April 2018

Blazemark®

critical data when you need it most

Software and Security FAQ's

What is Blazemark?

Blazemark, is an "All Hazard Pre-Incident Planning" program compliant with NFPA 1620, NIMS and FEMA. When seconds can be the difference between life, death, and property loss, first responders and facilities personnel need critical information quickly and effectively to allow them to make the best strategic and tactical decisions necessary to save lives and reduce risk to themselves. Pre-planning your building(s) and other hazards is essential to providing the critical data when you need it most.

Blazemark is very intuitive and extremely user friendly, making your building, property and infrastructure details available to responders. Blazemark is a technical tool for non-technical users.

Our clients include Fortune 100 companies (pharma and manufacturing), healthcare systems, campus and school district settings, and governmental agencies. Preplans span the breadth of office buildings, commercial buildings, malls, manufacturing facilities, test labs, oil train lines, high-density traffic interchanges, airports, and much more. Using preplans has saved our clients and their communities a lot of money by helping to lower insurance premiums and ISO ratings.

Blazemark is a web application, Software as a Service (SaaS), hosted "in the cloud." There are a few basic parts to consider:

1. The application known as Blazemark
2. The server(s) that host Blazemark
3. The server(s) that host our Database

What is the Cloud?

If you're not familiar with the cloud, the first question you'll want answered is "What is cloud computing"? Cloud computing is a way of delivering computing resources to run websites or software applications that are stored or accessed off site via the Internet.

This allows Fire Planning Associates to concentrate on what we provide (the preplanning and software architecture expertise), and leverage the extensive (and expensive) hardware and networking and security services of a cloud services provider at a very reasonable cost.

Where is my data?

The first question we usually address after introducing new clients to cloud computing is "Where is my data?"" Since the "cloud" seems like an intangible place, we remind clients that they may

already be using the cloud in other aspects of their lives and businesses, such as online banking, Google mail, LinkedIn, DropBox, etc.

In the case of Blazemark, your information is stored at data centers hosted by Flexential (formerly Peak 10 and Via West). They have global clients hosted through the use of 41 data centers, housing over 4,200 corporate clients with 3+ million square feet of facilities. (We welcome all of our current and potential clients to join us in a tour of these impressive facilities at any time.)

What is required to support a cloud service?

The significant value of Blazemark's cloud-based solution is the speed in which you can deploy pre-incident plans with very little resources required. Since everything is hosted off site, the technology requirement is as simple as a **modern** web browser and an Internet connection – including on a cell phone. With the cloud, we do all the "heavy lifting" for your organization as there are no server and infrastructure requirements and no additional IT workload to administer and support Blazemark.

There is basically nothing to install! Updates are automatic.

Can I use mobile technology with cloud-based applications?

The advantage of cloud-based technology is that the only requirement is access to an internet browser, such as Google Chrome, Firefox or Safari. Using Blazemark with mobile technology is natural, as any updates will be seen by all connected users in real time. What better way to keep all on-site and off site stakeholders up to date on situational status?!

What if I lose or break my hardware (laptop, tablet, phone, etc.)?

Because data is stored in the cloud, it is not dependent on your device. You can literally grab a new device, get Internet access, login, and never miss a beat. All your data is there, and you'll never have to worry about data transfer again.

You should be certain you use proper security on your physical devices to protect your data. Devices can be lost or stolen! Should such an unfortunate incident occur, you should take steps to change your password immediately and inform us so we can help monitor your Blazemark account.

What if I don't have an Internet connection?

No problem, all Blazemark Pre-incident plans can be exported to a PDF file at anytime for printing, email, or local drive storage for off-line viewing if needed. Just be sure to update the "hard copies" so that you are not using incorrect data in the field!

Is software through the cloud more expensive than my current solution?

No! A local emergency service just starting off can begin today with less than $1,000. Our subscription-based cloud solution requires less upfront cash investment in IT infrastructure. And in most cases, had you tried to host yourself, that infrastructure may only have a shelf life of 2-4 years. The cloud allows Blazemark to leverage new technology, passing it on to our customers, while also providing the flexibility of being able to easily scale up or down usage as needed.

How often are updates performed, and who is responsible for doing that?

Our cloud hosting provider is constantly making feature updates, enhancements, security and performance improvements to the underpinnings of our application delivery. Since Blazemark is a cloud-based solution, all Blazemark application updates and upgrades happen globally and are part of your annual subscription. In most cases you won't even know that it has happened until we let you know of a new or enhanced feature, or you are pleasantly surprised to see improvements appear.

