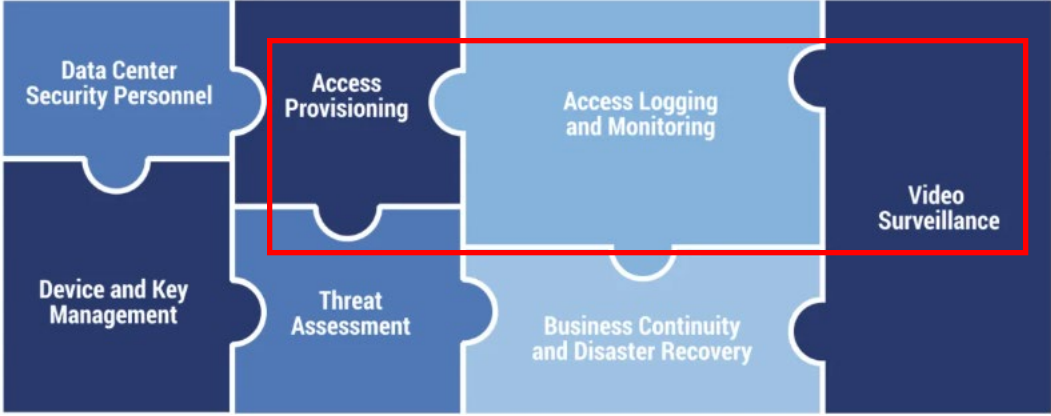


Exhibit 6

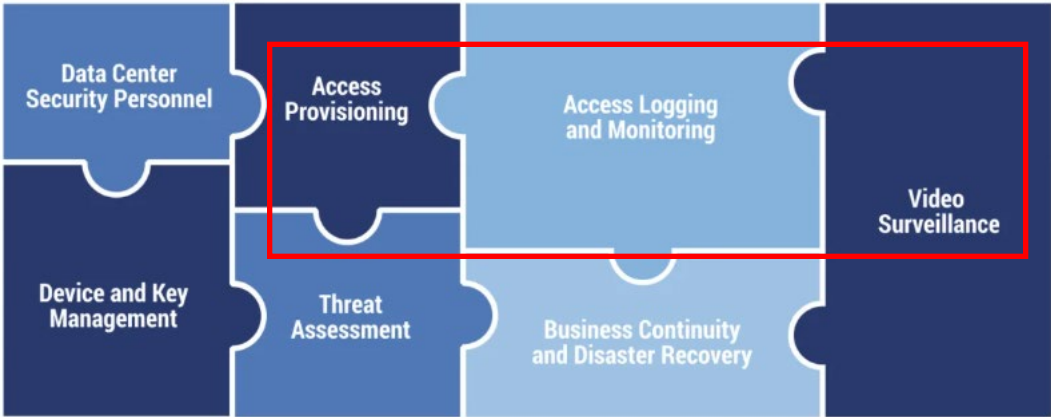
U.S. Patent No. 7,057,509 – Infringement Claim Chart – TierPoint

Claim 17	Exemplary Evidence of Infringement by TierPoint
[17pre] A method of monitoring an object, said method comprising:	TierPoint performs a method of monitoring an object in its data centers, as evidenced below. For example, TierPoint’s virtual tour illustrates a secure sign-in area that uses biometric scanning to identify visitors/personnel that enter its data centers and uses security cameras for video surveillance and monitoring. TierPoint’s Dallas-Allen Data Center  See, for example, https://www.youtube.com/watch?v=O4hj2AqYDPs

Claim 17	Exemplary Evidence of Infringement by TierPoint
	 Physical Security Security experts often discuss the OSI's 7-layer Network Security model, with the initial layer being the physical layer. In fact, physical data center security is one of the reasons many businesses choose colocation. The most secure colocation data center facilities should focus on data center security, evaluation of potential threats, facilitating access, maintaining access records, consistent monitoring, ensuring business continuity and disaster recovery, managing devices and keys, and employing video surveillance. https://www.TierPoint.com/blog/holistic-approach-to-secure-colocation/
[17a] generating identification data associated with each monitored object located at an identification gateway of a monitored environment, wherein said	TierPoint generates identification data associated with each monitored object located at an identification gateway of a monitored environment, wherein said generating identification data is performed by an identification system.

Claim 17	Exemplary Evidence of Infringement by TierPoint
generating identification data is performed by an identification system;	For example, TierPoint uses biometric sensors to identify visitors/personnel entering its data centers. TierPoint's Dallas-Allen Data Center  See, for example, https://www.youtube.com/watch?v=O4hj2AqYDPs The generating identification data is performed by an identification system (e.g., biometric scanner).

