Establish effective cloud security platform with 5 basic steps

According to CSO statistics, more than 80% of organizations and businesses have been using services from 2 or more public cloud infrastructure providers, and nearly two-thirds of them That service is using from 3 or more providers.

According to CSO statistics, more than 80% of organizations and businesses have been using services from 2 or more public cloud infrastructure providers, and nearly two-thirds of them That service is using from 3 or more providers. In fact, the problems encountered in moving enterprise-class IT platforms and models to the cloud model also bring serious concerns to data security and security. Full information. Time is one of the most important factors in this process. However, with the need to accelerate the transition to the cloud platform, organizations and businesses will have to face the challenge of potential security threats arising from any Any weakness in the cloud environment.

Young people are too confident when talking about online security!

Cloud safety is a term referring to a set of policies, processes and technologies that must be tightly coupled to protect the safety of cloud-based systems. in general. After all, the goal of cloud security is to protect data, privacy and at the same time set effective security authentication rules for both users and devices.

Software related to cloud security can be configured according to the exact needs of each specific business or organization. Therefore, they can be managed in a way that is maximized for each IT activity. In addition, these software can also be built to allow more attention to other important tasks.

Mix and combine in multicloud - the future of cloud computing

According to CIO research, up to now, nearly 96% of organizations and businesses are using cloud-related services. In addition, according to the Forbes report, the damage caused by data breaches worldwide each year is estimated at $ 3.86 million. These figures imply that in the context of the use of cloud services almost become mandatory today, the cloud security platform in general will also have to achieve adequate growth rates.

If an organization does not prioritize investment in security and at the same time fails to realize the value of system integrity monitoring software, they will have to pay a very high price, even bankruptcy. However, IT managers should also proactively know that they must provide the cloud environment with the necessary and appropriate protection.

Here are 5 basic steps to set up an effective cloud security platform compiled by experts from CSO, please consult.

1. Authentication tool on many enterprise VPN applications that are bypassed by hackers

5 basic steps for an effective cloud security platform

1. Develop security strategies
2. Highly alert with APT attacks
3. Detecting and minimizing risks
4. Detecting vulnerabilities on cloud platforms
5. Practicing information security 'hygiene'

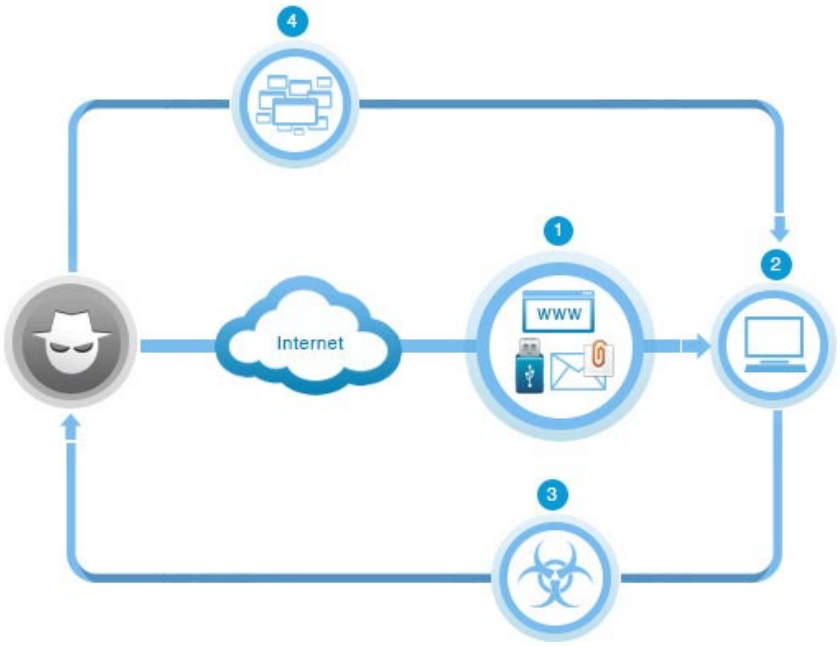
Develop security strategies

Cloud service and application security posture management providers will often be responsible for bringing their customers (businesses) a strong frontline security shield. However, organizations should also create additional security and compliance measures. Another advantage is that such security tools can significantly shorten the time between important security checks every year or quarter, monthly, weekly or even daily to identify and Quickly handle any vulnerabilities before they can be exploited to damage the system.

