Data security and availability are key concerns for risk management and compliance when cloud-service providers manage customers' data. Barracuda Networks provides cloud-based services for email security delivered as pure cloud-based SaaS and as hybrid solutions integrating cloud, hardware, and software components. The purpose of this whitepaper is to provide information about the architecture of Barracuda Network's multitenant services for email security and the standard practices followed to ensure the security and availability of customers' data. The information presented here relates to:

- The Barracuda Email Security Service including email encryption through the Barracuda Message Center

- The Barracuda Spam & Virus Firewall

    - Cloud-based aspects of Energize Updates.

    - Cloud Protection Layer

    - Central management through the Barracuda Control Center

    - Backup of configurations to the Barracuda Control Center

    - Email encryption through Barracuda Message Center

The various aspects of data security described below include:

- Physical security of data

- Technology safeguards that protect data

- Measures for business and data continuity

- Privacy and confidentiality

Data Security

Physical safeguards

Two-factor security: All data centers and colocation services that Barracuda Networks uses to provide cloud services are protected against access by unauthorized personnel. Each location implements a sign in and ID check before granting access to personnel. Most of the colocation facilities require two-factor security for access using a pass code and a biometric scan. Security checks are required at multiple locations inside the data centers. While different data centers apply security checks at different locations, these security checkpoints typically include:

- The building entrance

- Entrance to the colocation facility

- Entry to a specific cage within the colocation facility

Limited access: Barracuda Networks does not permit outside (nonemployee) personnel to access data centers and other physical locations. The list of authorized personnel is strictly controlled with designated members of the Barracuda Networks operations team having access. Permission to enter a location is only granted on an as-need basis. In special cases, Barracuda Networks development engineers may receive access to facilities.

Technology safeguards

Protecting data in motion: Barracuda Networks encrypts data using industry-standard technologies to prevent unauthorized access to data during transmission to and from data centers. These include:

- Secure HTTP: a combination of HTTP with SSL which provides encrypted web communication as well as verification of web servers' identities

- SSL (Secure Sockets Layer): provides secure transfer of email

While these technologies are available to all customers, TLS must be configured for each domain.

Digital certificates: Industry-standard certificate authorities (CAs) provide all publicly accessible certificates used by Barracuda Networks' web and email servers. These include, but are not limited to, VeriSign and GeoTrust. To request a digital certificate, a certificate signing request (CSR) is generated. The CA contacts a named person in the operations team to ensure validity of the request.

Strength of the private key: The US National Institute of Standards and Technology (NIST) has advised against using 1024-bit keys for RSA-based encryption. Instead, NIST recommends using 2048-bit keys. According to NIST, 2048-bit keys should provide adequate protection against brute force attacks until the year 2031. All certificates used by Barracuda Networks use 2048 bit security and are signed RSA Encryption.

Protecting data at rest

Emails marked for encryption through the Barracuda Email Security Service and Barracuda Spam & Virus Firewall are protected at rest. This includes all encrypted emails stored at the Barracuda Message Center. Advanced Encryption Standard (AES) with 256-bit cipher provides high-grade encryption. Barracuda Networks physically stores data encryption keys separately from the encrypted data providing an added layer of security.

Per-recipient keys for email encryption: Emails transferred to the Barracuda Message Center (BMC) from either a Barracuda Spam & Virus Firewall, or the Barracuda Email Security Service are encrypted using separate keys for different recipients.

These encryption procedures and technologies ensure data remains secure during storage.

Protecting the infrastructure

All of Barracuda Network's cloud servers run an operating system based on a hardened, stable Linux kernel which has undergone strict scrutiny by top security researchers. All production servers are also secured following industry-standard best practices for security and hardening.

Ensuring Business and Data Continuity: Barracuda Networks employs procedures to ensure that customers' data is accessible if faced with operational issues, disasters and increased demand.

High-availability servers

A dedicated Barracuda Networks operations team continuously monitors all servers and services for faults, errors and other outages. Barracuda Networks uses state-of-the-art tools and technologies to ensure all services are always available. If a server fails, services automatically migrate to redundant servers.

Servers are provisioned to ensure N+1 redundancy of components. If the N+1 redundancy is compromised due to an outage, a dedicated operations team allocates and provisions new servers or needed components to restore redundancy levels.

