

## Cloud-based data security for a cloud-based world

A recent survey suggests 85% of IT professionals are confident<sup>1</sup> in their cloud vendor's ability to provide a secure computing environment.

This increased trust is helping organizations feel more comfortable placing confidential information in the cloud.

What would happen if your cloud - private, public or hybrid - were breached? Could the exposed information be used against you or your customers?

If left unencrypted, the data loss could be catastrophic, both in terms of monetary damage and loss of customer trust.

What if you could ensure the availability, performance and security of your data in the cloud without making wholesale changes to your applications or IT infrastructure?

### Contact us

[sales@gazzang.com](mailto:sales@gazzang.com)

888.650.1112

### Data protection that enhances cloud computing

What's the first thing that comes to mind when you think about cloud computing? Is it the *flexibility* and *availability* of delivering on-demand scale-out compute resources, applications and data? Is it *ease of use* or *performance*? Perhaps it's *affordably* adding (or retiring) software, hardware and infrastructure on an as-needed, pay-as-you-go basis.

However you think about it, there's no denying the impact of cloud computing. In fact, according to Forrester Research, cloud computing will be a \$241 billion market by 2020<sup>2</sup>.

Increasingly organizations are storing sensitive data - email addresses, account information, patient records and intellectual property - in the cloud. This is compounded by the emergence of big data, where the proliferation of digital devices and low-cost cloud storage are helping create and store data on a massive scale.

Before you can truly maximize the value of this data deluge, you first need to protect the data from risk of unauthorized access or attack.

### Gazzang ezNcrypt

Gazzang ezNcrypt can help ensure the availability, integrity, performance and confidentiality of your business information. This includes sensitive customer data as well as proprietary company information such as scripts, Java byte code, logs, intellectual property or any executable file stored on disk.

Our cloud-based software transparently encrypts and secures data "on the fly" whether in the cloud or on premises, ensuring there is minimal performance lag in the encryption or decryption process. Advanced key management and process-based access controls enable organizations meet compliance regulations and allow users to store their cryptographic keys separate from the encrypted data.

Access controls provide out of the box rules for controlled, protected access to sensitive information. Gazzang ezNcrypt now includes Dynamic Kernel Module Support (DKMS), which supports virtually any Linux kernel version, ensuring maximum uptime for Gazzang customers during a security patch or kernel modification. This support is delivered via RPM and Debian packages.

\$5.5M

The average cost of a data breach in 2011.<sup>3</sup>

## Advanced key management

- Stores keys separate from the encrypted data to ensure a data breach does not also result in the loss of the cryptographic key
- Symmetric key is secured by certificates, fingerprints and other advanced methods to ensure secure and controlled access

## Transparent data encryption

- Protects data 'at rest' resulting in no noticeable performance impact
- Requires no complex changes to databases, files, applications or storage
- Encrypts sensitive data within data files to prevent access from the operating system

## Process-based access controls

- Restricts access to specific processes rather than by OS user
- Limits data availability to only those who need it
- Parent/child controls provide maximum flexibility and control by letting child processes inherit access from a parent

## Encrypt and decrypt structured and unstructured data

- Includes ALL databases, applications, scripts and files running on a Linux operating system
- Secures personally identifiable information, intellectual property, log files and any other sensitive data that could be considered damaging if exposed outside the business

### System Requirements:

- Linux kernel 2.6.19 or higher. Red Hat & CentOS can use 2.6.18-92 or higher
- Supported Linux Systems: CentOS, CloudLinux, Debian, Fedora, openSUSE, Red Hat, Scientific Linux, Slackware, Ubuntu and more.

### Helps meet compliance guidelines for:

- PCI-DSS
- HIPAA, HITECH Act
- FISMA, FedRAMP
- FERPA
- FDA
- EU Privacy

1. [http://www.cio.com/article/703064/How\\_Secure\\_Is\\_the\\_Cloud\\_IT\\_Profs\\_Speak\\_Up](http://www.cio.com/article/703064/How_Secure_Is_the_Cloud_IT_Profs_Speak_Up)
2. <http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702>
3. <http://bit.ly/GDqJuv>