Guide

Radware 360° Application Protection

The Need for Consolidating Your Application Protection Solutions

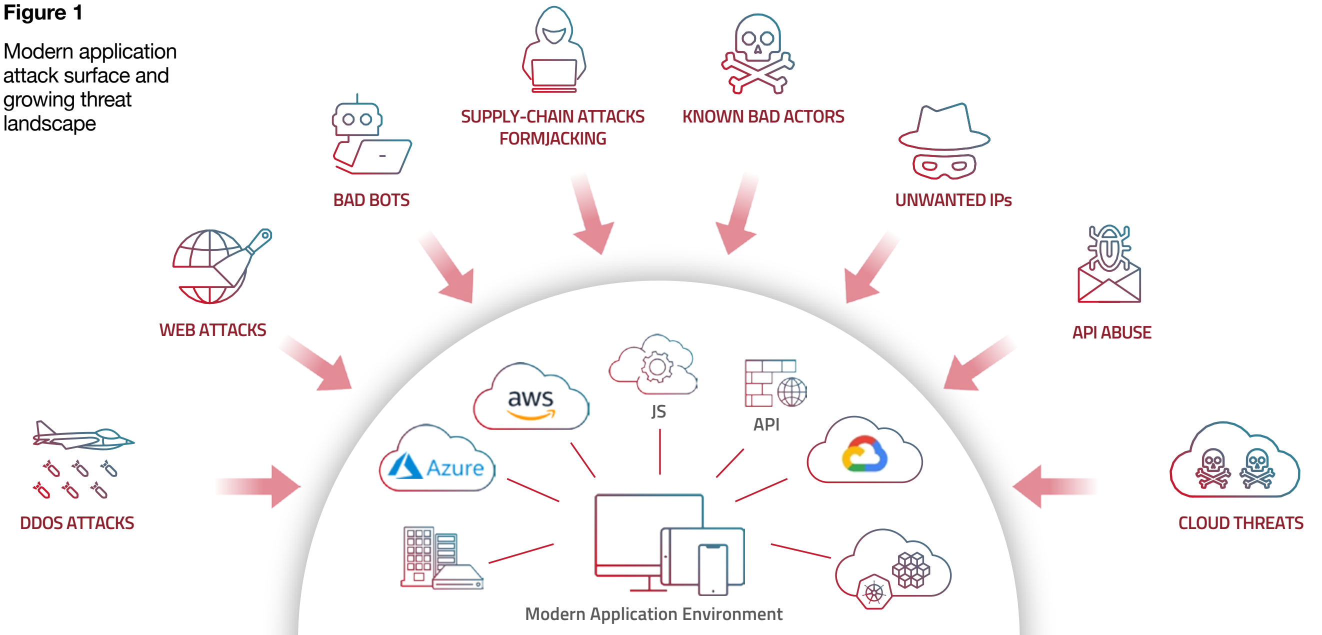
For many organizations, the greatest concern they have about migrating their application environment to the cloud is what it may mean to their attack surface. Their concern is valid. No question, their attack surface will expand. But that hasn't stopped them from moving to the cloud anyway. Research shows that less than 0.05% of organizations don't deploy applications in the cloud and at least 95% use at least two types of cloud infrastructures.* Almost all still maintain some applications and workloads on-prem. What does this mean to network security? Yes, it is complicated. There are a lot of issues and architectures to think about.

Here are a few other factors to consider: Cyberattacks are up, the number of threat actors is increasing and there are so many security options to choose from in the marketplace. Also, the array of threats you need to protect against is staggering. There are data breaches, identity thefts, hijacked accounts, DDoS attacks, API abuse, sophisticated human-like bots and more.

* Link to the Osterman Report – https://www.radware.com/multi-cloud-report-2022/

Figure 1

Modern application attack surface and growing threat landscape



Combine this complexity with tightened budgets and the shortage of security expertise worldwide and thoughts of securing your applications becomes even more stressful. Trying to cobble together a security plan with different vendors only serves to muddy the waters. It results in poor security and higher costs. It creates security siloes that can spell disaster.

Holistic Application Protection – From Browser Side to Server Side

Whether organizations use private, public or hybrid cloud solutions, it's important that they choose an application protection solution that provides blanket protection. The threat landscape is too varied and complex. In war, you have to protect from air, land and sea. Application protection is no different. You must protect against all threats, not just a percentage of them.

For instance, while protecting against The OWASP Top 10 Web Application Security Risks imperative, the application protection solution in use may not be the right one to protect against other threats, such as sophisticated API abuses or Gen4 bots. Security gaps need to be filled. Threat actors are good at finding open ones. Unfortunately, this is the career they've chosen—and they're good at it.