Storage redundancy

Data is stored on either enterprise-class disk drives or Solid State Drives (SSDs) to ensure appropriate levels of performance. In the event of single failures, data remains available for continued access using industry standard technologies like Rapid Array of Inexpensive Disks (RAID).

Geographic replication

RAID is augmented with proprietary Barracuda Networks technology that replicates data to at least two different data centers that are widely separated geographically. This technology ensures that data remains available for access even if a catastrophic failure occurs at a data center.

Power security

All locations have redundant, independent power circuits including free-standing generators. All systems are backed up by N+2 battery power. This allows UPS maintenance without risking any downtime.

Multi-tenant architecture

All services are built on multitenant architecture to provide scalability and data isolation.

Data isolation: Barracuda Networks' multitenant architecture ensures different customers' data is kept separated logically and physically. An organizations' data is isolated from other organization's data at multiple levels. Depending on the service in question, this includes:

- Databases
- File storage
- Web and mail access
- Private key

Scalability: In addition to protecting privacy, this architecture ensures a customer can never negatively impact any other customer's service or performance. Each customer's workload is isolated and prevented from impinging on another customers' service.

Privacy and confidentiality

Use of data

All data stored in Barracuda Networks facilities is considered confidential and private. Data is secured using standard and proprietary encryption methods. Information is not used for any marketing purposes. Occasionally, notifications and other communications pertaining to account maintenance might be sent.

During the normal course of operation, Barracuda Networks uses cookies, IP address and other technical connection details to improve and further develop the services that are delivered.

Access by Barracuda Networks' personnel

Occasionally upon a customer's request, Barracuda Networks personnel assist in setup processes, data restoration processes, or review information in the web-based interface. These actions may expose information and the contents of an organizations' data to Barracuda Networks personnel. Even under these circumstances, Barracuda Networks protects data from unauthorized use and disclosure.

Conclusion

A combination of architecture and best practices ensures that performance, availability and security of all provided services meets or exceeds industry-accepted levels. To continue providing best-in-class service, the technical aspects of all services are subject to change without notice. However, the underlying security and privacy of data is unchanged.

About Barracuda Networks Inc.

Barracuda Networks combines premises-based gateways and software, virtual appliances, cloud services, and sophisticated remote support to deliver comprehensive content and network security, data protection and application delivery solutions. The company's expansive product portfolio includes offerings for protection against email and Web threats as well as products that improve application delivery and network access, message archiving, backup and data protection. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 150,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International Headquarters in Campbell, Calif. For more information, please contact CPA Technology at (610) 862-1998, a Certified Barracuda Partner and preferred dealer*.

The Barracuda Networks Difference

Since its founding, Barracuda Networks has continued to gain wide acclaim from customers, media and analysts by offering exceptional customer service, top-notch products and engaging partner programs. Companies and organizations of all sizes rely on Barracuda Networks solutions for five key reasons:

- **Live in 15 minutes:** With no software to install or network modifications required,
  all Barracuda Networks products are easy to deploy and use.

- **No IT expertise required:** All Barracuda Networks products feature an intuitive web UI that ensures smooth
  product management and does not require your IT staff to be "experts" in a particular solution.

- **No support phone trees:** Specially trained Barracuda Networks support technicians are
  available 24x7 to answer customer calls and provide superior support.

- **Automatic product updates:** Barracuda Central is the 24x7 operations center operated by Barracuda Networks
  to monitor and block the latest Internet threats. Data collected at Barracuda Central is analyzed and used
  to create definitions for automatic Energize Updates that fuel the Barracuda Networks products.

Powerful Products & Services

Barracuda Networks' portfolio includes: Barracuda Spam & Virus Firewall, Barracuda Web Filter, Barracuda Web Application Firewall, Barracuda NG Firewall, Barracuda SSL VPN, Barracuda Email Security Service, Barracuda Web Security Flex, Barracuda Load Balancer, Barracuda Link Balancer, Barracuda Message Archiver, Barracuda Backup Service, and the BarracudaWare software portfolio. Barracuda Networks also has a growing portfolio of virtual solutions.

* During ordering, be sure to mention CPA Technology as your preferred Barracuda dealer to receive the maximum savings.