FROST & SULLIVAN

AUGMENTING SECURITY WITH ALWAYS-ON

HYBRID DDOS PROTECTION

A Frost & Sullivan White Paper for

RADWARE

radware

The impact of a DDoS attack is massive. Web Services remain unavailable due to volumetric attacks and enterprises incur hefty losses that run into millions. Today, multi-vector attacks dominate the DDoS landscape and morph into far more dangerous and challenging threat scenarios. It is critical for enterprises to deploy a DDoS Mitigation solution that understands next generation threat actors and can inspect both inbound and outbound traffic 24x7.

EMERGENCE OF WEB 2.0 AND THE THREAT PERSPECTIVES

THE NARRATIVE

Web 2.0 refers to the second generation of World Wide Web applications that moved static HTML pages to a more interactive and dynamic web experience. It became a medium for enterprises to remain connected with customers irrespective of their place, time and situation. Enterprises have realized that customers want a platform that is more engaging, inclusive and offers better user experience. Traditional modes of business resort to ways that do not sync well with today's customer expectations and often affect business performance. Hence the rise of Web 2.0 focused on bringing in a culture of collaboration, content sharing, customer engagement, and integration.

The way enterprises have become dependent on Web 2.0 has changed drastically over the last few years. Companies have developed applications and relied on third party management systems that interact with customers, collect data, and process information to furnish tailored recommendations. While, the dependence on web is perceived as a step toward digitalization, this has opened new threat opportunities for enterprises to take preventive action.

EVOLUTION OF DDOS ATTACKS AND THE NEED FOR MITIGATION SOLUTIONS

The Distributed Denial of Service or DDoS attack is one of the most powerful perils on the internet. "Bringing down of a website" by hackers often makes news; this refers to a DDoS attack, in short. Flooding websites or online applications with unwanted traffic and limiting access to the web server thereby create a disruption in normal traffic flow.

DDoS attack is defined as a state of the system where multiple computer systems are compromised (a server, website or network resource) and results in denial of service for users. The flooding is caused by illegitimate incoming messages, connection requests and fake packets to the target system.

DDoS attacks have become a consistent phenomenon for enterprises. Large corporate houses have constantly been losing revenue due to compromised data and network outages. The growing importance of IoT devices and the emergence of botnets have increased the instances of DDoS attacks. Of late, traditional DDoS attacks have mutated into Advanced Persistent Denial of Service that target the database and applications apart from affecting servers. Hence the need for Mitigation Solutions meant for today's threat vectors.

Emerging threat vectors call for having in place a solution that can not only stop the most common DDoS attacks, but next generation intelligent threats. Botnets like Torii and DemonBot are capable of launching DDoS attacks that understand modern enterprise architecture and elements. Torii can take over IoT devices and is considered a far more persistent threat than Mirai – the malware that infects smart devices running on ARC processors. DemonBot has the capability to hijack Hadoop frameworks by using vulnerability in Hadoop's resource management tool to infect cloud servers. A scary trend observed recently is the availability of a new DDoS platform called 0x-booter; this has the ability to launch an attack on 16,000+ IoT devices with the Bushido malware – the Mirai variant.

"Security mechanisms should be put in place to inspect any web traffic (ingress or egress) with high scrubbing capacity

EXHIBIT 1: THE NEXT GENERATION DDOS AND WEB APPLICATION ATTACKS

Source: Radware

To fight against these advanced threat vectors, enterprises need to arm themselves with the most sophisticated security solutions. This would range from having the capability to mitigate volumetric attacks, network DDoS attacks, behavioral analysis, intrusion prevention system, SSL Protection and prevention of web application vulnerability exploitation. The benefit of Automation needs to be leveraged to withstand the evolving threat landscape.

FROM ON-PREMISE DDOS MITIGATION TO CLOUD-BASED PROTECTION SERVICES: THE NEED FOR BOTH

Traditionally, DDoS defenses relied on hardware-based appliances located in the customer's datacenters. However, in recent years, enterprises have been shifting more and more of their defenses from premise-based defenses to cloud-based DDoS scrubbing services.

