

Online Business Protection with Radware

You Put a Lot into Getting Your Business Online. Let Radware Protect it from the Threats Trying to Bring it Down.

Organizations of all sizes and from all industries are transforming into online businesses. Organizations that sell products or services through online channels consistently experience higher growth and increased profits over those that don't. Even companies that don't sell or deliver over the Internet have come to rely largely on online processes or systems to increase customer or partner engagement and make employees more productive.

However, as organizations' reliance on the Internet continues to grow, so too do the threats that can interrupt or exploit online systems. According to a survey of over 300 IT professionals in Radware's 2015-2016 *Global Network and Application Security Report*, over 90% of organizations have been attacked and 62% of those suffered downtime or degradation. Downtime results in a complete loss of online revenue and productivity. Performance degradation is also a significant problem, as customers now will wait 3 seconds or less before moving on to a competitor site.

To ensure online revenues, avoid negative customer or partner experience and manage the threat of sensitive data breach, organizations need a comprehensive solution to address threats that target website availability, sensitive transactions and data.

Radware's Online Business Protection solution ensures the integrity and availability of your network-based business by providing protection from today's cyber-attacks. The solution helps business and IT executives reduce the risk of lost revenue, customer churn, employee and partner productivity by protecting networks and applications from threats to availability and data breach.

Today's Threats Against Online Business

The cyber-security threat landscape continues to evolve in ways that challenge the ability of security teams to protect critical assets. Among the many trends related to the threat landscape is the dramatic increase in multi-vector attacks: attacks that employ a variety of tactics to complicate detection and mitigation. Over 50% of the attacks Radware mitigates on behalf of customers include more than five attack vectors, including advanced application attacks and "smoke screen" attacks that use DDoS attacks to mask other tactics. To target an organization's blind spot, attackers deploy parallel, multi-vector attack campaigns by increasing the number of attack vectors launched in parallel and targeting different layers of the network and data center. If only one vector goes undetected, the attack is successful and the result is highly destructive.

To effectively mitigate all types of DDoS attacks, organizations need a single vendor, hybrid solution that can protect networks and applications for a wide range of attacks.

Coordinated Protection from Innovative, Patented Technology

To support Online Business Protection, Radware offers a hybrid solution that integrates on premise, real-time attack detection and mitigation with on-demand, cloud-based protection to block volumetric attacks. The solution includes all the different technologies needed, including DDoS protection, behavioral analysis, IPS, encrypted attack protection and web application firewall (WAF). Collectively, these technologies provide protection from advanced application and network attacks that threaten downtime and pose a risk to sensitive data.

Radware's solution features innovative, patented automation capabilities to minimize manual maintenance and keep up with today's automated threat landscape. Real-time signature development and automated policy generation ensure protection from all known threats as well as zero-day threats, new attacks you haven't previously seen.

Because an increasing percentage of traffic managed by online businesses is encrypted, Radware's solution delivers unique capabilities for detecting and mitigating attacks that other solutions miss because they are hidden within encrypted traffic. Attacks leveraging encrypted traffic as an attack vector are on the rise, further challenging many of the cyber threat solutions currently in place. Most cyber-attack mitigation technologies do not actually inspect SSL traffic, as it requires decrypting the encrypted traffic. According to Radware's *2015-2016 Global Network and Application Security Report*, as much as 25% of attack activity today is using SSL-based attack vectors. Radware offers the industry's most complete SSL attack mitigation solution. The solution meets the needs of high capacity mitigation solutions, supports all common versions of SSL and TLS, and isolates suspicious encrypted traffic using behavioral analysis to limit legitimate user impact.

Built to Scale and Evolve with Your Business

Today's IT environments are undergoing constant change, further complicating the challenge of providing protection. Radware's solutions for Online Business Protection can evolve with the evolution of your online business infrastructure through seamless security orchestration across hybrid environments that include assets in data centers and multiple cloud hosting environments. As applications and other IT assets migrate to the cloud, Radware can provide coordinated security across on premise and cloud-based components. Radware's Cloud Security platform provides a highly scalable infrastructure with over 2 Tbps of attack protection enabling it to scale to the largest of volumetric threats.

