Dallmeier

NEXT-GENERATION CASINO SURVEILLANCE

WHITEPAPER

For IT Managers

MADE IN GERMANY

See more.

There are more choices to make than many think

HOW IT MANAGERS IMPROVE THEIR SLEEP – GAMING FLOOR SURVEILLANCE DONE RIGHT

Many IT managers in casino operations still view video surveillance as a completely separate issue from IT operations. However, taking a closer look and understanding the "IT impact" of modern video technology offers advantages for everyone involved.

As is well known, things develop more dynamically in high tech than in other areas. In this respect, IT and video surveillance differ little from each other. But it makes it all the more important for both classic surveillance managers and IT managers to have their finger on the pulse of the times in order to be able to assess developments and make the right decisions.

The IT-triple: more security, less complexity and lower cost

Of course, the situation is different in each casino: While in one company the strategy is to place the surveillance issue entirely in the IT department, in another casino it may be the right model to leave as much autonomy as possible to the surveillance colleagues.

But regardless of whether the end result is the complete embedding of surveillance in IT or whether security continues to be operated completely separately: there have been numerous technical and non-technical developments in video surveillance in recent years that are worth to be understood and which provide tangible advantages for the three key properties every IT manager is looking for: More cybersecurity, less complexity and lower overall costs.

Security is the number one IT concern – also in casino environments

Modern video surveillance solutions are almost exclusively IP-based. This has many advantages, but also one major disadvantage: video technology is "by design" just as vulnerable as other network-based systems. IT decision-makers are therefore well advised to at least participate in the technology decisions of their security colleagues. How are systems technically secured? Are there the security precautions known from the IT world, from protection against hacker attacks to the possibility of separating the networks even within the video system, e.g. to separate cameras and recording, to forcing strong passwords and the like? What about the geographical origin of the systems – do they come from countries with a constitutional framework or is there a danger of accidental or deliberate "backdoors" into the systems through intervention by autocratic governments?

SECURITY & PRIVACY BY DESIGN? CHECK YOUR PROVIDER!

How neutral is security testing?

How important is it to the manufacturer to obtain a neutral evaluation of the degree of security of its systems, for example by independent penetration tests during and after development?

How deep is the value added in production and development?

Deep integration usually improves the quality of total solutions and consequently the customer benefit as well. What proportion of the portfolio originates in-house? Where is production performed?

Does the manufacturer believe whole heartedly in the idea of the platform?

As with all trends towards greater "manufacturer uniformity", given the complexity of modern systems it is very important that they are open, fully support standards such as ONVIF, and allow third-party systems to be integrated easily.

How well does the manufacturer know the technology and the industry?

There is no substitute for years of experience in video security technology and a profound knowledge of the industry. The manufacturer should be able to demonstrate these qualities.

Does the manufacturer offer complete solutions or modules?

Particularly with regard to security considerations, the "everything from a single supplier" approach has advantages because the individual elements are perfectly tuned to each other.

Is there any documentation of the measures and functions for data security and data protection?

The GDPR threatens severe consequences if its principles are ignored. A manufacturer should document credibly and comprehensibly how the complex, interrelated issues of data protection and data security are addressed.

Who am I dealing with?

When choosing a manufacturer, aspects such as possible political influence in the country of origin or financial dependence on shareholder interests must also be considered.

