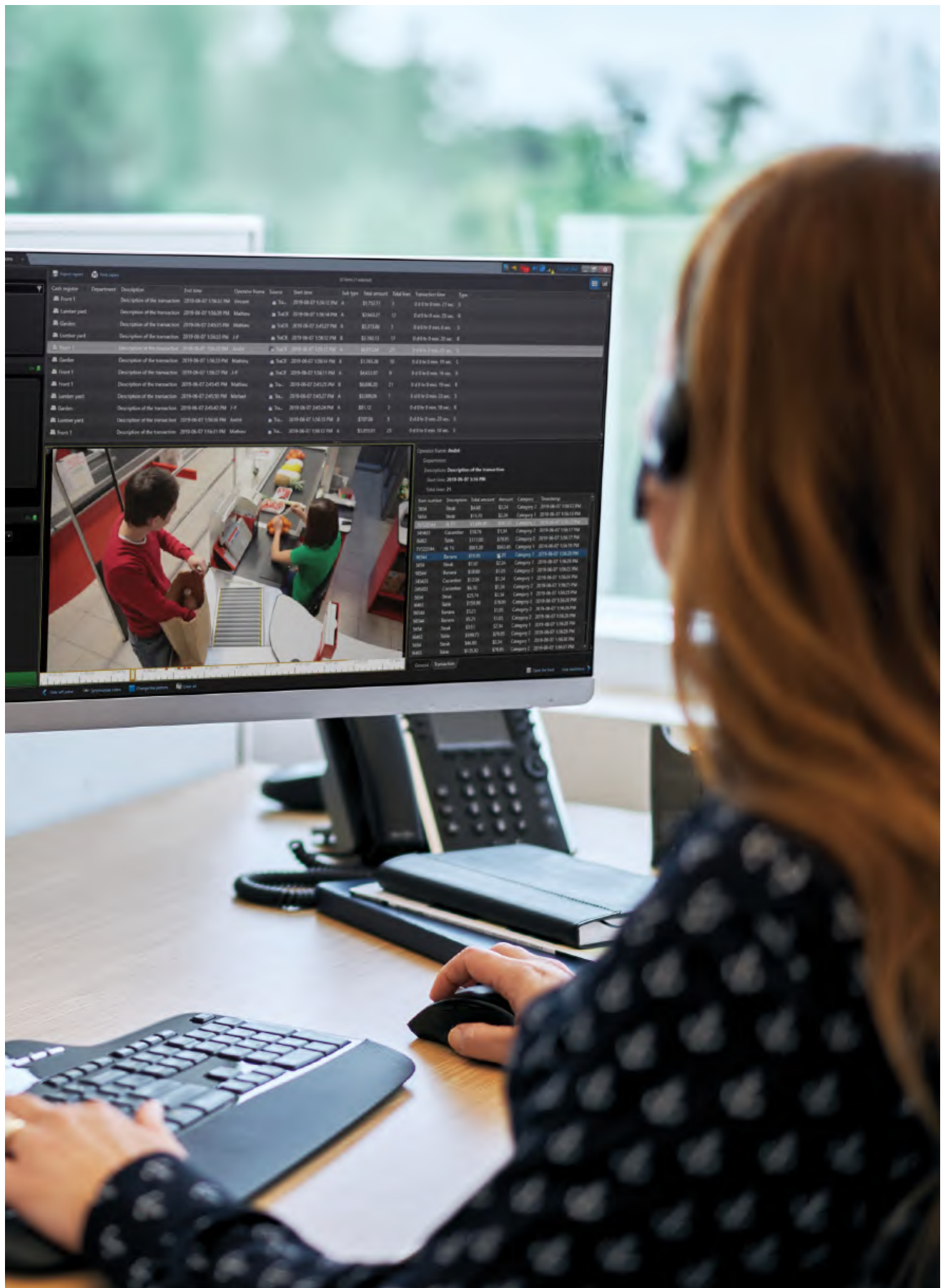
Physical security solutions for retail





Contents

Executive summary	5
How frictionless shopping impacts retail shrink	8
The importance of video surveillance	10
Benefits of cloud-based systems	12
Why a unified security platform is essential for retailers	14
Conclusion	16



Executive summary

Modern physical security solutions for retail offer benefits that go far beyond simply improving security. Today's systems gather a wealth of data from video surveillance systems, access control, automatic license plate readers, identity management, and a variety of other sensors and systems. Yet without a fully unified software solution, it's hard to see how all these puzzle pieces fit together.