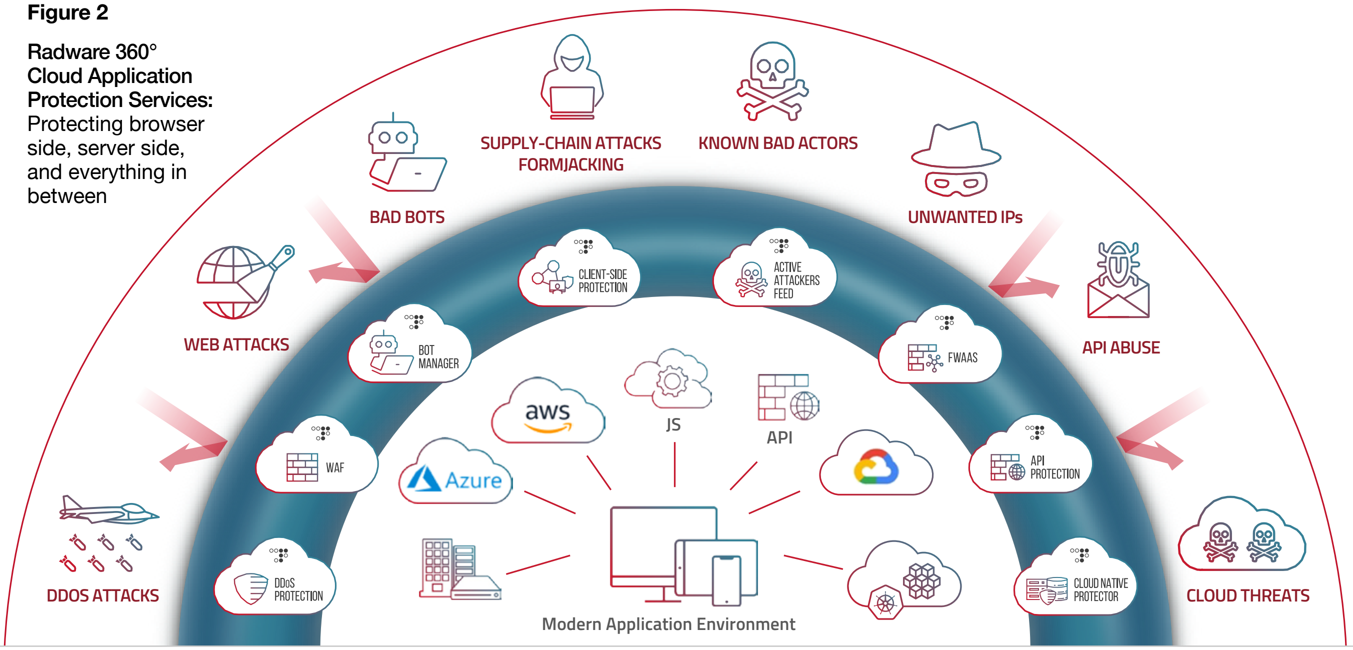
Easy Oversight and Simple Management from a Single Console

While having the right solutions in place to fight today's and tomorrow's threats is important, don't ignore the importance of management. Fighting against so many different types of threats can be difficult—even more so if you need to manage against each one from a single console.

The idea is to make management as simple as possible. The simpler the management, the less likely a security ball gets dropped. And a dropped ball is another way of saying security gap. That's what you have to avoid. Management should be easy, yet comprehensive, and capable from a single console.

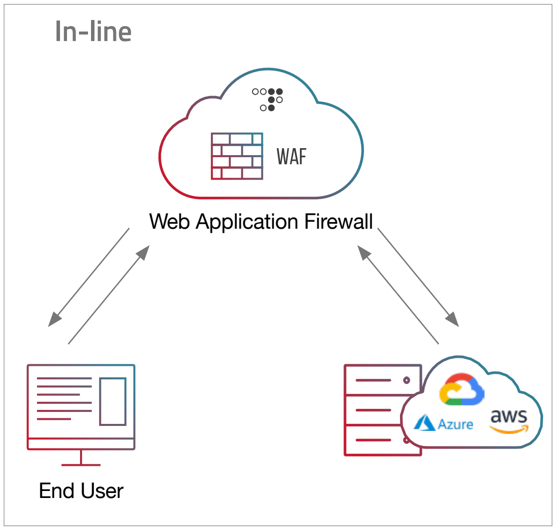
Figure 2

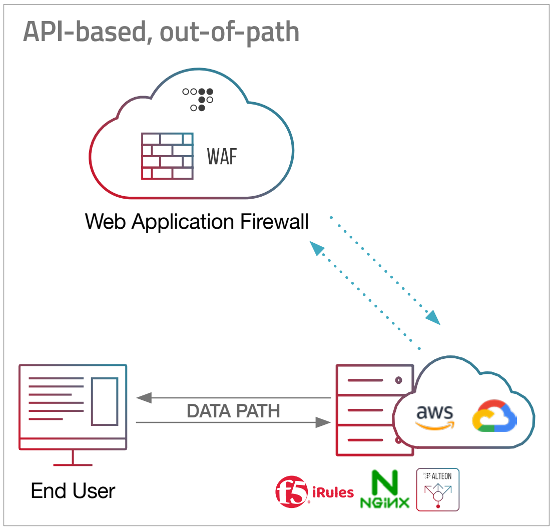
Radware 360° Cloud Application Protection Services: Protecting browser side, server side, and everything in between



Multiple Deployment Options

No two networks and architectures are alike, so selecting a security platform that will accommodate your unique needs is critical. You shouldn't have to accommodate a security vendor's pre-determined architecture. Security solutions need to be flexible to meet your deployment needs. For instance, you can choose to deploy inline in your virtual cloud or on-prem environment,or you may need the option of deploying it without traffic redirection or without sharing SSL certificates. You can do so as an API-based, out-of-path service across your public cloud or on-prem/virtual application delivery controller (ADC).





Whether a cloud or hybrid environment, having options means that your security can remain consistent across your varied environments and not get in the way of planning and migrating your applications to new environments. Your trusted application protection solution must be future proof and agnostic to your applications' hosting or content delivery network (CDN) environments.

Managed Services Reduce Overheads and Tighten Security

Protecting your organization from cyberthreats is a daunting task. Chances are that most of your team is focusing on the several threat areas they are familiar with. And there is a better than average chance that you do not have the security skill sets on —or enough security engineers—on staff to allay fears you have about being the next cyber victim. That's why selecting a security platform that provides fully managed service around the clock is critical for reducing operational costs and ensuring superior protection. Doing so will help you save on resources used for configuring security policies, mitigating attacks and sorting through the noise of endless security events. Last but not least, it will help you reduce false positives and ensure that security does not stand in the way of your business.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity 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 quickly to market challenges, 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: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.