Whereas in 2014, DDoS protection appliances accounted for nearly 75% of revenue of the DDoS protection market, Frost & Sullivan estimates that by 2019, over 50% of market revenue will be based on services.

The biggest advantage of Cloud-based DDoS defenses is the pay-per-use SaaS subscription model, which enables organizations to quickly scale up or down as per need and doesn't require the allocation of substantial capital funds for procurement. Cloud-based DDoS services provide visibility into inbound traffic of the organization where inspection happens and malicious traffic is flushed out. These solutions have the capacity to stop high volume DDoS attacks that often saturate the inbound communication pipe.

However, cloud-based scrubbing services usually have visibility only into the inbound traffic channel, and in certain cases there is a need to have visibility into both inbound and outbound traffic channels to avoid a DDoS attack. This includes Out-of-State Protocol Attacks, Reflection or Amplification Attack and Scanning Attacks.

Relying on a premise-based hardware DDoS Appliance offers several advantages. For example, there are certain types of Layer 7 (Application Layer) DDoS Attacks that exploit known protocol weakness in order to generate many forged application requests to saturate server resources.

Secondly, while some of these attacks can be mitigated by using a cloud-based scrubbing center, others require application awareness that most cloud-based DDoS service fail to provide. SSL encryption is another important layer of inspection that most cloud-based DDoS Mitigation services do not provide due to their inability to inspect SSL-based traffic or use full proxy SSL offloading.

Finally, a hardware-based appliance in combination with cloud-based service is an ideal layered protection approach that enterprises should think about incase malicious traffic percolates through any one of them.

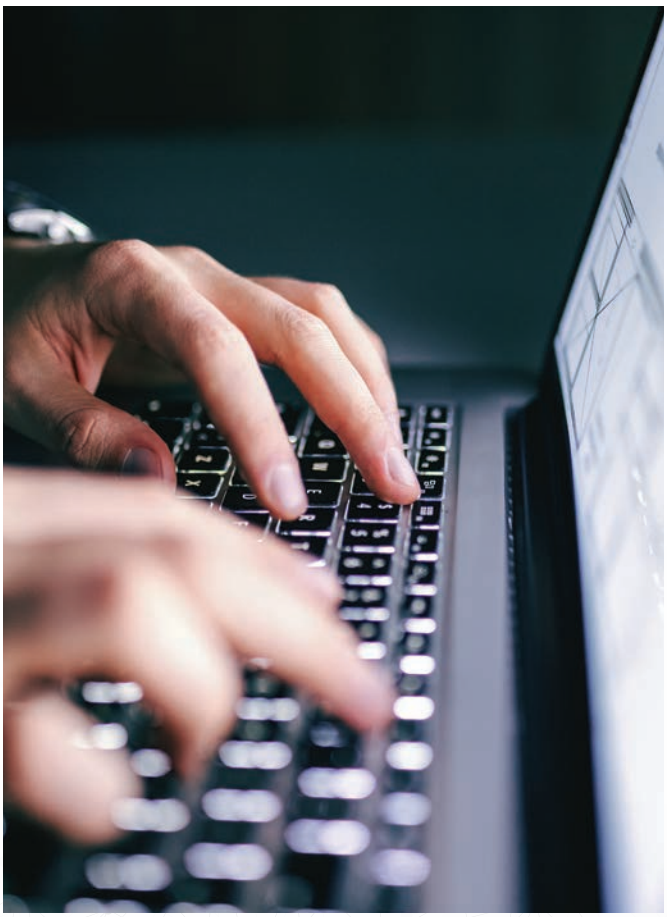


EXHIBIT 2: ADVANTAGES OF PREMISE-BASED AND CLOUD-BASED DDOS MITIGATION SERVICE

PREMISE-BASED DDOS APPLIANCE	CLOUD-BASED DDOS MITIGATION SERVICE
Ability to provide visibility into both inbound and outbound traffic	Offered as a Pay-per-Use Model
Better Application Layer (L7) DDoS protection and SSL handling capability	Highly Scalable and flexible
Better protection from SSL-based attacks	High Mitigation/Scrubbing Capacity
Dedicated hardware with complete control over threat mitigation	Easier Management, faster on-boarding process
Provides better application state awareness	Leverages latest technology capability: automated and behavior-based

