ATI Est. 1983
Advanced Telecommunications of Illinois, Inc.

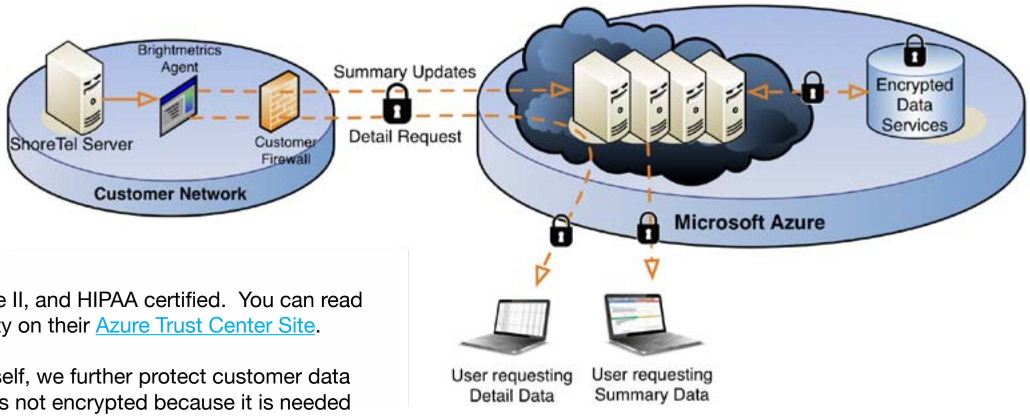
brightmetrics
www.brightmetrics.com

BRIGHTMETRICS MAKES IT POSSIBLE

ShoreTel Reporting & Data Analytics Services

For more information about Brightmetrics, or a free trial contact your ATI representative

Brightmetrics takes data security very seriously. Our service provides multiple levels of protection to make sure customer data is never exposed to unauthorized parties. We break our security into four distinct areas.



Secure Hosted Facilities

Our first level of protection is a secure hosting environment. Brightmetrics is powered by Microsoft's Windows Azure, which means our services run in one of Microsoft's secure Azure datacenters. Microsoft's Azure platform is ISO 27001, SAS70 Type II, and HIPAA certified. You can read more about Microsoft Azure's commitment to security on their Azure Trust Center Site.

Beyond the security offered by the Azure platform itself, we further protect customer data by encrypting it within our database. Numeric data is not encrypted because it is needed for calculations, but all identifiable text data such as workgroup names, trunk group names, employee names and extensions, site names, etc, are all encrypted using 256-bit AES encryption[1], the same level of encryption required by the U.S. government for top-secret information[2].

Encrypted Data Storage

Moreover, the data is not encrypted with a single key that our front-end systems use to connect to the database, as is the case with many database encryption systems, but rather with each user's password, which means that the application-level controls that restrict each user to their own company's data can not be subverted to allow access to another company's data -- unless you have a valid username and password that has been granted access to a company's data, that company's data simply can not be decrypted.

Think of it like this: each company's data is stored inside a locked box. Each user who has been granted access to the company has a copy of the key to that lockbox, which is stored in another locked box. The key to each of those user's boxes is that user's password. If a user is removed from a company, their lockbox and the key it contains are destroyed and they can no longer unlock the company's data.

As is best practice, we do not store any user passwords in the clear or even with reversible encryption, we store only a one-way SHA-256 hash[3] of each user's password, which is sufficient to determine if the correct password has been provided when the user logs in but does not give anyone a way to determine the actual password itself -- only the person who sets the password knows it.

For system maintenance we do have our own key to the lockbox as well, which we need if you forget your password (otherwise if you lost the only key the data would be completely irretrievable and you would have to delete your company and start over). You can think of it like an emergency key that's kept in a safe in a different building that only authorized people can access. Our general support and systems management staff does not have access to this master key. For example -- for support, or assistance in creating reports on your account, you will need to explicitly add a Brightmetrics engineer as a user on your company and can then remove them after any necessary support is provided.

Limited Data Storage

All of those protections are in place for what is a limited set of data to begin with. We do not store detailed call records, only summary aggregate data. The total number of calls and call minutes for a given user during a given hour according to call type, for example. We do not store the CallerID of callers, the numbers users dial out to, the length of a given call, or any such detailed or protected information, only the bare minimum that is required to provide our dashboard data and to run summary reports. Whenever you drill down through the charts to the individual call level or run a detail report, we are making a live query to the ShoreTel MySQL database to get that data and then sending the results to the browser -- it is not retained in any permanent storage.

Encrypted Transmissions

Finally, all data transmitted from the agent to our servers and from our servers to the end user is encrypted with the highest level of SSL encryption available. https://webapp.brightmetrics.com/ has a 2048-bit Extended Validation (EV) SSL certificate, capable of 256-bit AES data encryption.

Brightmetrics, Inc
1129 Industrial Ave, Suite 206
Petaluma, CA 94952

707-238-4455
info@brightmetrics.com
http://www.brightmetrics.com

[1] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[2] http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf
[3] http://en.wikipedia.org/wiki/SHA-2