WHITE PAPER: THE ULTIMATE STRATEGY FOR SECURITY IN CLOUD COMPUTING.

Author: Samwriterr

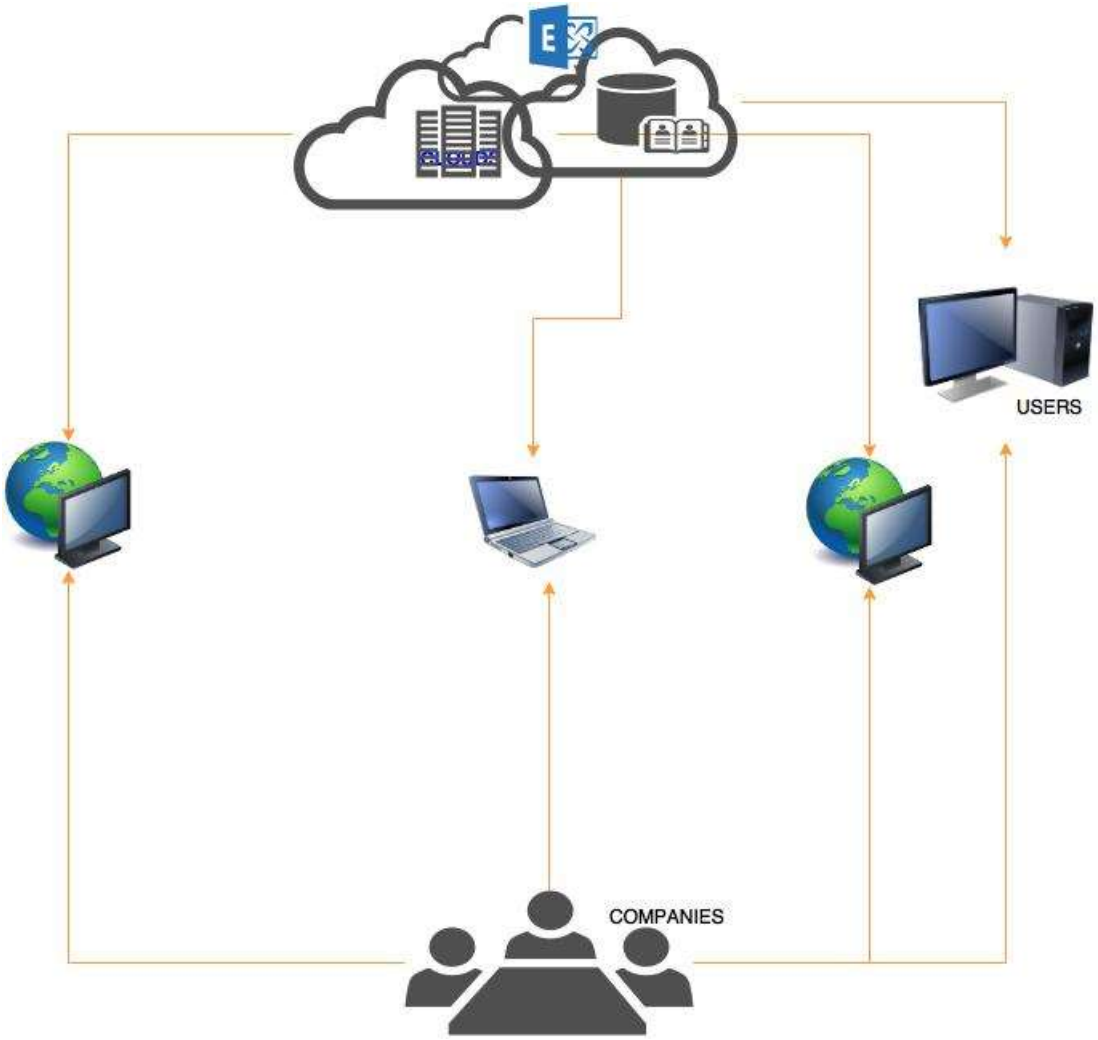
EXECUTIVE SUMMARY

Deficiency of proper data security and privacy is a turn off for many companies. The current cloud computing solutions exposes private companies' data to many security vulnerabilities. Service providers are working day in day out to solve this problem with most of them assigning a number of network security methods. Among them include employing neural networks, implementing DDoS attack protection as well as big data analytics. While this solutions seem to work, they do not solve the giant problem of data security. Data is the basic denominator in cloud computing. Protecting loss of data should be at the frontline of any cloud service provider. Service providers concentrate on protecting the network and omit the ultimate purpose of cloud computing security; securing and storing data. Cloud networks are subject to high attacks some which cannot be detected on time.