When you can bring data from many different sources into one place, you get a complete picture of what's happening in your retail environment, and that helps everyone on your team work more effectively. Marketing and merchandising managers can visualize how customers move through their store, and adjust the layout or displays to remove bottlenecks and improve flow.

The arrival of frictionless shopping solutions such as curbside pickup and self-checkout have introduced new challenges for retail security teams. To combat them, unified security platforms offer a range of ways to keep up. Asset protection managers can easily review the video of self-checkout systems if theft is suspected, and share it with law enforcement as needed. IT teams can spend less time updating software and focus their time on higher-priority tasks. And, of course, corporate security managers can work

more effectively and efficiently with a full view of the connected store.

For many retailers, a gradual migration to a fully unified, cloud-based system is the most practical and cost-efficient solution. For example, replacing and upgrading systems for thousands of store locations all at once may not be feasible. Instead, transitioning over time to fully connected stores can help retailers protect profits. By streamlining or automating workflows, you can improve operational efficiency, loss prevention, and monitoring of customers' buying behavior. With a unified system, retailers can also solve investigations more quickly by having access to the right information when concerns arise.



1

How frictionless shopping impacts retail shrink

The pandemic accelerated a massive transformation already underway in retail towards a frictionless shopping experience. Solutions like curbside pickup, self-checkout, and mobile checkout became even more popular during the years marked by social distancing. Yet the addition of new technologies aimed at streamlining checkout and contactless shopping experiences have also created more opportunities for retail shrink.

While frictionless shopping solutions are an effective tool for many retailers to keep checkout lines flowing smoothly despite staffing shortages, this technology opens the door to theft and shrinkage due to errors (such as forgetting to scan certain items). One way retailers are mitigating these challenges today is through the use of physical security solutions at checkout. Monitoring point-of-sale areas can help with loss prevention and keeping people honest.

Today's retail loss prevention investigators may be tasked with reviewing hundreds of incidents at several different stores, as well as preventing internal theft at warehouses and distribution centers. A unified physical security platform empowers loss prevention professionals to accomplish their investigations more quickly and efficiently.

When it comes to loss prevention, complexity is the enemy. The masterminds behind organized retail theft are strategic. They look for opportunities to gain knowledge of internal systems and exploit weaknesses in broken processes.

To defend against shrink, retailers must be constantly monitoring for breakdowns in routine processes that can expose opportunities for theft or shrink. From switching product labels to void transactions, to sweetheart discounts for friends, new strategies are created every day. Some degree of shrink will always exist, but strengthening your processes and introducing better monitoring systems can make you more resilient to these threats.

E-commerce security, fulfillment, and logistics concerns

The continuous development of e-commerce has also introduced new security concerns, as well as the need for inventory management logistics at distribution centers.

When a customer clicks the 'buy' button on your website, the goods they order are prepped for pickup by truck drivers, shelf-stockers, order fulfillment staff, and other warehouse workers. Because many people are involved in coordinating behind-the-scenes tasks to deliver each package, a lot of different individuals move through distribution centers who aren't regular employees. Sophisticated software solutions are required to keep up with these dynamic workplaces for loss prevention, as well as to ensure employee safety.

Automatic license plate recognition (ALPR) technologies can play a key role at distribution centers to keep track of who comes in and has access to products. In retail specifically, ALPR can record who has received their products from a curbside pickup station. It can also help identify organized retail crime suspects by checking to see if a vehicle is on record as having been involved in previous thefts.

Supply chain management is another area where retail security technologies can play an important problem-solving role. Using article tags and video surveillance, retailers can mitigate losses by monitoring surroundings and tracking individual products as they move from a supplier to a warehouse, and to a store.

2

The importance of video surveillance

Video cameras have come down in price and increased in quality, so it's no wonder that many retailers lean heavily on video surveillance as a critical component of their security solutions. Yet adding more cameras may also introduce new challenges.

When cameras are recording during store hours, you can be collecting hundreds of hours of video per store, every week. That can be a lot of data to sift through. Simply storing that video footage isn't enough—you need to equip your team with tools they can use to make sense of it.

With a unified security platform, you can correlate video with other systems. Cross-referencing video footage with other analytics such as the direction of travel, heat mapping, or people counting, can reveal powerful insights. Using these tools can improve your awareness and understanding of your customer's journey through the store and at checkout, so you can improve their shopping experience.

