Physical Security Vertical Market Assessment:

US Data Centers

In partnership with:

Brought to you by Informa Tech

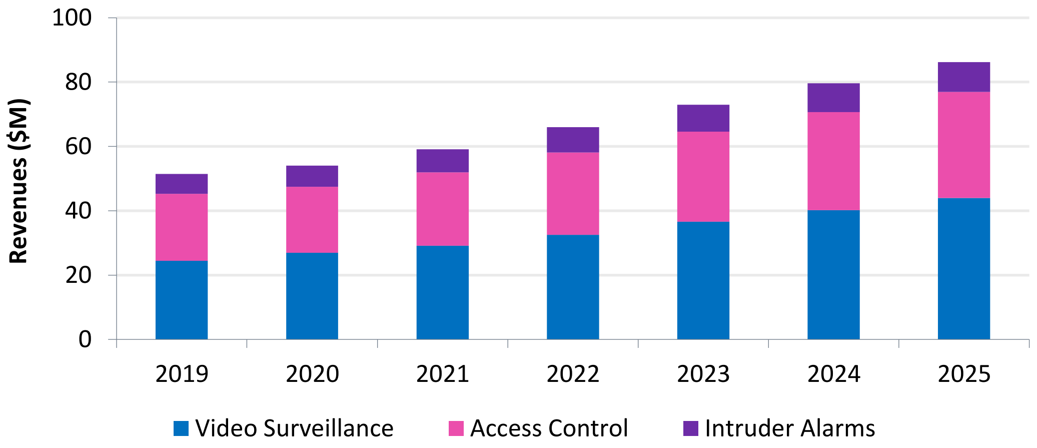
Data Centers

Digital transformation is changing how people live and work. It is also changing how companies look at their infrastructure and business processes. Over the last two years, the transition has been accelerated by the COVID-19 pandemic. Demand for consumer and enterprise cloud services increased as companies learned to work more remotely, and people learned to socialize through web-based platforms. These cloud-based solutions require data centers to support their operations.

Furthermore, workloads, such as artificial intelligence (AI), that require a large pool of powerful processors are also generating demand for data center compute. AI is one of the fastest growing technology trends globally.

Data centers protect sensitive information. Consequently, their physical security requirements are rigorous and multilayered. This includes perimeter protection solutions, managing physical access to different locations, and the monitoring of key locations for suspicious activity. Solutions also need to support process efficiency, as well as safety and compliance regulations. Data center physical security leaders have a complex and diverse set of requirements.

US market for physical security equipment in data centers



Source: Omdia © 2022 Omdia

The data center market includes all facilities (commercial and private) used to house computer systems. Data centers are typically used for telecommunications, offsite storage, and cloud services.

Video Surveillance

Video surveillance systems are used at various locations in the data center. High-resolution security cameras with analytic capabilities can be deployed at the perimeter of the site to provide early warning of any intruder. In more remote locations, integrated security cameras and short-range radar systems can provide a cost-effective approach to intruder detection and identification. Thermal cameras are also being deployed at the perimeter to detect people in difficult environmental and lighting conditions.

Thermal cameras are being deployed indoors, too. They can be used for process requirements such as monitoring servers for heat fluctuations. Traditional security cameras are also located around the data center buildings and are typically monitored regularly by the security team. At least one leading cloud provider uses video surveillance cameras to monitor the front and back of every server rack in their data centers.

Physical security end-users can take advantage of the very solutions they are supporting in their server rooms. Cloud-enabled security solutions, which provide live and recorded remote viewing and remote monitoring of the health of systems, are being deployed to protect data center locations.

Video surveillance technology development is being driven by the storage systems in the data center. Cloud, because of its scale, multi-tenancy, and scalability needs, continues to be a driver for new storage architectures. Its business model has been disruptive to enterprise data center vendors. To keep up with cloud storage equipment initiatives, equipment vendors have been adding automation and AI to their storage equipment. This has resulted in new storage management features, scaling improvements, and types of equipment, such as hyper-converged infrastructure.

Access Control

Data center physical security is complex because of the number of sites within one location. Server rooms, cooling facilities, and sub-stations are high-risk locations where entrance is on a need-to-access basis. There are also main building locations, staff break rooms, and other lower priority locations where access control is less critical.

Data centers need robust physical access control solutions. This includes physical barriers at the perimeter, such as high fencing and vehicle entrance control. Two-factor authentication using cards and a biometric component is common to ensure that those accessing the site are correctly identified. Features such as anti-passback can also be deployed. This permits an authorized individual to enter a restricted area but blocks their card from another entry so it cannot be used by an additional person. There is also a need to change permissions quickly based on variations in the security situation.