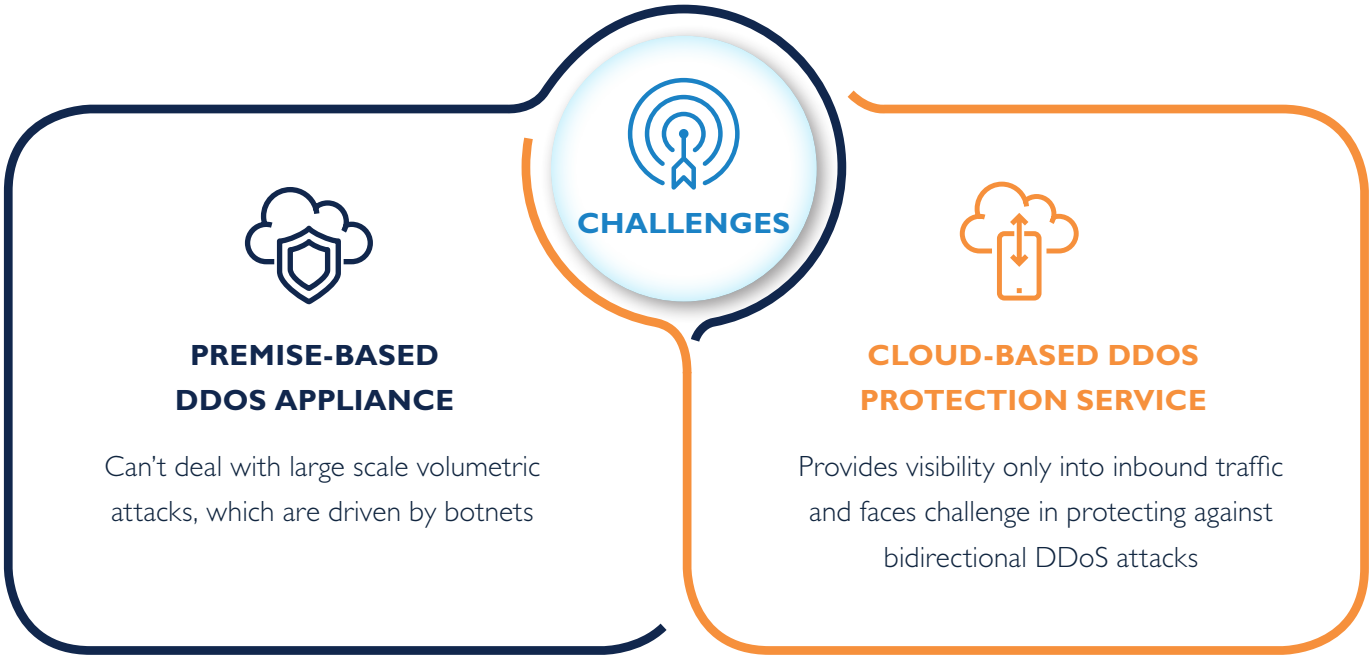
Source: Frost & Sullivan

THE IDEAL SOLUTION: HYBRID ALWAYS-ON DEPLOYMENT MODEL

Being an enterprise, it is important to gauge the advantages that any specific technology or service model offers. And in this case it is evident that both the on-premise and cloud-based services offer unique value propositions, yet do not provide complete coverage when measured separately. It is best if enterprises can employ the benefits of both worlds and derive a measurable outcome.

In the current state of volumetric DDoS attack where sophistication of attacks has constantly bothered security professionals, a Hybrid Always-On Approach is considered to be an optimal solution.

EXHIBIT 3: WHY EMBRACE A HYBRID MODEL?



