radware

White Paper: **Frictionless Security**

Best Practices for Frictionless Application Protection

Table of Contents

Overview 3

Challenges To Securing Applications 3

What is Frictionless Security? 4

Best Practices For Protecting Networks, Applications and APIs 5

Frictionless Security with Radware 7

- Application Protection 7
- Denial-of-Service Protection 8
- Public Cloud Protection 8
- Application Delivery 8

Overview

Organizations continue to migrate applications to the cloud at an increasing rate. During 2020 and 2021, transition to cloud-based deployments exploded as businesses adapted to the pandemic by focusing on digital transformation and delivery. A recent survey by Harvard Business Review/ Splunk found that 69% of respondents say that 60% or more of their organizations' infrastructure and applications will be in the cloud in 2022.

Not only are businesses transitioning to the cloud, they're adopting a multi-cloud strategy. According to Flexera's 2022 State of the Cloud Report, 89% of respondents reported having a multi-cloud strategy, and 80% are taking a hybrid approach by combining the use of both public and private clouds.

DevOps, agile development and the modernization of legacy applications going through a "lift and shift" to the cloud means safeguarding applications across hybrid environments is becoming increasingly difficult.

Challenges To Securing Applications

1. Uncertainties In Cloud Migration And Deployment

- It is impossible to predict what infrastructure or security threats will look like in a few years, so organizations need to be environment agnostic, adaptable and flexible in their approach to securing applications

2. New Technologies And Architectures

- New forms of application development scalability and packaging, such as API-driven, microservices and container-based architectures, require modern approaches to securing east-west traffic and to accommodate agile, fast-paced DevOps development cycles.
- Agile software development: In many cases, the main driver for migration to the cloud is more agile and flexible application development. Security often falls by the wayside. In other words, applications hosted in the cloud frequently change but must be secured in a frictionless manner that will not become an obstacle to agility.

3. Complexity of Multi-Cloud Deployments

- Many organizations deploy several cloud environments in parallel, further complicating the task of cloud security. It is very difficult to protect multiple cloud platforms, as each has its own capabilities, APIs, management and reporting.

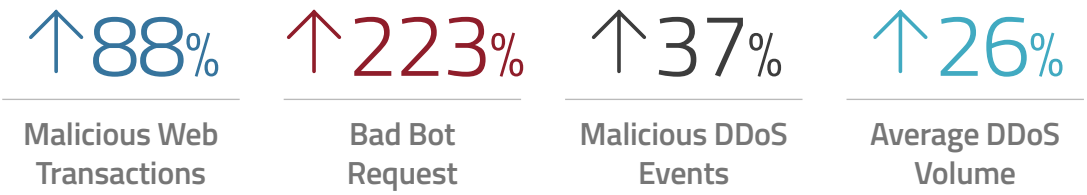
4. Wider Threat Surface and Emerging Threat Vectors

- The sophistication of cyberattacks continue to grow as hackers improve their techniques, thinking of new ways to attack organizations and circumvent existing protections. This exposes applications to new attacks, which cannot be mitigated

with traditional or existing defenses. According to Radware's 2021-2022 Global Threat Analysis Report, average DDoS attacks per customer increased by 26% while microflood attacks that target applications increased by 79% in 2021 compared to 2020.

Figure 1

Radware's 2021-2022 Global Threat Analysis Report



- In the past, organizations had direct control over the application's backend infrastructure, leaving only the customer-facing side exposed externally. However, in a cloud environment, both the application surface and the application infrastructure are exposed. Both require protection.

5. Lack of Consistency

- Every vendor provides their own monitoring tool, often working differently to accommodate differences in the cloud environments. This creates an issue of consistency in both deployment as well as management of configurations, logs and policies.

6. Actionable Visibility

- Lack of insightful and actionable reports for both NetOps and SecOps.
- Dependency on security experts for addressing false positives and other application threats.
- Poor end-to-end visibility with SLA, single pane of glass for configuration, management, monitoring, analytics, and reporting that covers all deployment environments.

7. Lack of knowledge and control of security and deployment domains

- Rapid digital transformation to meet the needs of the evolving market, new "remote" lifestyle and to keep up with competition requires rapidly acquiring relevant digital security knowledge, infrustructure and in-house expertise.
- Although security staff is commonly tasked with protecting cloud environments, they frequently have no authority over the choice or management of cloud environments. According to Radware's research, 92% of organizations stated decisions about cloud platforms are made by stakeholders other than security staff.