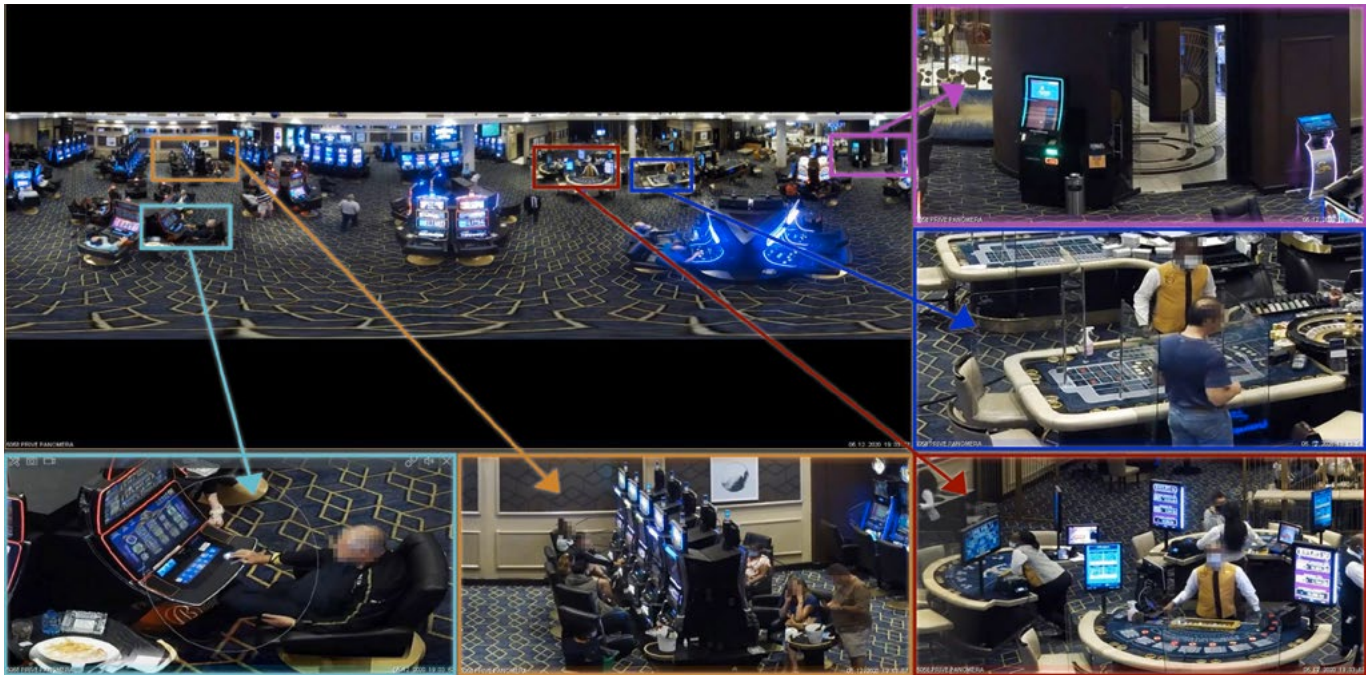
The Panomera® W8 shows a complete 360-degree hemisphere, without blind spots.

How many devices does surveillance really need?

Linked to the cybersecurity aspect, but primarily associated with cost, is the issue of complexity. It is not uncommon for IT managers, when talking to their security colleagues, to come across a whole series of procedures and set technology "truths" that are seemingly unalterable, but above all cause complexity and thus high costs and risks. A classic example is the adherence to the so-called "PTZ" (Pan Tilt Zoom) technology for the general gaming floor surveillance. These allow the operator to change the field of view as desired and to zoom in and out of certain areas. The disadvantage of these cameras, however, is that usually only a certain detailed area can be "observed". For a complete monitoring of the gaming floor, a large number of cameras must be installed, supplied with a network connection and maintained.

90% less time to catch the guy – at 25% lower cost

There are more efficient alternatives: Particularly powerful 360° cameras (see box for selection criteria) reduce the number of cameras significantly and offer an overall view of very large spatial contexts. In particular, resolving incidents and tracking one or multiple persons can be performed much faster than with these "traditional" PTZ-systems. Casinos using these systems report up to 90% less time needed to resolve situations or catch offenders.



By using modern technology, operators can oversee huge areas of e.g. a gaming floor while at the same time being able to open as many "virtual PTZs" as needed to zoom into details. Casino operators report times to solve incidents going down from 20 minutes to 3 minutes.

Assessing 360° camera technology
Choosing the right 360° camera technology requires a few considerations – below list might be worth consulting between the surveillance manager and the IT decision maker.

