Omnisite Server Hosting Specifications

Omnisite understands that the protection of your data within our GuardDog cloud-based software system is of utmost importance to your organization. To that end, we have created a hosting solution which is far superior to what can be achieved by the budget of a typical facility manager. It is not to say that it can't be done; it can. However, it would be very expensive, and likely not practical or economical to provide your own system which would have the same protections, or level of maintenance. Following is a discussion of how Omnisite protects your critical data. For additional information or questions, refer them to Tom Ward, President, Omnisite email: tward@omnisite.com

The Hosting Facility

Whilst keeping security as our number one priority, OmniSite has upgraded from using one hosting facility to using Amazon's services, or AWS, which provide several hosting facilities and can host our servers in a more secure way. AWS also provides multiple hosting facilities that are spread all around the world. Below is a 3D rendering of how one of their facilities looks like.

AWS has provided some examples of how they have secured each facility they own. They describe 4 layers in their documentation: perimeter, infrastructure, data, and environmental layers.

Perimeter Layer

AWS data center physical security begins at the Perimeter Layer. This Layer includes several security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. Scroll down to learn more about the types of security measures we have in place within the Perimeter Layer of the data centers we operate around the world.

Infrastructure Layer

The Infrastructure Layer is the data center building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer.

Data Layer

The Data Layer is the most critical point of protection because it is the only area that holds customer data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, we deploy threat detection devices and system protocols, further safeguarding this layer.

Environmental Layer

The Environmental Layer is dedicated to environmental considerations from site selection and construction to operations and sustainability. AWS carefully chooses our data center locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity.

For more information regarding the data centers in Amazon's facilities, please go to their official website to read on how they deal with security, emergencies, and other important maintenance to keep all our data, and yours, secure. Link: https://aws.amazon.com/compliance/data-center/data-centers/

Amazon Web Services (AWS)

What are Amazon Web Services? In short, AWS is what is known as cloud computing. Cloud Computing is an on-demand delivery of IT resources over the internet with pay-as-you-go pricing. This means that instead of buying, owning, and maintaining physical data center and servers that can be hosted in a secured facility where you would "rent" space to host your hardware, you can now access technology services, such as computing power, databases, and storage on an as-needed basis from a cloud provider. These services are maintained by Amazon using their own hosting facilities, and all we must do as their customers is "rent" space in their servers, which are maintained by them, to run our applications using their hardware. This facilitates the creation of any application by not worrying about hardware needs.

Redundancy

One of the many advantages of using AWS and their cloud computing resources is that a virtual server can be created in seconds. A virtual server can be described as a small computer that can run just about any application inside a larger computer that uses the normal hardware to run. These virtual servers are very flexible in how you want them to perform. You can customize how fast the server will be, the type of storage used, and storage size.

Since servers can be created instantly, AWS provides many ways to add extra redundancy to help businesses avoid any downtime for their applications. The biggest redundancy factor they provide is that they own many data centers all around the world. This makes it possible to host the same application across multiple servers across multiple parts of the world. Amazon separates each data center by regions, in which each region contains multiple data centers that can be accommodated for extra redundancy. As an example, AWS has a big data center region in Ohio, in which they have split multiple data centers within this region (called Availability Zones) where applications can be hosted with security and redundancy within the same region. If an AWS user would like to host their business applications in one region, they can choose to create multiple virtual servers hosting the same applications in different Availability Zones within the same region so the applications can thrive in the case of a critical disaster in one of the Availability Zone's data centers.

For OmniSite, we have utilized these resources to include redundancy they provide. We recently started using a service called Kubernetes, which allows us to manage our servers automatically without having to intervene manually. This service can detect when an application goes down in

a server and automatically restarts the application, so we don't have to manually intervene. With this service combined with multiple servers carrying our duplicated applications across different Availability Zones within AWS allows us to have extra redundancy so all our applications, and your data, stays safe and available.

Database

Following the same ideas from our applications, our database has also changed to include extra redundancy, so all your data stays secure. With AWS, we were able to create a database that "mirrors' into another Availability Zone within AWS. This means that we have our database running on one region, and a duplicate that gets updated at the same time as the main database in another zone. This allows us to prepare for any kind of disaster if it were to happen to an entire Availability Zone in AWS.

AWS also provides ways to create back ups for our database. We have built a backup plan where daily backups are created, and we have also created a daily backup plan. With these plans in mind, we can restore all your data in case of a massive disaster. As an extra step, we also implemented a way to copy each of the backups into another region within AWS, in case of a complete breakdown of a whole region. So, with multiple Availability Zones being used for the database, daily and hourly backups, and copies of these backups into another completely different region, your data will continue to be secured.

Compliance and Certifications

AWS participates in the voluntary Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) Self-Assessment to document its compliance with CSA-published best practices. The CSA is "the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment". The CSA Consensus Assessments Initiative Questionnaire (CAIQ) provides a set of questions the CSA anticipates a cloud customer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions, which can then be used for a wide range of efforts, including cloud provider selection and security evaluation. For more information, please visit the following website: https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/aws-risk-and-compliance-program.html

Disaster Recovery

Disaster Recovery Planning: Your Insurance when Disaster Strikes

Disaster is uncontrollable and often unpredictable – fire, floods, tornados and even power outages are just a few ways your business can be disrupted. Both natural disasters and disasters related to human error can be detrimental to running your business, and **disaster recovery** (DR) can be a hassle when you are forced to define solutions during a calamity.

