



Vol. 2, No. 2, March 2010

Flagship Solutions Group eNewsletter

Gartner: Seven cloud-computing security risks

Cloud computing is fraught with security risks, according to analyst firm Gartner. It has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing," Gartner says.

Here are seven of the security issues Gartner says customers should raise with vendors before selecting a cloud vendor.

1. **Privileged user access.** Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data.
2. **Regulatory compliance.** Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider.
3. **Data location.** Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.
4. **Data segregation.** Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but is not a cure-all. "Find out what is done to segregate data at rest," Gartner advises.
5. **Recovery.** Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."
6. **Investigative support.** Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns.
7. **Long-term viability.** Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your information will remain available even after such an event.

To learn more about how Flagship can help you safely migrate to the cloud, contact Flagship Solutions Group at **(561) 208-FYI1 (3941)** or visit www.flagshipsg.com.

Upcoming Events:

Webinar: Sealing the Security Hole

Is your network really safe?

Current security breaches and catastrophes say no!



Join us for a webinar on March 25th to learn how you can address these new threats and make sure your IT network is free from malware. Be sure to [register today](#).



April 22nd starts the NFL Draft. Reserve the Date!

Flagship has something special in store for you so reserve the date. Details to come soon!

Flagship and the Miami Dolphins

Off the field, one of the greatest IT challenges for the Dolphins is tackling the increasing volume of critical information – data, image, and video files – which reside in two data centers located at the Stadium and at the Miami Dolphins Training Facility in Davie.



To achieve this, the Dolphins recruited Flagship Solutions Group and IBM to conduct an assessment of its existing IT infrastructure and to recommend a smarter, more sustainable solution that meets the Dolphins' future growth and related capacity requirements.

Mark Wyllie, CEO of Flagship, stated "The Miami Dolphins, like many midsize businesses today must meet the dual demands of upgrading capabilities and controlling costs. Through proven IBM methodologies, we were able to assist the Dolphins in achieving a win-win by providing redundancy and increasing the computing power of their data center and IT infrastructure, while at the same time reducing the physical footprint required and related energy costs."

The solution, which was installed at both the Stadium and the Training Facility in mid-December, has enabled the Dolphins to consolidate from various makes and models of servers to two of the newest IBM Blade S servers. It also provides redundant capabilities to prevent unplanned power outages and data loss, and high-availability services and business continuity as well as energy and cost efficiencies. Tery Howard, Senior Vice President–Chief Technology Officer of the Miami Dolphins, said, "People may think the role of IT in the NFL is just about blocking and tackling – building computer networks and storing information. But for us, IT is a real competitive differentiator, enabling us to do things smarter for the benefit of our players, staff, and most importantly, our fans."

Contact Flagship Solutions Group at **(561) 208-FY11 (3941)** or go to www.flagshipsg.com to see how we can help you fulfill your IT needs.

Optenet: New Entrant on Secure Web Gateway Magic Quadrant



Gartner positions Optenet in the secure Web Gateway Magic Quadrant. With over a decade of security expertise, Optenet leads the industry with the most advanced technology for dynamic content protection, based on Optenet's Multi-content Inspection and Dynamic Analysis System (Optenet MIDAS™) and Optenet's Global Intelligence Acquisition Network for Threats (Optenet GIANT™) providing the highest rate of accuracy with unparalleled protection against Web 2.0 threats.

Optenet's Cost-Effective Security Solutions for the Enterprise provide:

Lowest Total Cost of Ownership (TCO) in the market today - Optenet's solution is based on a 100% subscription model that dramatically lowers TCO with no different platforms to manage, no third party licenses or hidden costs.

Integrated All-in-One Security Suite - delivering integrated security services with web security, email security, malware protection, anti-spam, anti-phishing engine, IDS/IPS, firewall, and traffic acceleration.

Flexibility in Delivery of Services - enterprises have the flexibility to choose the delivery of these services in-the-cloud or "on-premise" in the gateway, enabling companies to deploy a hybrid model adapted to their needs.

Powerful Reporting Engine and Capabilities - data is collected continuously and reports can be viewed in real-time, providing critical information.

Optenet Security Solutions:

- Enterprise Solutions
- SaaS Solutions
- Hybrid Solutions
- Multi-Location Solutions
- Protection of Minors

Contact Flagship Solutions Group at **(561) 208-FYI1 (3941)** or visit www.flagshipsg.com for more information on Optenet's Secure Web Gateway.

Kneber Botnet Attacks PCs Worldwide

Security firm Netwitness has discovered a new botnet. Called the Kneber Botnet, this new form of malware has infected more than 74000 computer systems across the world and is focused on stealing login credentials for email systems, social networks and banking sites.

Kneber is incredibly hard to detect and has reportedly compromised data from nearly 2500 corporate and government and corporate networks around the world. Netwitness says Kneber controlled machines are in 196 countries. The five countries with the most significant instances of infected machines are Egypt, Mexico, Saudi Arabia, Turkey, and the United States.

Kneber only targets Windows systems, and computers running Windows XP Professional SP2 make up the majority of the botnet. Kneber is primarily found on machines in corporate and government infrastructures, but home users can be affected as well.

The Wall Street Journal is reporting that affected companies include Merck & Co., Cardinal Health, Paramount Pictures and software company Juniper Networks Inc.

There is a way you can protect your company against Botnets such as Kneber. **Safe Media's Clouseau is the safe way to keep your organization's IT infrastructure healthy and fit and protect you against data breaches.**



For more information about this revolutionary technology that stops all forms of malware in its tracks, contact Flagship Solutions Group at **(561) 208-FYI1 (3941)** or visit www.flagshipsq.com.



Flagship Solutions Group
3701 FAU Blvd, Suite 210 • Boca Raton FL 33431 • 561.208.FYI1 (3941)
www.flagshipsq.com
sales@flagshipsq.com

Our Partners:

