September 30th 2017

Whitepaper

Security in the Cloud

V3iT

SAP Certified
in Application Management Services

SAP Partner

Contents

Table of Contents

Why Now – What is the need?

On September 7th of 2017, the world saw one of the biggest security breaches that affected nearly half of the population of the United States. Even for companies that have mature cybersecurity processes in place, sometimes missteps or control failures can occur. Cyber-attacks are inevitable. layered, defense-in-depth strategy, such as the one we espouse at our V3iT cloud, includes multiple, layered security controls so that there is rarely a reliance on a single control to provide sole and complete protection, as well as periodic inspections of a company's security posture to validate that controls are functioning as intended. There have been fundamental shifts in Cyber-Security threats and trends, TTP's (tactics, techniques and procedures) used for cyber-attacks. From the board of directors down through every end user in an organization, the threat of a cyberattack is finally becoming a top-of-mind operational concern. The impact of a breach incident spares no office, or officer. No corporate reputation is safe from the distrust a company is tarnished with when it's compelled by regulatory requirement to publish breach-related information. The average cost per cyber incident continues to rise, and even with greater awareness, the frequency of incidents is also rising. So how should companies be thinking about cybersecurity investment and preparedness outside of their walls? What cybersecurity assurances should they request from their vendors and their supply chain partners? How can they be sure that electronic security system integration goes beyond the simple installation and maintenance of equipment, and becomes part of an organization's overall cybersecurity life cycle management?

Cost of Data Breach and differentiating on-premise vs cloud systems

In a recent 12th annual Cost of Data Breach Study that was sponsored by IBM, the industry's gold-standard benchmark research, independently conducted by Ponemon Institute. This year's study reports the global average cost of a data breach is down 10 percent over previous years to $3.62 million. The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased from $158 in 2016 to $141 in this year's study.

However, despite the decline in the overall cost, companies in this year's study are having larger breaches. The average size of the data breaches in this research increased 1.8 percent to more than 24,000 records.

Contrary to several myths, cloud is more secure than traditional IT systems and here is why. According to Alert Logic's State of Cloud security report, the variation in threat activity are not as important as where the infrastructure is located. The report further finds that Web application-based attacks hit both service provider environments (53% of organizations) and on-premises environments (44%). However, on-premises environment users or customers actually suffer more incidents than those of service provider environments. On-premises environment users experience an average of 61.4 attacks, while service provider environment customers averaged only 27.8. On-premises environment users also suffered significantly more brute force attacks compared to their counterparts.

In most offices, a locked door is the main defense to protect IT equipment, important files, and personal- and business-related data. In contrast, the top cloud service providers' (CSP) data centers have multi-layered security defenses. Precautions include high fences, barbed wire, concrete barriers, guards that patrol the area, and security cameras. These physical barriers not only prevent people from entering the data center. They also monitor activity near the space.

When data is stored off-site in the Cloud, employees, vendors and visitors are physically separated from a company's mission-critical data. This lack of physical access makes it more difficult for third parties to stumble across data and use it negatively. The amount of human risk decreases.

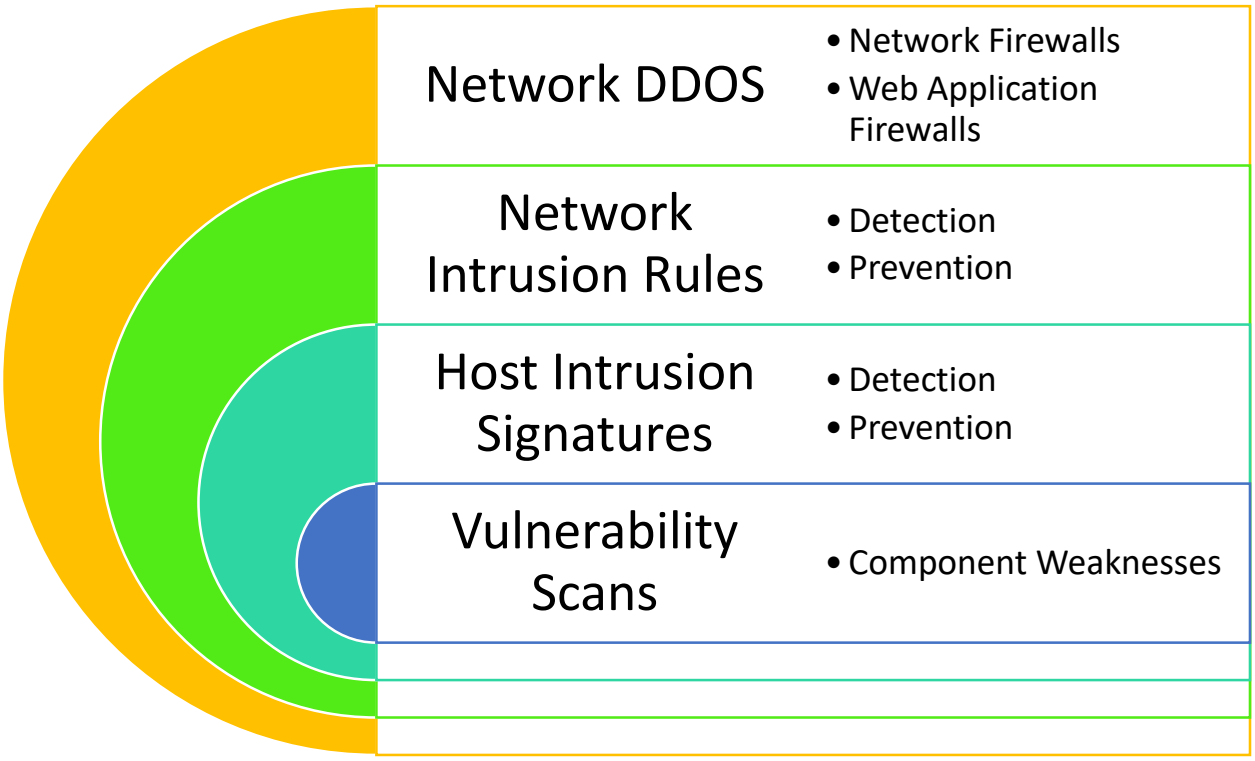
CSPs specialize in keeping data safe. Cloud infrastructure is monitored at all times in order to head off potential security threats.

Moreover, CSPs undergo yearly audits to protect against flaws in their security systems. However, on-premise systems more often than not do not have this requirement.

As more businesses begin using the Cloud, it is inevitable that they will see tangible benefits, such as improved business efficiency, better access to data and security.

Building Blocks of a secure cloud model

As we peel into layers of most cloud infrastructures, it becomes apparent as to what goes on beneath the surface, to ensure the systems and data are at the bottom-most layer and the harder to penetrate through each of these layers.



Building off the foundation certification and compliance most cloud platforms deliver a secure platform at every level of the architecture. Some points to note here include:

- PCI , HIPAA, ISO27002, NIST800-53 and other certifications including data center certifications of SSAE16 Type 2, SOC1, SOC2
- Activity logging – monitoring and detection
- Biometric and key-card access control
- No customer access to shared infrastructure
- 24X7 Security Service and CCTV monitoring
- Best practices such as ITIL v3
- Redundant layered firewalls
- Encrypted VPNs
- Continuous upgrades and ensuring compliance with standards as they become available

The V3iT difference

For SMB and enterprise customers, who are concerned about loss of productivity, revenue (or fines) or loss of reputation caused by security breaches or failure to compliance of all sorts, V3iT provides a defense in security through their cloud services and the multiple layers of security, that provides a peace of mind to our customers.

Some of our key differentiators include:

- Tailor-made regulatory compliance requirements followed for each customer, which are important to SMBs who may be vendors to big organizations or subsidiaries of large corporations
- 24X7X365(366) and as necessary ITAR compliance through US persons support (including all the hardware, OS and hypervisor support structure that we get from our support vendors)
- Defense against sophisticated multi-layered attacks
- Tailor-made custom reporting based on individual customer requirements

1717 N. Naper Blvd. Suite # 103, Naperville, IL 60563 | Phone: 630.245.1400 | Fax: 630.245.1401

info@v3it.com | www.v3it.com