Source: Frost & Sullivan

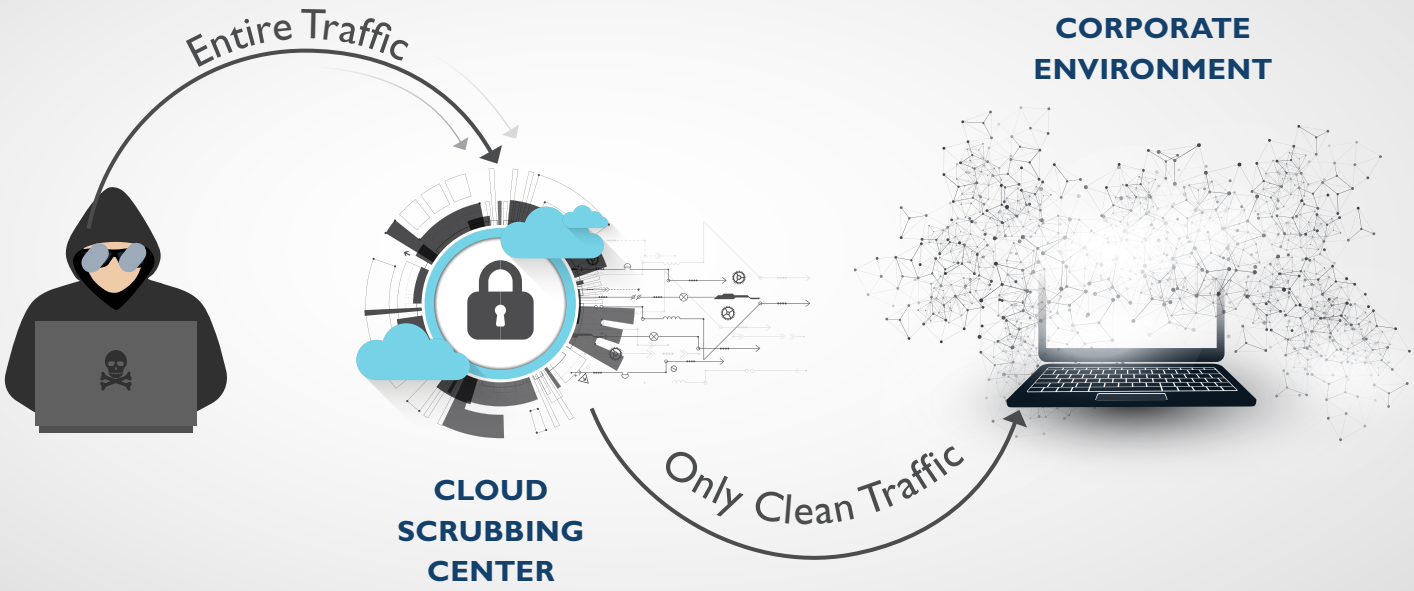
The Hybrid approach ensures that web servers/ applications are always running as they combine DDoS hardware appliance with cloud-based scrubbing service. As compared to the pure cloud-based service model, the integrated and hybrid always-on model takes a multi-layered approach against symmetric DDoS attacks that fills-in the egress traffic and allows maintaining SSL certificates on-premise.

A DDoS Service delivered over the cloud can come in two deployment models: on-demand and always-on. On-demand Cloud Service is a deployment scenario where the traffic is diverted from the customer premise to the cloud-based scrubbing center only when a DDoS attack is being detected by the system. While on-demand model does not call for any latency, it is handicapped and cannot detect non-volumetric attack vectors.

Moreover, one of the key limitations of on-demand cloud services is that there is also a diversion gap between the time a diversion is initiated and until the scrubbing center can take over. This diversion gap is the result of the time that it takes routing tables to update globally.

In contrast, for an Always-on Cloud Service the traffic is routed permanently through the cloud scrubbing center where it is always inspected and only legitimate clean traffic is passed on to the customer. Unlike on-demand services, there is no diversion gap, and traffic is always protected.