1. [Infographic] 7 effective ways to protect businesses from Ransomware

Incident reporting tool is also an essential element, which is responsible for detecting basic system weaknesses. Security scans can be scheduled automatically or manually to find any security holes on the system. Of course, choosing how to monitor the integrity is reasonable will depend on the manager's decision and the actual situation.

Highly alert with APT attacks



1. Insider attacks are becoming more and more popular and difficult to detect

The basic security barriers that are widely deployed today such as antivirus software or firewalls may not provide enough power to cope with sophisticated, advanced attack methods targeting the cloud service. Therefore, the appearance of additional security barriers will play an extremely important role. Advanced persistent threats (APT) - a set of secret and continuous computer system attacks, usually arranged by a person

or group of people targeting a particular entity - as one of the threats leading for cloud-based systems because identifying them in the cloud environment is extremely difficult. Of course there are still characteristics that can help identify an APT attack, so organizations should invest more in building an effective defense system for these attacks.

Detecting and minimizing risks

$ 100,000 is the average number of losses per hour that a typical enterprise IT system is forced to deactivate or paralyze against attacks. Therefore, the process of detecting and reducing risks is also an important step that businesses should not take lightly. One of the best ways to keep it safe and minimize your cloud risk is to plan the worst cases that can happen. For example, how quickly can the data warehouse be restored, how complete is it, how much is lost? Then consider how to find a way to prevent a security disaster from happening in the first place.

1. The alarming increase in the number of attacks targeted at IoT devices

A meticulous and reasonable cloud disaster recovery plan can serve as the most effective solution, especially when the system data warehouse is properly concerned. In addition, to create real protection measures for endpoint equipment and data assets, the ability to troubleshoot when detected will be one of the prerequisites.

Detecting vulnerabilities on cloud platforms

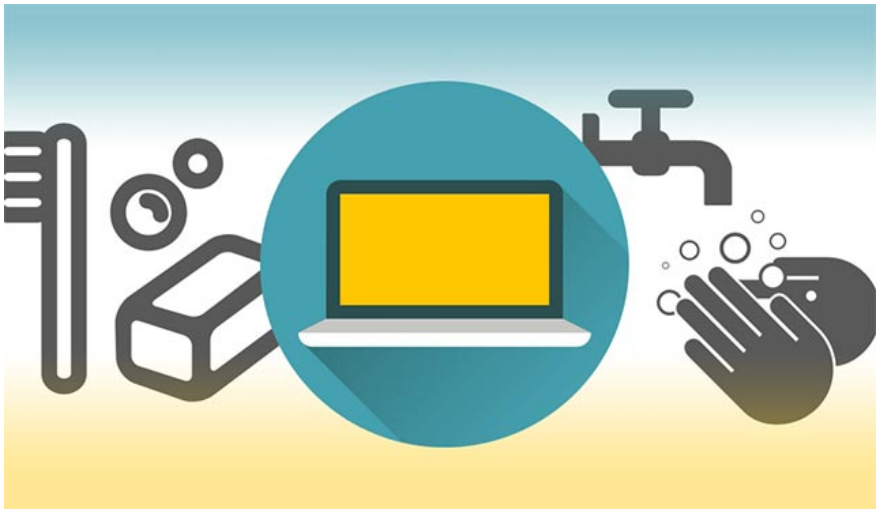
After all, the data whether stored on the cloud or in the local system will still need to be protected by security solutions, and security solutions will also need to be managed and Clear configuration. However, do not ignore the early detection of security holes on cloud platforms.

McAfee expert explained how deepfake and AI are drilling through the cyber security wall

The cloud-based vulnerability may sound 'sublime' but in fact they can be merely problems arising in data backup, application security, over-access, user monitoring. , or password concerns. Because additional devices and applications are often included in a business organization, additional tools are needed to help assess vulnerabilities as well as existing security threats in the cloud.

Skilled IT teams should be tasked with detecting and identifying any indicators related to segmentation or violation of security colors.

Practicing information security 'hygiene'



DDoS is ranked as the top threat for businesses in 2018

Finally, check and 'clean' your account, as well as cut off all cloud access to objects you think are 'unqualified'. Let's start with checking our cloud and user privileges. There should not be any instances where user accounts are exempt from checking. Users should be provided with more permissions needed to perform their work. Besides, cutting down access can also help you avoid unnecessary vulnerabilities and risks.

The above are 5 basic steps to build an effective cloud security platform. Hope the information in the post useful to you!