In order to deal with cloud computing securities issues, this white paper proposes that the data centric patterns of security protection is worth the effort. Instead of protecting only the networks, it important to put in mind that internal attacks come from within and hence, are not limited by the network wall. Further down, the white paper proposes a specific solution offered by Proof Point. In fact, internal attacks and data losses take place even during maximum security. Companies can employ services such as proof point which concentrate on securing and privatizing data from when it's new, during transfers and during storage.

AN EVOLVING CLOUD COMPUTING TECHNOLOGY.

Cloud in its most basic definitions means the internet[5]. Cloud computing is the process of storing and accessing company resources or information through the internet from a third party server. It has evolved through different phases. In 1969, Lickliter introduced the idea of interconnected network. His vision was that one day people would access data wherever they are and whenever they want without having to travel. Then in 1970, IBM introduced their concept of time sharing. The popularization of cloud computing came into existence in the 2006 dot-com bubble burst when Amazon.com invented its Elastic Compute cloud (EC2). Through this program, Amazon.com allowed people to use their servers for proportional fee to the time used the servers. For example, when user A rented the elastic compute program for four hours he or she would pay a different price to user B who used the server for ten hours. The server acted were simplified virtual machines. From Saas, Paas and Iaas, cloud computing has become the most famous method of software and hardware data management[2].



'DACING WITH THE CLOUDS': A changing environment.

In the traditional business environment, operational costs were very high. Businesses had to use a lot of time and money to create their own servers and computer networks. Maintaining this servers was not easy task. Big companies had to hire many personnel and buy millions of apps in order to fulfill their data management goals.

With the invention of cloud computing, the business environment has changed and the problem is quickly eroding. Many companies can now dance with joy since the threat on performance and cost is reduced. Using cloud computing, companies are able to pay for only the space they need. Businesses can now manage their entire network from accounting to human resource through the cloud. Cloud computing helped businesses to cut on cost and spaces while improving performance and productivity.

While cloud computing may have been a solution to many business, it create a bigger problem; risks of data loss. Cloud security became and is still a big problem. The outsourcing of data protection to third parties puts organizations at high risk. Many a time, to save space and resources, cloud service providers centralize the location of stored data and information from different organizations. Subsequently, this affect the privacy of sensitive company information as it can other users and even the competitors[4]. At the same time, software is man-made thus susceptible to errors. In this structure the risk of data loss or infection is substantial. Although many service providers are working hard to convince users on how well their software is managed and secured, this still remains to be a huge problem facing the cloud computing network in its entirety. Besides, cloud storages are met by huge risk issues such as data breaches , malware, shared risks, data loss just to touch on a few.

HOW MUCH LOSS IS LOSS; Factualizing the cost of data loss

Data loss for any company is bad for business. It could mean moving from being a market leader to huge losses or the closure of company. According to recent survey conducted by IBM, 50% of businesses that lose data culminate within the first 10 months[2]. Even more, a report from the Strategic Research Institute revealed that businesses that do not survive data loss within the first 5 months of an attack, never survive at all. When a data loss occur, companies are more likely to spend billions of money and a lot of time in recovering. Moreover, according to the market statistics as analyzed by Helmed Security showed that internal threats to cloud storages come from disappointed employees especially those who have been fired. This statistic alone is enough to show the magnitude of cost out of data loss to a company

Security in the cloud could result from both external and internal attacks. It is with no exception that cloud security issues have confronted even big companies such as Amazon, Google Gmail as well as the Boeing[5].