EXHIBIT 4: ALWAYS-ON CLOUD DDOS MITIGATION SERVICE



Source: Frost & Sullivan

> *The Hybrid Always-On DDoS Mitigation Service helps organizations fight web threats by offering minimum latency and quick mitigation capability*

THE RADWARE WAY: INTEGRATING ALWAYS-ON CLOUD SERVICE WITH HARDWARE APPLIANCES

Radware is a trusted brand in the Web Application Firewall and DDoS Mitigation market. The company has one of the largest scrubbing networks in the world with over 5 Tbps of scrubbing capacity. Currently, the company operates in 11 cloud-based scrubbing centers with an ability to guarantee long term DDoS mitigation capabilities.

DefensePro is the premise-based DDoS Mitigation appliance from Radware. It integrates with Cloud-based scrubbing centers using DefenseMessaging, an information sharing mechanism for different layers of DDoS Mitigation.

Radware offers hybrid solutions, which can combine a premise-based DefensePro appliance either with its "on-demand" Cloud DDoS Protection Service or its "always-on" cloud service. For deployments based on always-on cloud service, there will not be any diversion time gap, and user traffic will be constantly protected by both the hardware appliance, as well as the cloud scrubbing center. The DDoS vendor has built separate data paths to scrubbing centers for always-on traffic.

Given the capability that Radware as a company has in terms of owning and developing its own equipment (doesn't have to depend on any third party vendor) the company has the capability to inspect any kind of traffic. To increase threat detection capability, Radware receives threat intelligence feeds that get integrated with DefensePro Mitigation appliances. The unique DDoS attack detection capability built on Always-on Hybrid DDoS model makes Radware a leader in the space.

EXHIBIT 5: CAPABILITIES OF RADWARE ALWAYS-ON/HYBRID DDOS PROTECTION MODEL

FEATURE	CAPABILITY
Detection	For both Volumetric and Non-volumetric DDoS Attacks
Diversion Time Gap	No
SSL Key Storage	On-premise
High Capacity Volumetric Protection	Yes
Bidirectional DDoS Protection	Yes
Ideal For	Best for mission-critical applications that cannot afford downtime