Imaging

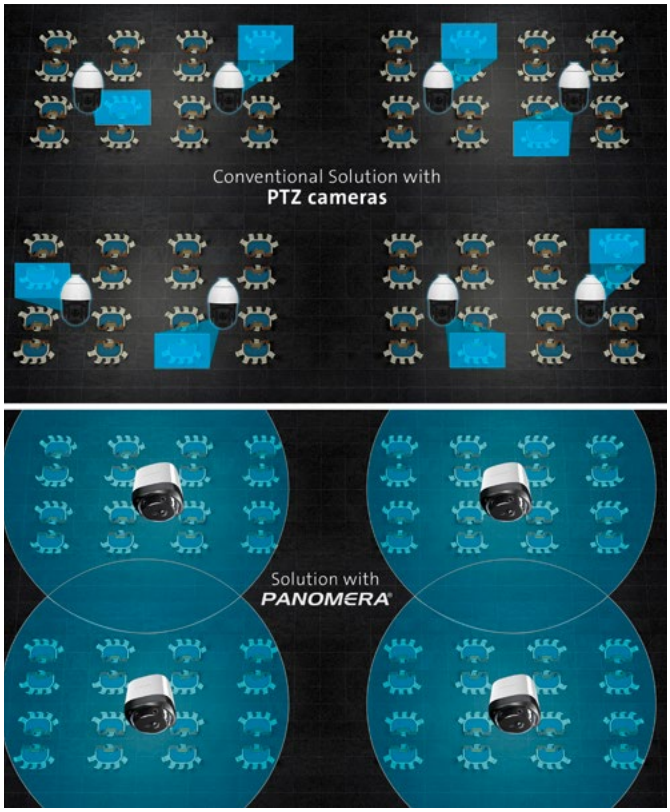
- Optimized image de-warping – "not a fisheye"
- No blind spots – including underneath the camera
- Eight 4K sensors to cover the entire hemisphere scene

Operation

- One large overview image
- Seamless tracking across the entire spatial context
- Multi-user capability: Unlimited zoom windows / screens with just one click

IT readiness

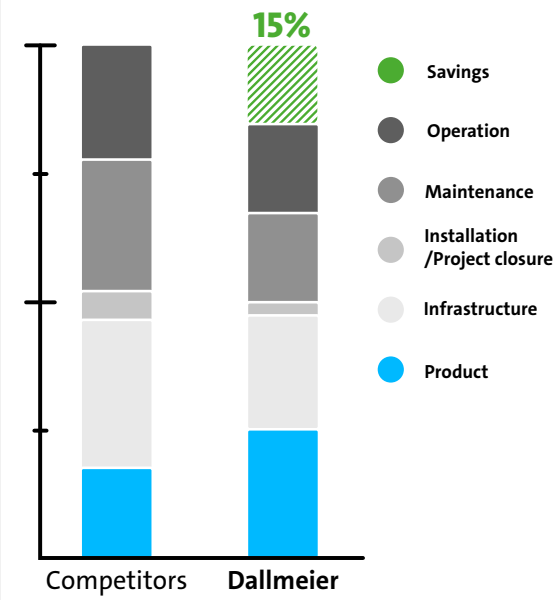
- Low number of devices
- Easy to deploy
- Latest security features
- Fits corporate ethical responsibility guidelines



One Panomera® W8 camera can replace several PTZ cameras, while at the same time providing a consistent overview as a post to limited zoom areas.

Less of everything – more for both the IT Manager and the security chief

However, it is important to look closely: Only a few systems are able to show a complete 360-degree hemisphere; most of the time, the cameras have a "blind spot" directly below the camera and are therefore only suitable to a limited extent or not at all. For the IT decision-maker – apart from the improved objective security – there is another decisive reason to consider such systems: Significantly fewer cameras – even at a higher price per camera – mean significantly less complexity and less infrastructure: fewer ports, fewer cables, less installation effort, less maintenance, less susceptibility to malfunctions and attempted attacks. In short: more efficiency and effectiveness and goal achievement for the IT department as well as for the surveillance manager.



State-of-the-art technology significantly reduces Total Cost of Ownership.

Cloud and virtual machine environments

Ease of deployment is high on the agenda for many IT managers – keyword VM capability and cloud readyness. Here, too, there are major differences between the various software offerings in the field of video security. Is there a strategy to unify hardware platforms via virtualisation solutions such as VMware? Is cloud on the horizon or already planned? Or is the traditional, on-site, separate infrastructure the preferred option? In any case, it is advisable for IT decision-makers to ensure that the systems can be designed accordingly.

Making the right decisions is not difficult – and ensures a good night's sleep

As an IT manager, making the right decisions – or at least influencing them in the sense of a modern and efficient IT strategy – is often easier than expected. A good overview of the current camera technology and future developments, a healthy portion of scepticism towards solutions from the "we've always done it that way" camp and the consideration of one's own deployment strategy is usually sufficient. And a good night's sleep for the IT manager is the result.

Dallmeier

Dedicated to quality. Driven by passion.

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

Tel: +49 941 8700-0
Fax: +49 941 8700-180

info@dallmeier.com
www.dallmeier.com

MADE IN GERMANY

See more.