Claim 17	Exemplary Evidence of Infringement by TierPoint
	Device and Key Management When your servers are on a rack in an unlocked room, it's all too easy for someone to lift a server and walk out. A good data center provider will have options that range from a simple PIN or electronic key access to devices and areas of the data center to more sophisticated controls such as multi-factor identification and biometric scans for more sensitive areas of the facility. https://www.TierPoint.com/blog/data-center-physical-security/
[17b] generating tracking data associated with each monitored object located within said monitored environment, wherein said generating tracking data is performed by a tracking system;	TierPoint generates tracking data associated with each monitored object located within said monitored environment, wherein said generating tracking data is performed by a tracking system. For example, TierPoint generates tracking data using access logging and monitoring (e.g., video surveillance) to identify unusual patterns of behavior. Access Logging and Monitoring Sometimes, how someone is using the access they are given tells a more important story than what access is being provisioned. Data centers that log and monitor access can better identify unusual patterns of behavior that may indicate a potential risk to physical security.

Claim 17	Exemplary Evidence of Infringement by TierPoint
	Visitor Access Visitors should only receive access to the necessary parts of a data center through pre-ordained controls and proper monitoring. Secure data centers can help organizations define the levels of access needed based on the type of visitor to avoid confusion and mitigate risks. https://www.TierPoint.com/blog/data-center-physical-security/
[17c] merging and storing said identification data and said tracking data of each monitored object to form monitoring data for each monitored object; and	TierPoint merges and stores said identification data and said tracking data of each monitored object to form monitoring data for each monitored object. For example, TierPoint continually maintains access records and consistently monitors the visitors/personnel (e.g., using video surveillance). 

Claim 17	Exemplary Evidence of Infringement by TierPoint
	Physical Security Security experts often discuss the OSI's 7-layer Network Security model, with the initial layer being the physical layer. In fact, physical data center security is one of the reasons many businesses choose colocation. The most secure colocation data center facilities should focus on data center security, evaluation of potential threats, facilitating access, maintaining access records, consistent monitoring, ensuring business continuity and disaster recovery, managing devices and keys, and employing video surveillance. https://www.TierPoint.com/blog/holistic-approach-to-secure-colocation/ Video Surveillance Camera systems can help you catch a criminal in the act and can also help you present critical evidence for an investigation, trial, or insurance claim. At a minimum, your data center provider should have cameras at every entry point to the facility. Fewer windows are better, but if you can't control that, there should also be cameras on these as they are access points. Security cameras make easy targets for theft as well, so a good data center should digitally archive the data in real time. https://www.TierPoint.com/blog/data-center-physical-security/
[17d] comparing new content of said monitoring data of a monitored object	TierPoint compares new content of said monitoring data of a monitored object with prior content of said monitoring data of said monitored object.

Claim 17	Exemplary Evidence of Infringement by TierPoint
with prior content of said monitoring data of said monitored object.	For example, TierPoint compares new content of a monitored object (e.g., a visitor or personnel) with prior content of the monitored object (e.g., prior access credentials) to perform a threat assessment or identify unusual patterns of behavior.  The most secure colocation data center facilities should focus on data center security, evaluation of potential threats, facilitating access, maintaining access records, consistent monitoring, ensuring business continuity and disaster recovery, managing devices and keys, and employing video surveillance. https://www.TierPoint.com/blog/holistic-approach-to-secure-colocation/

Claim 17	Exemplary Evidence of Infringement by TierPoint
	Physical Security Security experts often discuss the OSI's 7-layer Network Security model, with the initial layer being the physical layer. In fact, physical data center security is one of the reasons many businesses choose colocation. The most secure colocation data center facilities should focus on data center security, evaluation of potential threats, facilitating access, maintaining access records, consistent monitoring, ensuring business continuity and disaster recovery, managing devices and keys, and employing video surveillance. https://www.TierPoint.com/blog/holistic-approach-to-secure-colocation/ Video Surveillance Camera systems can help you catch a criminal in the act and can also help you present critical evidence for an investigation, trial, or insurance claim. At a minimum, your data center provider should have cameras at every entry point to the facility. Fewer windows are better, but if you can't control that, there should also be cameras on these as they are access points. Security cameras make easy targets for theft as well, so a good data center should digitally archive the data in real time. https://www.TierPoint.com/blog/data-center-physical-security/

Claim 17	Exemplary Evidence of Infringement by TierPoint
	Access Logging and Monitoring Sometimes, how someone is using the access they are given tells a more important story than what access is being provisioned. Data centers that log and monitor access can better identify unusual patterns of behavior that may indicate a potential risk to physical security.