

Top 10 Security Features Data Centers Should Have

A data center is an outside location that houses equipment and information that is used for your business. This information or equipment can be accessed from a remote location. Many businesses use a data center, especially when customer information must be retrieved. This is especially true with customer service centers. When you call with a question or problem, you may get a different call center each time. However, they are able to pull up the same information every single time. This is because they are pulling that information from a data center. This allows for retrieval of information from all authorized parties at any time, which also results in consistency.

With such access, this may make one wonder how secure a data center really is. All of this information is being transferred to and from using a computer can seem somewhat dangerous, especially since much of the information is very sensitive.

That is why it is important that each data center be equipped with top-of-the-line security features that protect that information:

1. **Encryption:** Encryption is a code that cannot be cracked. The information is transferred in this encrypted form that only the computer it is going to can decipher. The information that leaves the computer is once again encrypted to be stored in the data center. This is what prevents a lot of the information that is going back and from being stolen by hackers.
2. **Password protection:** It is important for the password to remain protected. If the password is entered incorrectly, then it is important to have a security feature that locks someone out after three attempts. This prevents someone from intruding and in order to unlock it, they must answer a security question.
3. **Individual security:** This is when each individual receives their own username and password to access the data center. This means the encryption key for each user is unique.
4. **Redundant power:** A data center that runs on redundant power is one that is going to survive such incidents as blackouts. This means they are running from separate sources of electricity and they also have backup generators. That way, if the power goes out there and not at your facility, you're still in business.
5. **Verification at each end:** Every single time a file is written to disk at the data center, their integrity is verified. They are verified each time they are written to the disk. If verification fails, it is transmitted to an identical server.
6. **Protocol security:** Protocols such as HTTP are vulnerable to hackers, so a secure data security system uses one that hackers do not target.
7. **Firewalls:** The firewall that is used should be similar to those used on home computers so that the business can connect with backup software and not be locked out.
8. **Restricting remote access:** This only limits access to certain IP addresses. This is so someone cannot access the data center from another location when they aren't supposed to.
9. **Virus protection:** Viruses come in all shapes and sizes and the data center must be protected as well. Virus protection keeps the data center virus free.
10. **128-bit Secure Socket Layer (SSL):** This is what you want to see to make sure information is not retrieved or corrupted in any way.

So if you're looking for a data center that can make your business as successful as you want it to be, these are ten security features that you can look for that will make a large difference in how securely you do business. You can also confidently ensure your customers that their information is safe.

About the Author

Fully Managed Hosting with complete end-to-end management of your mission-critical data will help your business achieve more up time culminating in greater revenues and success. Managed IT solutions will provide the service, hardware and ensure the care of data back-up and recovery.