How is my data backed up?

The Blazemark database is continuously backed up in another data center for an extra layer of redundancy should any major emergency hit our primary servers.

Our cloud-based hosting services provide the redundancy of 41 centers throughout the world, data backup and data recovery services. We view our data backup as another function of security measures as well as it is backed up in multiple physical locations. This is an excellent consideration for *business continuity* with many organizations; critical data is stored off site and backed-up, accessible from afar if you have a local catastrophic emergency, and off the local platform making it harder for those for those wishing to do your company cyber harm.

What about data center down time?

We do perform nightly updates, so there is a brief period of a few minutes when the system is updating and re-starting. (A future improvement will be to go to higher availability servers and continuous updates.)

How do cloud-based solutions secure my data?

We understand the importance of IT data security and compliance for our customers. Our data centers deliver a host of security services, compliance services and solutions aimed at helping us navigate and protect you from the ever-changing regulations and threats that target companies of every size in every industry. In doing so, we enable our clients to focus on their business without unnecessary data security and regulatory compliance concerns.

Security is one of the most asked about topics regarding our cloud-based Blazemark solution. Our solution has multiple layers of security to protect data with extremely high security standards.

Blazemark itself uses industry standard SSL (Secure Sockets Layer) for the entire web application. All of your data – from login to logout – is encrypted before being sent over the Internet (your browser will indicate that we use https secure protocol). Our chat service is similarly secured. Our user passwords require a high standard of patterns to encourage strong passwords.

Our cloud provider security addresses issues such as identity management and privacy through three layers of security.

1. **Physical security** – securing the physical location of hosting servers through steps such as; video surveillance, monitoring, dual-factor access controls and staff performs recurring walkthroughs at each data center. Our data centers are continually reviewing physical security and investigating new technologies and methods to strengthen its current procedures. This also includes stringently followed policies on authorized access lists, identity verification, access badging, access segregation and rules of conduct, client temporary access, visitor access, data center access controls, personal identification number, biometric scanner, staff data center access approval and training.
2. **Logical security** – firewalls prevent security breaches from Port Scanning (bots pinging IP addresses on multiple ports, mechanically looking for a way to get in somewhere). We employ multiple methods; policies, procedures, technical controls and training to ensure that appropriate engineering principles and operational procedures are in place to support the data center information security objectives. Industry-leading firewall hardware to protect all company applications and data are being used. As part of this logical security effort, we maintain a very strict policy regarding allowed traffic. External and internal traffic is monitored continually by the data center's security administrators. In addition, all back-office systems are protected by industry standard SSL (Secure Sockets Layer). Utilizing SSL allows documents and other information to be sent securely over the internet using an encryption protocol. Antivirus software is deployed on all data center owned information systems.
3. **Data backups and encryption**. Our business-class hosting includes far more security than most individual companies would provide on their own premises. The communication path between a user's computing device and hosting server(s) is highly encrypted, and access to the physical server racks in data centers are tightly secured and as previously noted requiring biometric scanning and employ 24-hour security services.

Redundancy is also a form of our security. Your data is backed-up to off-site locations in a server environment that is fully redundant. This means that there is not a single point of failure that would prevent access to the data.

Other Security Aspects

All of our clients have their own secure URL to access their pre-incident plan account. Within Blazemark your company can assign user roles such as read only, author, admin and secure notes viewing. Information can be further segregated to what and who can see views in the mutual aid section.

We use Cloud Flare as a further layer of protection against security breaches and denial of service attacks. All organizations can track user access and viewing in real time through activity logs.

Real World Security

Sorry to say… despite all the hard efforts and expense of building a highly secure system, most data breaches come from poor security practices by the **end user**. Scribbling down passwords or sharing logins is not good practice. We recommend using products such as 1Password.

We would be happy to make a customized "enterprise level" security plan upon request by clients. Such accommodations can include: password expiration, inability to use old passwords, limit to one logged in session per user at a time, expire an account after inactivity, verification code, captcha for sign in, captcha for sign up, two-factor authorization.

This was a very informative FAQ sheet, but I need to ask a real person questions about my company's unique data security needs.

That is absolutely no problem. Feel free to request a meeting with our Product Manager by emailing info@blazemark.com