STT Security Services Brings Physical Security Into Focus for Data Center Facilities

September 24, 2026

MT. PLEASANT, MI - September 24, 2026 -
STT Security Services is directing current operational attention to the physical conditions under which data center facilities operate. Those facilities house sensitive information and critical infrastructure inside rooms that can be entered only through controlled doors, loading points, and authorized corridors. In its published Data Center Guard Services description, the company sets out how access control, credential verification, surveillance, intrusion response, and emergency readiness function together so that the interior remains limited to authorized personnel while operations continue.

That combination of restricted movement and continuous availability is what separates data center work from many general commercial posts. A more open workplace may absorb visitors, vendors, and irregular public traffic without immediately exposing critical equipment. A data center is organized around limited entry and around hardware that is expected to remain available. Entry is therefore treated as the process that determines who may stand next to servers, networking equipment, and power systems.

According to the Data Center Guard Services description published by STT Security Services, personnel assigned to these locations control access points, verify credentials, and restrict unauthorized entry. The

same description states that personnel monitor surveillance systems, identify suspicious activity, and respond when a security breach is indicated. Those tasks occur at doors, corridors, loading areas, and equipment rooms. They address the physical path to the hardware rather than the network path to the data.

The company draws a direct distinction between the two domains. Cybersecurity measures remain necessary for networks and stored information. Physical security is presented as important alongside those measures because unauthorized access to hardware can create security and operational risks. Servers, networking devices, and power systems can be stolen, damaged, or tampered with if a person who should not be present reaches them. That exposure is separate from remote intrusion and appears when a badge, a visitor credential, a service entrance, or an interior door is not managed with consistency.

Jason vonReichbauer, VP of Operations and Partner at STT Security Services, described the sequence inside the building. ?Credential verification and observation have to hold at the entry points, because that is the only way the rooms that hold the infrastructure stay limited to authorized movement.?

Surveillance in this setting is described as an active watch on current conditions rather than a record created after an incident. The published account states that security personnel monitor systems in order to identify unusual activity and to respond when a breach is indicated, placing observation between an irregular movement and the equipment itself. Presence at access points is also described as a deterrent to break-ins, theft, and vandalism. The practical effect is to interrupt an unauthorized approach before it reaches the racks or the power systems that keep the facility running.

Operational continuity depends on the same physical discipline. The company?s description states that security personnel help prevent disruptions such as sabotage, equipment interference, or environmental hazards, and that they are trained to respond to fires, medical incidents, and security breaches in a manner that protects personnel and supports continuity. Emergency response still has to pass through controlled access. Responders must reach the correct room without opening the facility to people who do not belong there. The same description notes that technology plays a crucial role, while human assessment remains necessary when an event does not follow a predictable sequence.

vonReichbauer tied that requirement to the running of the facility. ?Unauthorized entry or an unmanaged emergency can interrupt operations even when digital controls remain in place, which is why physical security for data centers is a continuity function as much as an entry function.?

Data center physical security therefore applies familiar private-security skills to a narrower set of doors and to infrastructure that cannot be taken offline without consequence. Access control, surveillance, and emergency response have to operate as one posture because a failure at any of those points can expose equipment or interrupt service.

STT Security Services is a privately owned provider founded in 1973. The organization operates nationwide and includes data center facilities among the specialized environments it serves. As of September 2026, the company is part of Secure Environment Consultants and SEC SHIELD. It provides security, safety, investigative, training, and consulting services, and its personnel receive training in areas that include customer service, communication, de-escalation, situational awareness, and emergency situations. The company also employs proprietary technology for recording and tracking operational activity.

###

For more information about STT Security Services, contact the company here:STT Security ServicesCalvin Rusch800-860-1788info@sttsecurity.com1600 N. Mission St. Mt. Pleasant, MI 48858

STT Security Services

Operating throughout the USA, STT Security Services delivers a comprehensive portfolio of security, safety, and investigative solutions.

Website: https://sttsecurity.com/

Email: info@sttsecurity.com

Phone: 800-860-1788