Radware's solution also leverages patented Defense Messaging between Radware's security CPE and cloud security nodes, which shares real-time information on normal traffic baselines, protections and attack footprints, thereby eliminating blind spots and protection gaps across the organization's disaggregated network.

Another trend within online businesses is the proliferation of applications that are often generated via DevOps environments and undergo frequent code changes. Radware's solution supports dynamic application security to ensure protection in these fast-changing application environments and offers a

first to market Runtime Application Self-Protection (RASP) solution that automatically identifies changes in web application code and automatically generates new protections through a virtual patching process on the web application firewall.

Making it Easy to Find the Right Fit

Radware’s solution for Online Business Protection can be implemented with modular components, with each step aligning with the particular protection needs of different types of businesses. The below “Good, Better, Best” deployments align with common requirements, but can be tailored for an individual customer’s needs.

SOLUTION COMPONENTS			
	Radware Cloud WAF, DefensePipe Cloud DDoS Protection	DefensePro, Defense SSL, AppWall On-Premises WAF	Hybrid DDoS Protection, Hybrid WAF, Defense SSL, ERT Premium
	GOOD	BETTER	BEST
Volumetric DDoS	✓	✓	✓
Always On DDoS		✓	✓
Multi-Vector Protection	✓	✓	✓
Zero Day Protection	✓		✓
Automated Security Policy		✓	✓
Premise/Cloud Policy Coordination			✓
Encrypted Attack Protection		✓	✓
Fully Managed Service			✓

Because of the fast changing threat landscape, many IT and security teams are struggling to keep up in way that allows them to manage security solutions. Radware offers fully managed services to simplify the deployment and management of components of the Online Business Protection solution. Additionally, Radware’s solution offers the ultimate flexibility in financing options, enabling customers to utilize CapEx, OpEx, or a combination of the two.

Best-of-Breed Components in a Single-Vendor Solution

The technology components that make up Radware’s solution for Online Business Protection represent some of the leading products and services within their distinct security categories. Through coordinated protection capabilities, they represent an even more complete solution. The components include:

- **Radware DefensePro:** an award-winning, real-time, perimeter attack mitigation device that secures organizations against emerging network and applications threats. DefensePro protects the infrastructure against network and application downtime (or slow time), application vulnerability exploitation, malware spread, network anomalies, information theft and other types of attacks.

- **Radware DefensePipe:** cloud-based DDoS protection against Internet pipe saturation caused by volumetric attacks. DefensePipe provides access to more than 2 Tbps of scrubbing capacity. Based on the built-in synchronization between the data center, Radware's attack mitigation device and cloud scrubbing service, the in-the-cloud mitigation can start immediately.
- **Radware Appwall:** an on premise Web Application Firewall (WAF) that provides complete protection against web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages and more.
- **Radware Cloud WAF:** Based on Radware's ICSA Labs certified market-leading web application firewall, Radware's Cloud WAF service provides full coverage from all OWASP top-10 attacks. The service implements both negative and positive security models by utilizing its unique ability to automatically adapt to the continuously changing threat landscape and defendable online assets.
- **Radware Defense SSL:** mitigates SSL encrypted flood attacks at the network perimeter. The solution mitigates SSL-based attacks using challenge-response mitigation techniques and SSL decryption and challenge response mechanisms are enforced only on suspicious traffic. The result is the lowest latency SSL mitigation solution in the industry, as legitimate traffic is not affected by the mitigation efforts.
- **Radware Emergency Response Team (ERT):** 24x7 support for hands-on attack mitigation assistance from a single point of contact. The ERT provides expertise needed during prolonged, multi-vector attacks. This includes working closely with customers to decide on the diversion of traffic during volumetric attacks, assisting with capturing files, analyzing the situation and ensuring the best mitigation options are implemented.

Learn More

Online businesses that want to protect themselves from today's advanced cyber-security threats should turn to Radware for comprehensive attack protection. To learn more about Radware's flexible solutions for Online Business Protection, visit www.radware.com.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.