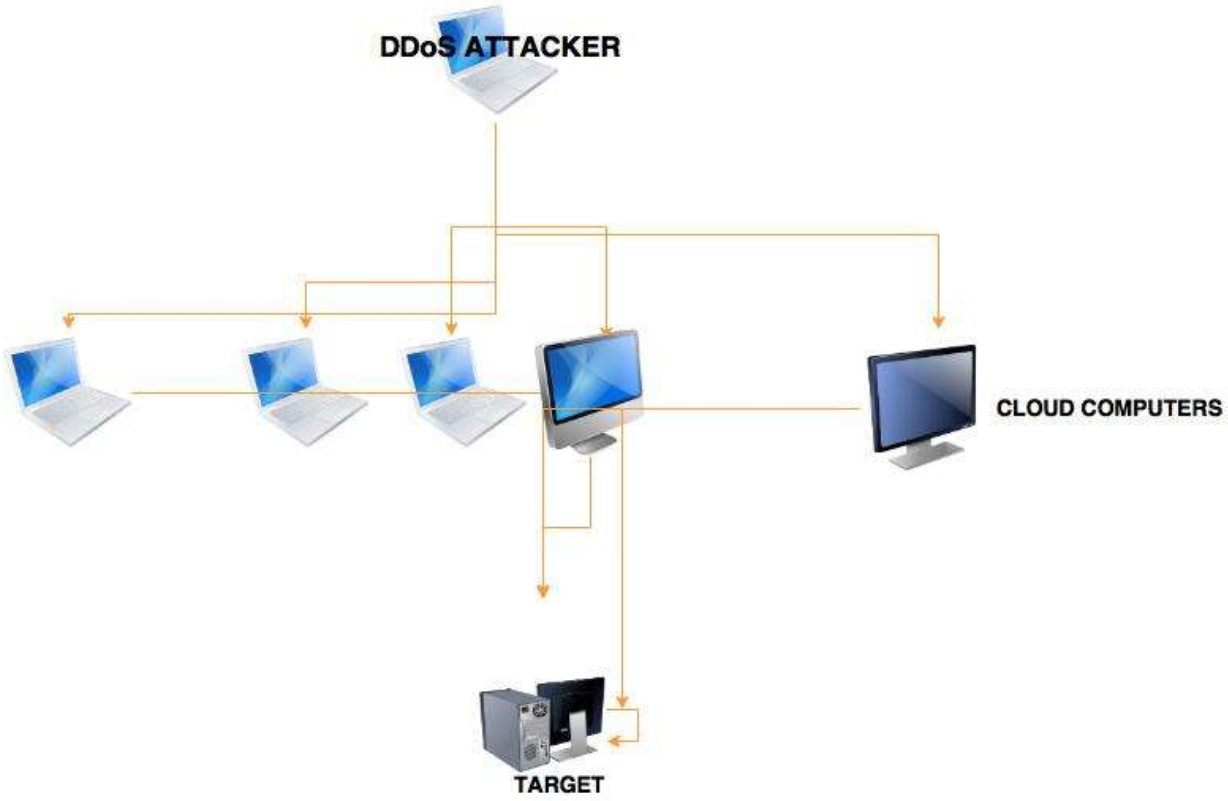
THE AILING SOLUTIONS; Is it working or not?

The current and most popular solutions for cloud computing security focus on the network. The protection of cloud network include the Denial of Service (DDoS) protection, the big data analytics as well as neural networks. The DDoS shields the relay networks as well as the target user. In their method, sophisticated cloud security providers engage locally built inline hardware along with carefully crafted elastic cloud networks[1].

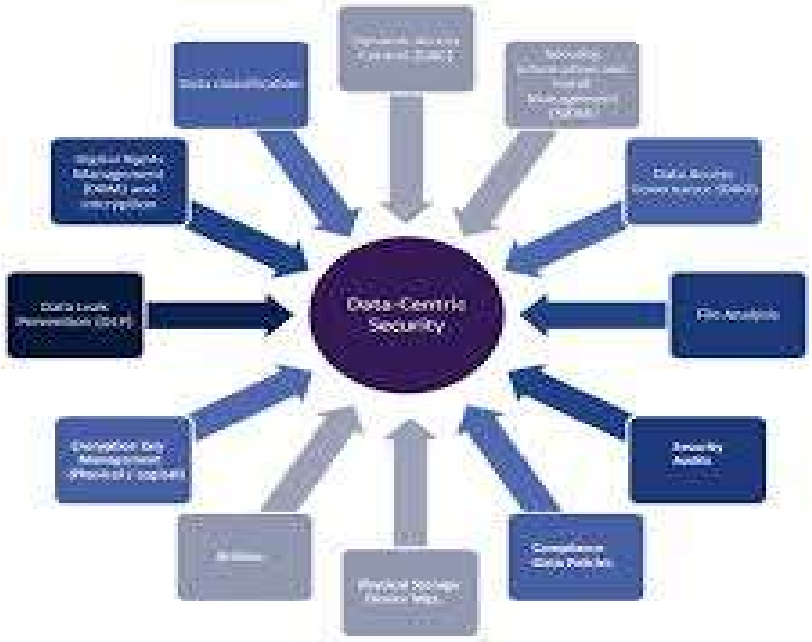
The big data analytics on the other hand aims at analyzing high volumes of company information and regrouping them in order to increase network speed which is usually a big threat for security. Through big data analytics, companies can analyze years of data across different categories and identify a potential threat or the source of security breach. The neural network helps to analyze complex patterns using software and hardware similar to the human brain. The neural is composed of a series of tiers which are dependent on each other to operate respond successfully. The neural networks are trained to work in a specific way according to the human inventor. This method is employed in cloud to manage different end points simultaneously. Using neural networks helps to create a response which can be traced to a security threat. This solution in itself is not giving so much confidence to the cloud users. It is quite ineffective.