What is Frictionless Security?

A frictionless security approach must address security concerns of customers migrating to a multi-cloud or hybrid deployment. Frictionless security also provides uniform security for applications everywhere to enable the same level of protection

agnostic to the application environment, whether it be private or public clouds, while not proving a roadblock to the business.

Here are eight vital best practices to ensure your security is as “frictionless” as possible.

- It is integrated as much as possible with the development cycle and does not interfere with business processes.
- It is adaptive to change in line with frequent changes to applications and the underlying deployment platform.
- It is agnostic to the environment and can be maintained throughout the cloud transition regardless of the pace of migration and the final destination of the application.
- Provides extensive protection which covers all the critical threat vectors for application security.
- Enables automated protection using advanced algorithms to focus on real threats and offloads manual tasks that can be automated.
- Provides continuous and automatic policy updates and refinements to keep up with security threats and keeps false positives to a minimum and keeps traffic flowing.
- Is consistent in providing state-of-the-art security for all apps regardless of the deployment environment - private/public cloud. This enables the same level of protection agnostic to where the apps are deployed.
- Promotes trust in your security provider that can take full responsibility and support you with the security expertise to implement your strategy.

A sound security strategy must protect infrastructure and applications from denial-of-service, application and bot attacks, vulnerabilities and manipulations, excessive permissions, entitlements and malicious user activity, and prevent service disruptions. Ultimatey, security strategies must be both *frictionless* AND *state-of-the-art.*

Best Practices For Protecting Networks, Applications and APIs

There are many areas that need to be addressed for securing infrastructure and applications. Best practices enables organizations to implement consistent security policies across application deployments. Education and awareness of techniques used in phishing and social engineering go a long way in mitigating factors that play a large part in human security failures. Ensuring that networks, APIs and applications are accessed by the right users that are authorized and authentic is critical. Removing configuration errors from creeping in during deployment by enabling automation as much as possible is now critical. Cloud workloads may have excessive permissions and should be checked frequently for breaches. In the event a breach does occur, having a defined incident response playbook will help.

Here are six best practices to ensure security doesn't become a roadblock to innovation and agility.

Figure 2

Best Practice for Scaling and Securing Applications

- **Define corporate compliance requirements and policies** for password, data security, backup, updates of operating systems, compliance and incident response. Educate employees and partners on social engineering, phishing and malware.
- **Enforce zero trust by enforcing access** for infrastructure, applications and APIs, including privilege access management and multifactor authentication.
- **Gain visibility into traffic** for proactive detection of malware, advanced persistent threats and to remove blindspots for encrypted traffic. Discover and secure any applications and APIs with external access and create reports of public exposure, misconfigurations and compliance violations with across multiple clouds. Correlate between security and SLA analytics or with SIEM.
- **Protect networking and application infrastructure and APIs** by integrating security practices in your development lifecycle. Routinely scan for vulnerability and protect your APIs and applications against service level breached due to DDoS, bot and web application attacks and implement denial-of-service protection, web API and application protection, protect against bot threats and document cloud assets and permissions.
- **Automate to reduce infrastructure, application and API misconfigurations** and automatically adjust security policies to optimally address peacetime and attack traffic.
- **Address multi-cloud networking and security expertise** by adopting processes that automate configurations to help with application scalability, monitoring, security and optimization across multiple clouds.