Having a **disaster recovery plan** can relieve some of the stress associated with recuperating from unexpected events and keeping your monitoring systems operational for your customers. Think of it as insurance for getting your systems up and running again and maintaining the security of your data and important information. Because your GuardDog data is hosted off site in multiple redundant facilities within AWS (which also backs up that data, again offsite), your data is protected from a disaster at your facility, regardless of the type, natural disaster or employee vandalism. Anywhere in the world where you can reach the Internet with a smart phone, tablet or personal computer, you can again have immediate access to your data, should your facility incur a disaster.

The ultimate piece of mind. However, piece of mind does not stop there. The GuardDog software also backs-up your data in real-time all day long each day. In the event of a disaster, there are no more concerns of recovering data from damaged PCs on site. This is done for you automatically as part of your annual subscription fee to OmniSite's services. Your annual subscription fee to Omnisite acts as not only your wireless connection to your critical equipment, but also protects critical data that can be difficult to preserve during a disaster situation. Our tech support is standing-by 24/7, at no additional charge for subscribed customers, to guide you through any problem, even a disaster.

Creating a Plan for Recovery

There are certain questions you should have at the top of your mind when you are preparing for disaster.

- What data is most important to your business operations?
- How long can your business operate without the availability of critical data?
- What type of disaster is likely to occur in your area and how can you prepare?
- What offsite backup accommodations have been made for your systems?
- What is the cost comparison between recovering from disaster and investing in a recovery plan?

Omnisite provides this plan for your Omnisite data. There's nothing else for you to do.

What Planning Ahead Means for Your Business

- Reduced risk for human disaster
- Guaranteed availability of backup systems
- Connectivity during outage
- Minimized business downtime
- Positive customer experiences, even during disaster

Business Continuity

Being able to continue operations after a major disaster is important to any business. A **business continuity** plan can be the piece of the puzzle that keeps your critical business functions available even if your offices or equipment are not accessible. Business continuity planning usually arises when you are developing your disaster recovery plan, and should include things like a business redemption plan, business recovery plan and a contingency plan. When you are constructing your plans, you want to consider identifying a secondary worksite that can be set up for your employees or a team of your staff to continue working. With OmniSite's data, this is done for you; however, you'll want to have a similar plan for your local facilities.

Having a place for your key personnel to work can be the difference between shutting down your business after the interruption and continuing to conduct business as usual. Proper planning also helps build customer confidence in your operations, and it can even give you a competitive advantage. For organizations that are regulated by compliance, business continuity can help you maintain legal and other such requirements. The most significant benefit is, of course, continued operations.

Thanks to the power and flexibility of AWS, we can work from anywhere in the world and access any information you may need amid disaster whilst keeping security in mind. AWS contains very robust rules within their networking configurations that allows us to limit the number of employees that can access the necessary servers and/or databases through the AWS website to continue operations.

Don't find yourself unprepared for a disaster. Power or connectivity losses don't have to mean a disruption of your business. **OmniSite's Business Continuity Plan** ensures your data and support is always ready when you need it. Contact us today to learn more about how we can help you stand amid disaster.

Offsite Backup

Your business relies on electronic data. Imagine losing all your data simply from a computer or server hard drive failure. What is your backup plan? Can your business survive? Having an **offsite backup solution** is a proactive way to secure the most important information to your business and to maintain business continuity.

At Omnisite our comprehensive **offsite backup services** are designed to run in the background in the cloud and provide real time data replication to a secure server within our data center. So, whether disaster strikes, or you suffer an equipment failure, we can restore your data anytime, anywhere. And there is no need to buy any additional hardware. We provide everything you need for **offsite data storage**.

- **Customizable backup solutions**. Whether you want your data updated and backed up every minute or once a week, we've got you covered
- **Extremely affordable price points**. Our "no hidden fees" agreement supplies automatic data backups, wireless service, and technical support all without hidden surcharges or unexpected price increases
- **Fast and easy setup**. Within five minutes you can have the GuardDog website up and running on your machine.
- **No charge to recover data**. Many solutions charge a hefty fee to retrieve your data. At Omnisite, the moment your systems fail, you can focus on getting your systems back up and running instead of worrying about the cost of data recovery.

Having a backup site should be hassle free and reliable, allowing you to rest easy knowing that your data is being backed up in a secure location. Whether you are choosing offsite backup as a means of disaster recovery or another layer of redundancy, Omnisite can offer an option that gives you the peace of mind you need. We like to think in terms of how your business benefits so here are a few advantages of choosing Omnisite for your **offsite backup solution**.

- No need to purchase additional hardware
- Protection for your data 24/7
- Compatible with Windows, Mac, Linux
- Disaster recovery protection
- Customizable options to meet your needs
- Single or double encryption
- One flat fee, no hidden charges
- Technical support from Omnisite staff or one of our trusted partners