RADWARE HOSTING AND CLOUD ATTACK MITIGATION SERVICES SOLUTION

Radware's DefensePro Technology enables cloud and hosting businesses to offer various levels of Attack mitigation services to their customers and better secure their cloud and hosting business.

Challenge
Cloud and hosting providers are challenged to differentiate their services, attract more customers and increase revenue. The cloud provider challenge originates from two sources including the increased risk to the cloud and hosting datacenter due to the exposure to the threats of multiple customers, and the overall demise in ARPU due to the hefty competition.

Solution
Radware offers cloud and hosting providers a transparent, scalable and easily manageable availability threat prevention solution designed to work in multi-tenant datacenters. The solution seamlessly integrates into the existing provider network and provides a highly available design that can easily be scaled and operated with minimal overhead, without any need to redesign the network. At the same time it significantly mitigates the risk that each of the tenants is exposed to and allows the operator to selectively offer different levels of attack mitigation security services to different tenants.

Benefits
- Increase amount of hosted customers by mitigating risk of off-site applications hosting
- Create revenue generating value added service offerings increasing revenue per user
- Flexibly define Attack Mitigation service policies – per tenant or per service bundle
- Highly-effective Attack Mitigation system reducing overall oeprator risk from DDoS, DoS and APT attacks.
- Enable providers to power their customers with volumetric attack prevention capabilities not achievable in their private data centers.

Traditional hosting and cloud infrastructures are required to offer their customers solutions to mitigate risks associated with the off-premise hosting of business applications due to the frequent attacks under which internet applications are threatened. Radware's solution enables providers to secure their shared infrastructure from various availability attacks as well as offer their customers a variety of attack mitigation services that protect against host targeted attacks and application targeted attacks. By implementing the Radware attack mitigation solution, providers can easily offer a secured hosting & cloud platform while introducing services that will increase ARPU.

The Challenge

Many factors are impacting the increased need for deploying applications globally and making them available 24/7. These include: employees BYOD, home based workforce, global business presence and more. IT organizations, in various industries, are looking to find the best ways to leverage their budgets and increase the reach of their company's applications. Managed hosting and cloud based virtual private hosting have become the preferred option for hosting applications, however, due to the high population of tenants in these data centers and the use of various shared infrastructure elements, the aggregate risk surmounts and becomes a concern.

Recently, as hacktivism and attack-for-profit activities are becoming more common, the risk originating from deliberate attacks have become more significant. Cyber-attacks carried out by these groups usually take form as one or more of following attacks:

Network DoS: Saturating the network link of the victim to a point where they can no longer connect to external resources or be accessible by external resources. Typically network DoS attacks are executed from multiple sources and are referred to as Distributed DoS or DDoS. The impact of a network DoS attack on a cloud or hosting provider is severe regardless of whether tenants/customers were targeted or the provider itself was targeted.

Host/Platform DoS: Overwhelming the computer resources of an infrastructure device in the provider network such as a firewall, router or virtual server host can significantly impact the availability of all or some of the provider infrastructure and impact multiple tenants. Such attacks will typically target operating system vulnerabilities and infrastructure architecture bottlenecks.

Application DoS: Overwhelming hosted applications, either by introducing race conditions or by simply requesting multiple computationally intensive operations is another form of popular application. Very similar to a platform DoS attack, an application DoS attack will target application specific architecture flaws and vulnerabilities. Typically, in a multi-tenant hosted data center, such attacks will be targeted at a specific tenant or at the provider applications and impact accordingly.

Application Targeted Attacks: These attacks, also known as Advanced Persistent Threats (APT), are attacks that typically take multiple forms and combine reconnaissance, vulnerability exploitation, and content-manipulation and diversion techniques. Typically, these attacks are targeted at very specific information that belongs to a particular organization; hence their impact is very narrow but often very severe on the target.