Intruder alarms

Intruder systems installed in data centers have an emphasis on redundancy. Many of the locations in a data center are staffed around the clock so traditional intruder systems can be less important. That said, there are some intruder systems installed, especially in the more remote locations which are mission critical but not as commonly entered. These include the cooling and power plants. Traditional intruder systems might also be installed around the server racks to protect these assets.

What are the market drivers and barriers?

The backdrop for the data center market is the growth in digital content and associated data. Where data used to be structured and collected in simple database records, there is now an explosion of unstructured data files from social media, wearables, IoT sensors, and computing devices, including tablets, phones, and apps. Globally, the demand for data centers is extremely high. The US market is no different, with large data center buildings located in cities across America, such as Portland, Los Angeles, Phoenix, Dallas, Chicago, and New York.

Market Drivers

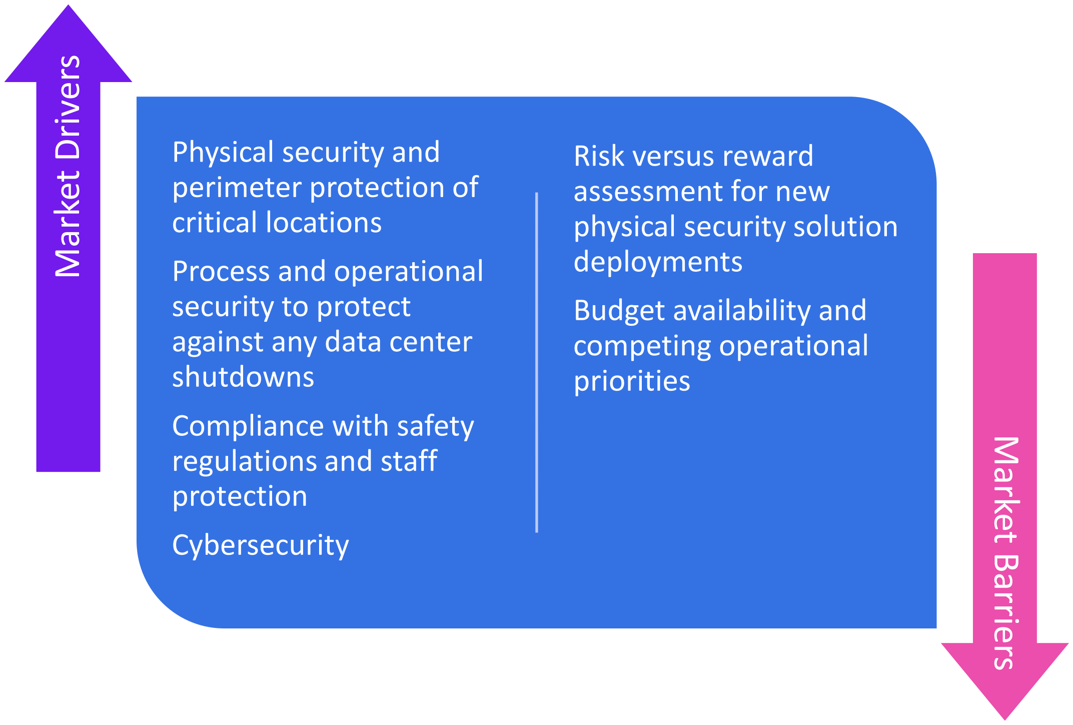
There are three main market drivers in data centers. First, the traditional security of assets and locations. This includes perimeter security applications, intruder alert monitoring (including video analytics), access control management solutions, and physical barriers to limit access. Data center location is an important consideration in the physical security decision. Some data centers are located at remote sites which suit surveillance-based perimeter solutions. Others are in city centers and need a more layered approach as the perimeter is harder to defend.

The layered security concept is one of the key principals of data center security. There are zones in a data center that require different levels of protection. In addition to the perimeter, there are general purpose buildings and staff premises, which are lower-risk sites. Beyond these locations, there are mission critical assets, such as power sub-stations and cooling facilities. These are high-priority protection locations and require more physical security than in the main buildings. Finally, there are the server rooms and racks where the data is stored. Access to these locations can require dual-credentialling and biometrics to ensure the highest level of protection possible.

The second market driver is securing the process and operational efficiency of the data center. Operational threats include server rooms overheating, energy management challenges, and the protection of support infrastructure. An example of physical security supporting this challenge is the use of thermal cameras to monitor heat fluctuations. Protecting against any shutdown in service is the primary objective.

Finally, safety compliance is a key driver with guidelines from the Environmental Protection Agency and the Occupational Safety and Health Administration important considerations for end-users.