Frictionless Security with Radware

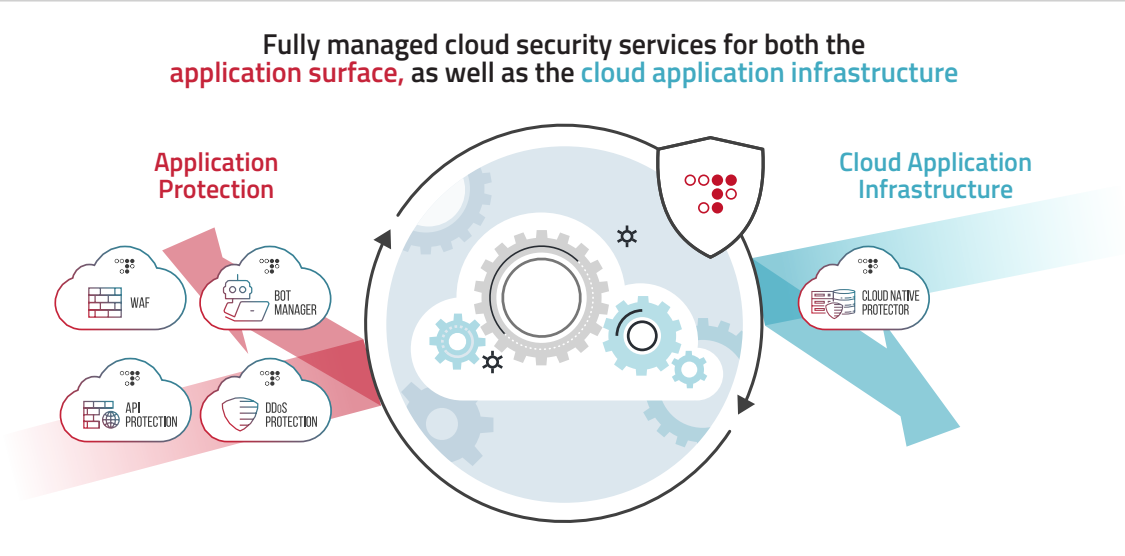
Radware's approach to security is frictionless and state of the art. It provides quality of protection while providing uniform security for applications deployed anywhere.

Radware provides a suite of tools that protect enterprises' public, private cloud and on-premise environments, offering solutions to safeguard both the internal and external surfaces of cloud and on-premise applications.

Radware's security solutions protect from denial-of-service, application and bot attacks, protects applications and APIs against vulnerabilities and manipulations, excessive permissions, entitlements and malicious user activity. It also prevents service disruptions while addressing trust and security concerns of customers migrating to a multi-cloud or hybrid deployments.

Figure 3

Frictionless Security with Radware



Application Protection

Web Application and API Protection (WAAP)

Radware provides an application protection and API protection/discovery solution suite for every environment, with automated security policy generation. The solution suite protects against 150+ known attack vectors, including the OWASP Top 10 Web Application Security Risks, Top 10 API Security Vulnerabilities and Top 21 Automated Threats to Web Applications.

The Radware WAAP solution is integrated with Radware Alteon (integrated WAF) as a managed cloud service (CWAF) or available as a solution in Kubernetes environments (KWAF) to easily integrate with common software provisioning, testing and visibility tools in the CI/CD pipeline.

Radware Bot Manager

Radware Bot Manager defends APIs against automated attacks and ensures that only legitimate users and devices can access the APIs while blocking any attempt to reverse engineer mobile SDKs. It uses intent-based deep behavior analysis (IDBA) behind an API request to block malicious activity

Denial-of-Service Protection

Infrastructure, applications and APIs may be attacked using a flood of requests to slow or disrupt a service or to gain access to databases. Many attacks, frequently using SSL, focus on rendering the web application layer unreachable, causing a denial-of-service state. A maliciously designed HTTP request can lead the web or application server to execute many internal requests that can consume all its resources. Radware's DDoS protection technologies, **Radware DefensePro and Cloud DDoS Protection Service**, provide the shortest time to detection and mitigation of HTTP-based DDoS assaults. Utilizing a patented keyless SSL protection technology, it keeps applications protected while maintaining user data confidentiality and compliance with privacy regulations.

Public Cloud Protection

Cloud Security Posture and Cloud Infrastructure Entitlement Management (CSPM, CIEM)

Migrating application workloads to the public cloud creates new threat surfaces which can be exploited by attackers and lead to theft of customer data. Radware's **Cloud Native Protector (CNP)** secures the cloud environment against identity and access abuse, protects against malicious user behavior, and secure the overall security posture of the public cloud environment.

Application Delivery

Reverse Proxy or Application Delivery Controller (ADC)

In an API-driven world, ensuring application SLAs are critical for ensuring the digital experience. ADCs are the foundation for keeping applications and their environments secure, scalable and available. **Radware Alteon** allows organizations to decouple user connections from applications to individually scale them while reducing both access latency and operational cost for scaling applications.

Learn More About How Adapting A Frictionless Security Strategy Provides Protection From Advanced Threats While Driving Business Agility

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.