For example, you can set up your system to automatically trigger a request for the floor manager to open a new checkout line when a certain number of people are in the queue. Or, if the system detects that a crowd is forming at the self-checkout line, you can set up a notification to tell employees to go see if customers need help.

Video can aid to identify operational issues too. For example, retailers can use video to ensure items are being sold and scanned correctly at checkout. If a set of two items are being scanned as one, that can lead to a significant loss of revenue. Once a retailer suspects customers are being undercharged, video footage can be cross-referenced with POS data to get a better understanding of how items are being scanned. With this ability to review and analyze data, operational problems can be easier to solve, so retailers can limit potential money leaks more quickly and effectively.

Set up your system to automatically trigger a request for the floor manager to open a new checkout line when a certain number of people are in the queue.

You invest a lot of time, money, and resources to set up your video surveillance system. Make sure you're getting the most value out of it by having the ability to fully understand your retail environment and take data-supported decisions. A unified system allows you to manage all your cameras' data alongside that from sensors, smart devices, and maps within one intuitive dashboard.

Video surveillance and privacy concerns

Video can be a powerful tool to understand customer behavior, but it's important to take special care to preserve your customers' anonymity—or you risk breaking their trust.

Privacy concerns related to video surveillance have been on the rise, as well as the growing awareness of personally identifiable data. It's important to only collect and store the data you need to improve security and the customer experience, and be transparent with customers about what information and video footage you collect and why.

Often you'll need to share video footage externally with law enforcement, legal advisors, the media, or other stakeholders. You will want to ensure you have a way to share video securely while protecting any personally identifiable information of bystanders captured on camera.

When video becomes evidence, it's important to mask the identity of any person who is not part of the investigation. To make sure the evidence will stand up in court, it's essential to watermark and authenticate video footage and ensure the chain of custody is clear. If new stakeholders are granted access, it must be documented along with the time stamp. There should not be any doubt as to whether unauthorized users are viewing or being forwarded the footage. Tracking the chain of custody also supports being able to confirm whether the video could have been tampered with or altered.

3

Benefits of cloud-based systems

Cloud-based systems make it easier for retailers to scale storage requirements as their business requirements change. Yet many companies hold back from making adjustments because of the logistical challenges involved in switching out aging systems and infrastructure. Transitioning to cloud systems is not something that must be done all at once. Many retailers have successfully navigated a more gradual evolution by embracing hybrid cloud systems.

It's a tall order to revamp your IT technology all at once—and for some companies, it's just not an option to make such a sudden switch. With a hybrid cloud approach, retailers can easily expand and scale, decluttering hardware environments over time. By connecting IoT devices as stores are upgraded or retrofitted, they can take advantage of new technology and functionalities. A hybrid cloud strategy allows you to continue to run on-premises systems that are meeting your current needs, and link these to flexible cloud-based technologies. If you have 10 new stores that use cloud-based systems and 10 established locations with on-premises systems, a unified platform will allow you to manage the data from all of them, in one place.

Cybersecurity considerations

Today, retailers face escalating risks from cyber threats including fraud, account takeovers, malware, ransomware, compromised business emails, and data breaches. Businesses suffered 50% more cyberattack attempts per week in 2021, yet half of U.S. businesses still do not have a cybersecurity risk plan in place.

IBM's annual cost of a data breach report found that in 2021 the average cost of a data breach rose from USD 3.86 million to 4.24 million.

Businesses suffered 50% more cyberattack attempts per week in 2021, yet half of U.S. businesses still do not have a cybersecurity risk plan in place.

When companies suffer a data breach, they not only face steep costs to repair the damage, but they also lose customer trust and loyalty which can impact their business for years to come.

Any device connected to your network—whether it's a smart IoT thermostat, an access control sensor, or a computer—has the potential to be a gateway for cyber criminals to access private data stored on servers connected to that network.

Because today's technology is so interconnected, data has to be secured and monitored at every step. Here's what that can look like:

- Ensure all employees, contractors, and partners who access your network follow good cyber hygiene protocols, such as creating strong and unique passwords, and implementing multiple-factor authentication where possible.
- Verify that cameras, access control devices, and IoT devices use certificate-based authentication and that all drivers and relevant software are kept up to date with the latest security patches.
- Provide training to employees to educate them about cybersecurity best practices, and ensure they are often prompted to update passwords.
- Secure communications over the network, and connection points between hardware and software roles with data encryption.
- Stay vigilant with bring-your-own-device policies to make sure your team can determine the security level of external devices.

