radware

Don't Let Security Concerns Impact Your Business
7 Things to Look for in a Cloud Security Service

Protecting web assets poses a daunting challenge. As the threat landscape rapidly evolves, attacks are growing in complexity and persistency, while zero-day attacks swiftly exploit newly-discovered vulnerabilities. Vicious, volumetric network-level DDoS attacks at staggering throughput rates easily take down organizations' network and applications and highly exploitive SSL-based and application-level DDoS attacks are more prevalent.

The accelerated change of both web-assets and attack vectors renders static web security solutions obsolete. Security teams need a solution that meets the distinctive needs of their networks and applications while automatically adapting to changing environments and new threats and minimizing human intervention. Here's a list **of 7 things to look for in a cloud security service** to safeguard your web assets.

1. Meets the Unique Needs of Your Network and Applications

Selecting the right service requires self-assessment. Are applications in your data center, hosted in the cloud, or both? Can your organization manage on-premises appliances? Is in-house expertise available to handle DDoS threats? Is the organization sensitive to the time it takes to mitigate massive volumetric attacks? Look for a service that combines attack protections and **provides multiple options**, whether it's **always-on, on-demand, or hybrid** and offered in a tiered service-based model.

2. Time is of The Essence

Zero-day attacks are fantastic at exploiting newly-discovered vulnerabilities, which is why precious time can't be wasted when it comes to generating new safeguards. Rather than relying solely on human intervention – which can take hours – **automated behavioral-based detection** and **real-time signature creation** generates protection within seconds.

3. Change is Constant

New applications and modifications to existing ones require new security policies and procedures. A cloud security service should automatically detect and protect new applications as they are added to the network by automatically creating new policies. Look for an **adaptive service** that automatically continuously adapts to evolving threats and protected assets.

4. Massive Scrubbing Capacity and Global Network

DDoS attacks are increasing in quantity and severity, complexity and persistence. If faced with particularly large or simultaneous attacks, you'll be grateful if your provider can scrub bad traffic in large volume while allowing legitimate requests through. Choose a service that has worldwide coverage and **enough total scrubbing capacity** to handle several attacks simultaneously, and constantly expands and upgrades based on changes in DDoS attack trends.

5. Communication is Key

Cloud adoption complicates management and orchestration of security policies. Look for **messaging capability** that atomatically generates protections for zero-day attacks within seconds through **behavioral-based detection** coupled with **real-time signature creation**.

6. Can't Hide Behind an IP

Bot-generated attacks leverage surreptitious techniques to disguise malicious traffic. To protect applications from these rogue-like tactics, look for a technology that can automatically identify, blacklist and block machines that are used for attacks, **regardless of the source IP they hide behind**.

7. Smart SSL Attack Mitigation

Not all SSL attack protections are created equal. Look for SSL-attack mitigation in the cloud that **maintains user data confidentiality** and removes operational dependencies between the service provider and the organization when keys are changed.

IN SUMMARY

Remember these key points and select a cloud security service that adapts to today's always evolving cyber threats. Learn about Radware's comprehensive, automated cloud protection service that continuously adapts to offer the fastest threat detection and mitigation.