While the variety of threats that impose risk on cloud and hosting provider customers challenge the easy adoption of off-premise hosted solutions; the ability to mitigate these risks with advanced technology, that is not always economically viable for private datacenters, offers a great opportunity for cloud and hosting providers to better protect their customers and offer additional services that create more revenue.

The Radware DoS Protection and Attack Mitigation Service Solution

The solution enables providers to offer various levels of Attack Mitigation security services to their customers such that different tenants can subscribe to different services. The flexibility of the solution allows providers to offer a baseline shared infrastructure DoS protection security policy to all tenants – and in turn increase enterprise IT confidence migrating applications off premise and accelerate the adoption of hosted / cloud based services in general. Additionally, the solution allows providers to offer more advanced services that are priced as premium services with appropriate customer value. Some of the options for specific services can be:

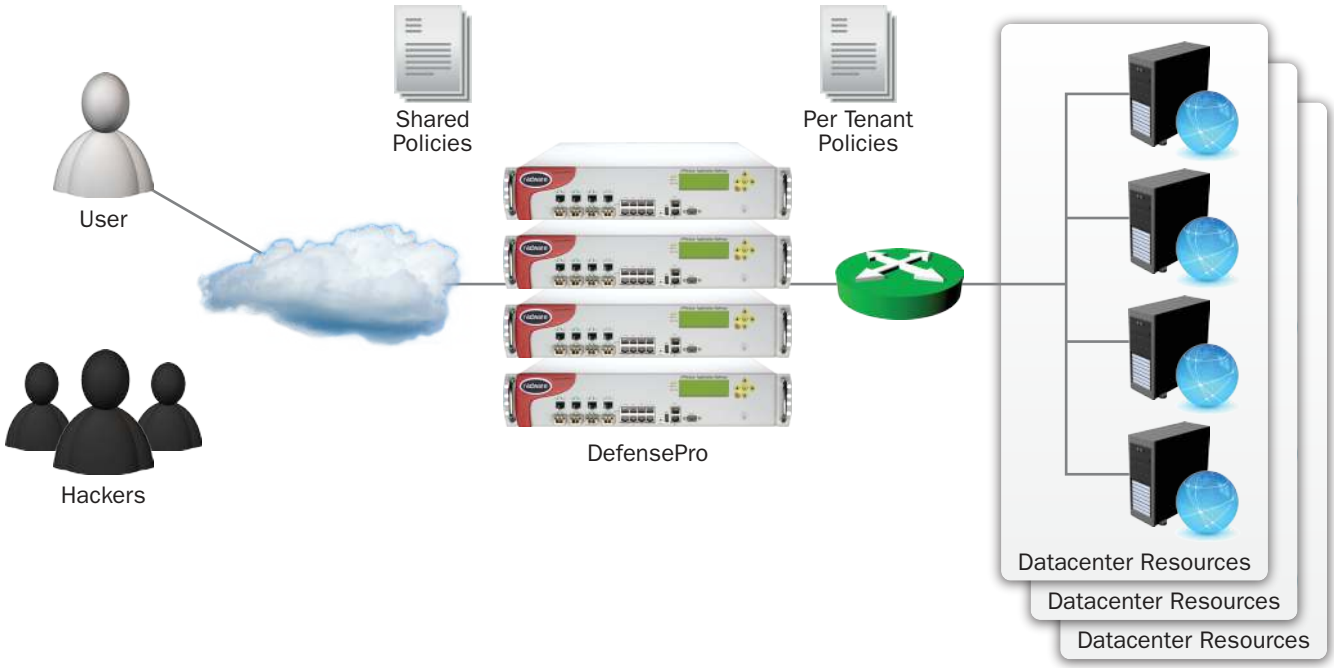
1. Application DoS protection services
2. Advanced threat protection services
3. Detailed periodic security reports

The Radware DoS protection and attack mitigation service solution, uniquely offers uninterrupted application performance during attacks by only removing the attack traffic from the traffic path and regularly forwarding unrelated traffic. This capability is critical in cloud and hosting environments as tenants who are not under attack or any tenant that subscribes to the attack mitigation service, expect to keep running their applications normally regardless.