When different solutions that were not designed to work together are put into place it can quickly become difficult for teams to manage, upkeep, and scale as your company grows. Manage everything with ease, using one unified security platform.

4

Why a unified security platform is essential for retailers

If your video surveillance system, intrusion monitoring, POS reporting, access control, and anti-theft systems are all separate, each one has its own software and user interface to manage. While you may be able to connect some of these systems through clunky integrations, your loss prevention and physical security staff still need to learn to use each system individually, and toggle between programs in order to get their work done.

When systems are designed in silos, it makes it more difficult to get the full value of the data you collect. Instead, leveraging a unified and connected store allows staff to access data from all these systems and more, such as license plate recognition, occupancy management, article tags for asset management, and two-way audio. Data from all unified systems can be combined and displayed in different formats such as customized dashboards, graphical maps, mobile apps, or a web client.

When you can view your data from different sources all in one place, new insights will reveal themselves. This is not only useful from a security and loss prevention standpoint, but can also provide business intelligence to improve customer experience, merchandising, marketing, productivity, and more. Too much data on the other hand can be overwhelming. That's why each user customizes their own dashboard to only display the data that is most relevant to them—everyone from upper management to security teams, to frontline employees, can easily manage the information they need.

Each user customizes their own dashboard to only display the data that is most relevant to them—everyone from upper management to security teams, to frontline employees

Every department, from asset protection to marketing, will be able to uncover different insights, bringing a variety of angles and solutions to the table. This is where interdepartmental collaboration can be key to developing new strategies. Some companies may also find hiring a specialized data analyst can be helpful to see the bigger picture.

Unification also helps to simplify scaling. Whether you are opening a new store in your first location or expanding an international brand with hundreds of locations, you need a solution that can continuously meet your needs as the business evolves. With the flexibility of a unified platform, it's much easier to keep your software current with the latest updates and security patches.

Streamline your training and onboarding processes

One side effect of the pandemic has been unprecedented employee turnover, making it much harder to keep staff. The turnover also makes it more challenging to ensure that access permissions and passwords are properly secured when employees leave.

A unified platform can also be easier to use, so staff can accomplish tasks more efficiently. In addition, its customizable interface allows for simpler training for new employees. Instead of learning how to manage six or seven different systems, with a unified solution staff only need to learn how to use one piece of software. There's no need to switch between different tabs or windows to access various data sources either—all the information you need can be organized in one place.

When your access control system is unified with other systems, such as an identity management system, access can also be tied to roles. This means you can automatically grant or revoke access when employees change roles, locations, or leave. Employees, contractors, and suppliers may have different rights and privileges to access specific spaces. Some may have access only under certain conditions, such as on specific days of the week or during certain hours.

5

Conclusion

1. Choose open architecture solutions over proprietary hardware and software for more scalability options, and the flexibility to add new tools and capabilities.
2. Minimize vulnerability to cyber threats by working with your security software partners. Develop a cybersecurity risk management plan, and establish best practices to maintain cyber hygiene.
3. Leverage security system data for business intelligence and uncover insights to improve customer experience, facility and occupancy management, marketing and merchandising, as well as security.
4. Scale your infrastructure investment to meet your business's evolving needs by investing in cloud and hybrid cloud systems.
5. Simplify your software stack with a unified platform, enabling your team to create personalized dashboards with access to data from multiple systems.

Discover our retail portfolio and see how we can help optimize your security strategy at [genetec.com/retail](https://www.genetec.com/retail)

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. The company's flagship product, Genetec™ Security Center, is a physical security platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montréal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 159 countries.

Video surveillance:

Achieve greater situational awareness and enhance security within your retail environment with the ability to share cameras across stores and facilities, providing a common operational picture and improving incident response time.

Access control:

Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Automatic license plate recognition:

Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Operational decision support:

Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts, through policy-based procedures to detailed case compilation export.

Investigative case management:

Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Cloud services:

Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

Genetec Inc.
[genetec.com/locations](https://www.genetec.com/locations)
info@genetec.com
[@genetec](https://www.genetec.com)

© Genetec Inc., 2023. Genetec and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.