support
cloud
storage
database
analize
information
tools
statistics
Big Data
mobile
processing
terabytes
NoSQL
compression


DDoS ATTACK


DDoS ATTACKER
CLOUD COMPUTERS
TARGET

The SUPERIOR SOLUTION



With the security threats involved, businesses cannot expect that the network security alone will protecting their data. Data is the main reason an organization continues to operate. It is the heart of an organization. Unlike in the past, companies now operate in a complex interconnected environments. The use of a data centric approach to data security is important. It deals with almost all security threats encountered by network only security approach. The data centric approach demands the implementation of detailed programs which help in protecting sensitive company information such as consumer data and tax returns. In this method, the company or organization review and analyze the process of information cycle and create the best ways to deal with sensitive data at each stage of the information cycle. The data centric approach aims at understanding how and where each data is stored. It then groups data based on sensitivity. The data centric approach recommends frequent audit on data protection and privacy programs[3]. The data centric approach uses different ways of protecting data such as encryptions, internal audits and data regrouping[4].

A good example is the proof point data protection model employs the concept of analyzing each stage of the information life cycle. Proof point utilizes a model that analyzes data deeply through fingerprinting. In their data centric approach, they analyze even the unstructured

data format. Along with this is the data discover method which helps companies to monitor and identify sensitive data. While the entire cycle of data centric protection develops, it does not affect the workflow of users at the end point. Effective use of data centric security on data is dependent on company's policy management[3].

The following are benchmarking tips for an outstanding data centric framework:

- ✓ It prevents the recovery of deleted files.
- ✓ It encrypts sensitive data using strong passwords.
- ✓ It does not affect the end user work flow.
- ✓ It allows the access of information to the audit team to deal with internal risk.

An effective concept to employ when a company employs cloud computing is to concentrate more on data protections compared to network protection. When companies concentrate on protecting the fence; the network, they lose focus on the most important factor; data privacy and safety. They even forget that even the most secure networks are vulnerable. Sometimes attackers attack networks just to destroy data. Massive loss of company data can ruin a company in its entirety. In summer of 2009, Microsoft Inc. lost massive data for Side Kick's T-Mobile users. More than 800,000 users were affected when Microsoft servers failed. According to Microsoft, this was a confluence error on server failure. Out of this loss, public confidence on Microsoft decreased. They even lost major cloud computing deals with Azure.

Aspen insurance Holding Limited addressed the issue of data privacy and protection when it implemented Proof Point protection. When a company protects its sensitive data regardless of the security of the cloud infrastructure, it enhances its future. It protects its brand and increases consumer confidence. Once that data has been protected, the company should enforce and implement regular audit on sensitive data in order to identify security threats.

An important consideration to note is that a data centric approach is more effective than the traditional network only security for cloud computing. The data centric approach helps to avert even the smallest attacks which could result from internal attacks[4].

CONCLUSION

When security threatens an organization's data, financial and business loss in terms of customer confidence, company competitiveness and operations are considerable. IBM's 2016 cost of data breach study showed that by 2016, companies' cost of lost data increase to $4 trillion down from 1.7 trilling in 2015. A successful data centric method, however, can reduce this number and improve cloud computing security. As a critical first point toward implementing the data centric security approach, companies must implement policies that concentrate on data protection. Proof Point summarized the importance of good cloud security by stating that "cyber-attacks target people, look beyond people."

End notes

1.Raya, Maxim, Panagiotis Papadimitratos, Virgil D. Gligor, and J-P. Hubaux. "On data-centric trust establishment in ephemeral ad hoc networks." In*INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

http://ieeexplore.ieee.org/document/4509775/?ctx=footnotes

2.Shaikh, Farhan Bashir, and Sajjad Haider. "Security threats in cloud computing." In *Internet technology and secured transactions (ICITST), 2011 international conference for*, pp. 214-219. IEEE, 2011.

3.Ball, Robert, Glenn A. Fink, and Chris North. "Home-centric visualization of network traffic for security administration." In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pp. 55-64. ACM, 2004.

4.Shi, Elaine, and Adrian Perrig. "Designing secure sensor networks." *IEEE Wireless Communications* 11, no. 6 (2004): 38-43.

5.Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee et al. "Above the clouds: A berkeley view of cloud computing." (2009).

About Proof Point

Proof Point provides a compelling data centric security for business with a proven track record of more than 95% happy customers.

Proof Point products are innovative, cloud based utilizing far reaching intelligence and visibility couple with a proven suite of solutions.

For more information about proof point visit

www.proofpoint.com