The solution is comprised of the following Radware products:

1. Radware DefensePro Attack Mitigation System – Attack Mitigation appliances operating at up-to 40Gbps, powerful enough to block attacks on the fastest Internet links available, include various hardware accelerated functions to improve accuracy and scalability of attack mitigation.

2. Radware Vision – Managing events and incidents while monitoring the security posture of the provider infrastructure and enabling providers to proactively control security incidents as well as provide their tenants deep insights into their individual environments.



Attack Mitigation service models supported by the Radware solution:

Service Model	Description
Shared Network & Platform DoS Protection	Due to the overall risk imposed to Cloud and hosting provider shared resources, providers should offer a shared infrastructure protection service to all tenants. This service will protect from attacks on the provider shared resources such as firewall, routers, network links, and servers and improve tenant resource availability.
Tenant Application DoS and Vulnerability Protection	As an entry level value-add service, providers may offer their tenants a service protecting from known vulnerability exploitation and application denial of service attacks.
Tenant Advanced Attack Protection	As a premium service, providers may offer their tenants a service protecting from advanced, multi-vector, and long-duration attacks. Accompanied by periodic security incident and posture reports.

According to the above service models, Radware has developed a unique business model with more flexible pricing, billing and licensing options, offering better alignment with end user billing and for cloud and hosting providers.

Additionally, according to the specific service offerings of the cloud and hosting provider, Radware offers the opportunity to join the Cloud partner program which provides additional benefits.

Features and Benefits

The key benefits of the Radware DoS protection and attack mitigation service solution for cloud and hosting providers surround the ability to dramatically increase the security posture of their tenants and improve customer confidence by applying a baseline security protection policy. This ability is enabled by simple integration of the service into the provider network, easy addition, change or removal of customer services and ultimately a carrier grade availability scheme offering internal and external bypass options that eliminate the effect of device related failures on traffic forwarding and ultimately the provider business.

Some of the solution features are listed as follows:

- Granular, operator defined security policies
- Highly scalable Attack Mitigation protecting links of up-to 40Gbps
- A highly redundant system with no single point of failure
- Easily managed for the creation of basic security profiles
- Per tenant security reporting, monitoring and forensics capabilities.
- Customized auto-learning per customer/application
- Line rate Network Behavioral Analysis and anomaly detection
- Improved tenant SLA control
- PCI compliance reporting per tenant
- Extremely low false positive and false negative ratio
- Automatically generated security policy for quick start

Summary

Radware DoS protection and attack mitigation service solution offers hosting and cloud infrastructure providers the ability to confidently attract customers by increasing both the basic security level of their tenants as well as being able to offer more advanced security services to them, ultimately improving revenue per customer and customer loyalty. With the challenges of the hosting and cloud providers in mind, the Radware solution offers improved continuity of operations while serving as an ideal platform to enable additional services for tenants. The solution can be introduced into the provider network without interrupting existing traffic and can be selectively enabled on a per tenant basis.

Radware's solutions for cloud and hosting providers are priced in ways similar to these used by hosting providers with their tenants, effectively easing the financial burden of investing in such a solution and offering very attractive tools to increase overall profit as well as revenue.

Next Steps

For more information about Radware DefensePro please refer to the following web page:
http://www.radware.com/Products/ApplicationNetworkSecurity/DefensePro.aspx

To find a Radware partner in your area, please view the following list of resources:
http://www.radware.com/Partner/FindaPartner.aspx

Radware AMS Technology Overview:
http://www.radware.com/workarea/showcontent.aspx?ID=1629297

Radware Web Flood Protection:
http://www.radware.com/workarea/showcontent.aspx?ID=1629158

Radware DNS Protection Solution:
http://www.radware.com/workarea/showcontent.aspx?ID=1629029

Radware SSL Protection solution:
http://www.radware.com/workarea/showcontent.aspx?ID=1629030