Source: Radware

THE RADWARE VALUE PROPOSITION AND UNIQUE DIFFERENTIATOR

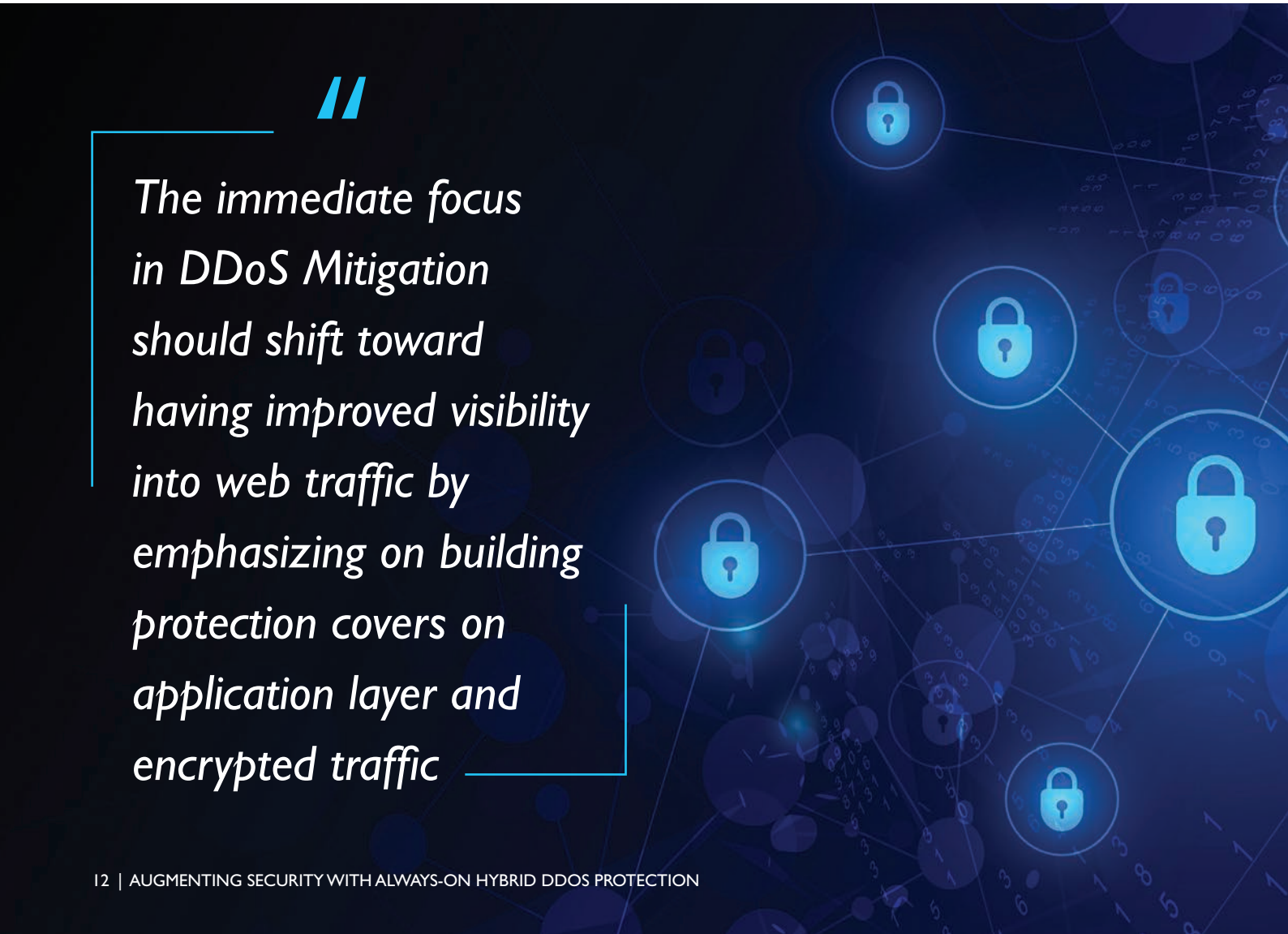
Being a world-class security vendor with strong focus on DDoS Mitigation, Radware has time and again proved its mettle in handling and stopping both volumetric and non-volumetric cyber-attacks. Its dedicated Always-on Cloud scrubbing center can mitigate the most powerful DDoS attack with minimum latency and faster response. The seamless integration of DefensePro with DefenseMessaging technology and intelligence feed makes Radware a trusted partner for all Application Layer security needs. The highest quality mitigation capability of Radware helps enterprises enjoy features of both premise-based and cloud-based DDoS mitigation solutions.

> *Radware has been honored with the prestigious 2019 Frost & Sullivan India WAF & Anti DDoS Vendor of the Year Award*

THE LAST WORD: WAY AHEAD IN DDOS MITIGATION

DDoS attacks have snowballed with far more devastating impacts for enterprises than they were almost 2 decades earlier. The acceptance of IoT and emergence of 5G network communications will constantly challenge the Anti DDoS mechanism for companies as attackers will take advantage of IoT devices, higher bandwidth, and faster internet speeds. Enterprises need to partner with security vendors who have AI-based and Automation solutions to minimize human intervention. Enterprises need to adapt defense strategies that focus on the 'intelligence' factor.

The future of DDoS solutions would analyze data streams, establish data communication profiles for the company and re-construct adaptive security strategies. It is time for enterprises to build cyber defense frameworks in-line with the current threat landscape and leverage the best in class security technologies.



"The immediate focus in DDoS Mitigation should shift toward having improved visibility into web traffic by emphasizing on building protection covers on application layer and encrypted traffic

ABOUT FROST & SULLIVAN:

For over five decades, Frost & Sullivan has become world-renowned for its role in helping investors, corporate leaders and governments navigate economic changes and identify disruptive technologies, Mega Trends, new business models and companies to action, resulting in a continuous flow of growth opportunities to drive future success. Contact us: Start the discussion.

www.frost.com

ABOUT RADWARE

Radware® (NASDAQ: RDWR), is a global leader of cyber security and application delivery solutions for physical, cloud, and software defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.