Market drivers and barriers for US data centers



Market Drivers

Physical security and perimeter protection of critical locations

Process and operational security to protect against any data center shutdowns

Compliance with safety regulations and staff protection

Cybersecurity

Risk versus reward assessment for new physical security solution deployments

Budget availability and competing operational priorities

Market Barriers

Cybersecurity is another important consideration. Data center end-users generally have a good understanding of what they need in terms of cyber protection. Consequently, security providers need to ensure their solutions are up-to-date and understand how to build cyber compliance into the systems they deploy.

In additional to the threat from IoT devices and hacking, prohibiting unauthorized devices from entering the critical areas of the data center is important. Security solutions can support scanning and alerting to potential breaches as a key part of the overall defense against this type of threat.

Market Barriers

Data center end-users have many of the same challenges and barriers as other vertical markets. For security leaders, the payback from deploying a new solution needs to justify the disruption and cost. The physical security decision is not federally mandated, so data center operators must decide what type of security solution they think is appropriate for their site. Large multi-national operators have transparent security protocols outlined on their websites. Smaller providers may decide these solutions are not required.

Budget is also a challenge. There can be competing demands, such as the need for a new cooling system, which can override the purchase of a security solution. The benefits of the cooling system may be easier to articulate than the physical security solution. This makes funding harder to obtain. A critical task is ensuring leadership knows the risks of not deploying any security system. The consequences of any breach or intrusion are detrimental to the operational and process efficiency of the data center and could damage the trust that customers have in the service. Again, large operators often have more funds available to mitigate this threat. Smaller operators could benefit from more education on the pros and cons of deploying a new physical security solution.

Impact of the Pandemic

Unlike most end-user markets in the US, the data center market proportionally benefited from the coronavirus pandemic. The move to remote working and cloud solutions has accelerated and it is unlikely to be reversed. There has also been an opportunity to sell analytics solutions to identify face masks, occupancy levels, social distancing, and body temperature in support of health and safety protocols. COVID-19 has been a growth driver for the market and this directional trend will continue in the coming years.

However, there have been challenges created by the pandemic that affect the market. COVID-19 limited the number of people who could be onsite, as well as the way data center employees could interact with each other. This has made it more difficult to deploy new security solutions. Changes may also be made to the way data centers operate to ensure that key personnel are kept separated in order to support redundancy in the overall business.

General Market Trends

Omdia’s Data Center Practice tracks the IT infrastructure and power solutions deployed in the data center market. There are also several trends that are relevant to the overall market.

AI-enabled analytics and intelligent monitoring for data-driven decision-making is gaining traction. Companies are looking into new ways to increase productivity and efficiency to deal with labor shortages while reducing risk. Automation and intelligent monitoring capabilities are enabling the next generation of smart and connected equipment. Data can be collected in real time for almost all equipment in data centers, including electrical and mechanical, as well as IT.

Furthermore, data centers are demanding more interactive technologies with enhanced capabilities to automate monitoring and management. Automation is becoming essential to operate facilities effectively and efficiently. More efficient and sustainable construction of data centers is needed in the future. Prefabricated modular data centers

(PMDCs) offer a road to it and are gaining a lot of traction. They provide standardization, improve speed of deployment, and can be right-sized and scalable based on the client's needs.

Edge data centers are also growing in number and demanding more equipment. As demand for edge computing increases, vendors are looking into edge data centers to satisfy the increasing infrastructure requirements while meeting efficiency, remote monitoring, modularity, flexibility, and sustainability goals. Workloads computed at the edge can be mission-critical, requiring a similar or improved reliability level to that of a large data center serving multiple regions.

Market opportunities: how to win?

- Education is key to supporting data center security leaders. Systems integrators can work with equipment vendors and other solution providers to better articulate the opportunities and benefits of physical security solutions. As more data centers are built, this investment in time should reap rewards.

- Process and safety compliance represents a revenue opportunity. Most data centers will have a significant physical security installation in place already. Solutions that address the threats to process and operational efficiency in data centers could open new project opportunities for the physical security industry.

- Integration of disparate equipment and sensors is also important. Integrators can provide end-to-end solutions that offer a more complete view of what is happening on site. Technology evolutions, such as sensor integration and artificial intelligence, will also create new potential solutions in the future. End-users need help to understand what could be possible. They can then start to build these solutions into their overall security plans.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

About the Security Industry Association (SIA)

The Security Industry Association (SIA) is the leading trade association for global security solution providers, with more than 1,200 innovative member companies representing thousands of security leaders and experts who shape the future of the industry.

For more information, visit www.securityindustry.org.