radware

Radware Solutions for Financial Services Providers

WHITE PAPER

SHARE THIS WHITE PAPER

TABLE OF CONTENTS

Financial Services Concerns and Challenges

Financial services have historically been at the forefront of adapting to changes in technology, regulations and consumer behavior. While businesses focus on the challenges of customer experience, digital transformation and cloud adoption, the industry is dealing with increased risks posed by operational challenges and cybersecurity attacks. Migration to the cloud helps with cost savings and efficiency but results in multiple environments, limiting control of the network. Encrypted traffic is increasing as a proportion of network traffic and while adoption of new encryption technology adds data security, it also adds latency and infrastructure-capacity issues, making it more difficult for organizations to adapt.

Staying Open for Business (Protecting Availability)

Users expect their applications and information to be available 24x7. IT teams are required to deliver availability for applications while optimizing the experience for end users. Application availability and service levels may be degraded thanks to cyberattacks that threaten application operation or due to application or ISP link outages.

Businesses require integrated and automated application and security solutions that ensure business continuity and protect against advanced threats, such as IoT botnets. Attack vectors are changing and growing with malware, bots and social engineering emerging as the most common.

Based on Radware's *2017–2018 Global Application and Network Security Report*, holding company information for ransom was the motivation behind 50% of attacks in 2017, with one in eight companies suffering a DDoS extortion. DDoS attacks were reported by 40% of financial services organizations. These are some of the most popular cyberattacks.

- **IoT botnets** have earned their "right" as one of the top threats for organizations given the dramatic increase in the use of IoT devices to create powerful botnets. With additional botnets uncovered in 2017, it is clear that their impact on cybersecurity has just begun.

- **Ransom denial-of-service (RDoS)** attacks are one form of ransom-based attacks in which perpetrators send an email threatening to attack an organization unless a ransom is paid by the deadline. RDoS attacks have increased annually since 2010 and are particularly insidious because they do not require the attacker to hack into the target's network or applications.

- **Burst attacks and advanced persistent denial-of-service (APDoS) campaigns** include short bursts of high-volume attacks at random intervals and attacks that can last weeks that involve multiple vectors aimed at all network layers simultaneously. These types of attacks have a tendency to cause frequent disruptions in a network server's SLA and can prevent legitimate users from accessing services.

DDoS Attack Types Targeting Financial Services[1]

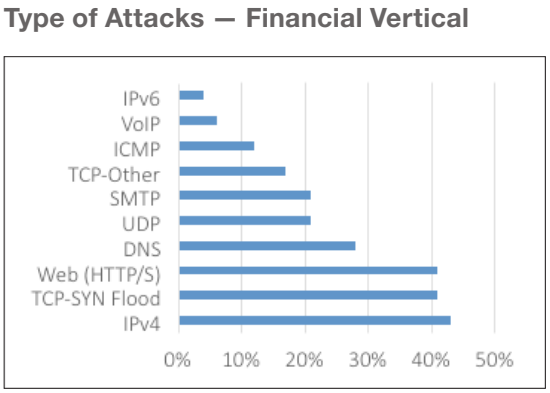

Figure 1: Which of the following attack vectors have you experienced this year?

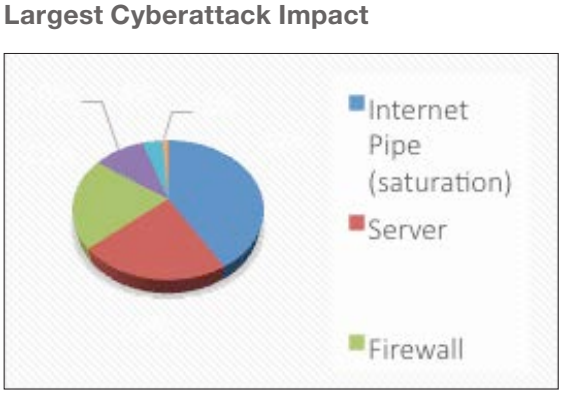

Figure 2: Point of failure during biggest cyberattack suffered?

Protecting Against Data Breaches

Complying to regulations and standards, such as PCI and GDPR, and protecting PII are constant concerns in the financial world. Based on Radware's *2017–2018 Global Application and Network Security Report*, protecting sensitive data is top of mind for most companies, with 28% naming data theft as their top security challenge, followed closely by availability and reputation loss. Results from the financial services sector mirror these trends.

- Forty-five percent of financial services respondents suffered a data breach
- Malware was reported by 50% of banks and financial services institutions
- Social engineering — getting a footprint inside the network and then leveraging it for various actions — was reported by 47%

In addition, applications are more frequently targeted as DDoS attacks shift to the application layer. Application attacks include DDoS attacks that use the Hypertext Transfer Protocol (HTTP) to exhaust their targets' resources, DDoS attacks that target application protocols, such as HTTPS, DNS and VOIP, with exploitable weaknesses, plus any attacks mentioned in the OWASP Top 10. Much like attacks targeting network resources, attacks targeting application resources come in a variety of flavors, including floods and "low and slow" attacks.

Encrypted Traffic Challenges

Encrypted traffic is increasing as a proportion of network traffic, reducing visibility to issues and attacks, while adoption of new encryption technology adds data security but makes it more difficult for organizations to adapt. Businesses need visibility into encrypted traffic and smart protection from encrypted attacks.

- **SSL/encrypted attacks:** Attackers are using SSL protocols to mask and further complicate attack traffic and malware detection in both network and application-level threats. Many security solutions use a passive engine for SSL attack protection, meaning they cannot effectively differentiate encrypted attack traffic from encrypted legitimate traffic and can only limit the rate of request.

[1]*2017–2018 Global Application and Network Security Report*

- **Limited visibility and new technology standards:** Network traffic encryption is necessary to keep data in motion secure; however, it limits organizations' visibility into their own data. Organizations are adopting new encryption algorithms, such as elliptic-curve cryptography (ECC), and newer transport protocols (TLS 1.3) while moving toward perfect forward secrecy (PFS) to protect data even when the encryption key is compromised. This sounds great, but how can organizations keep up with these technology requirements?

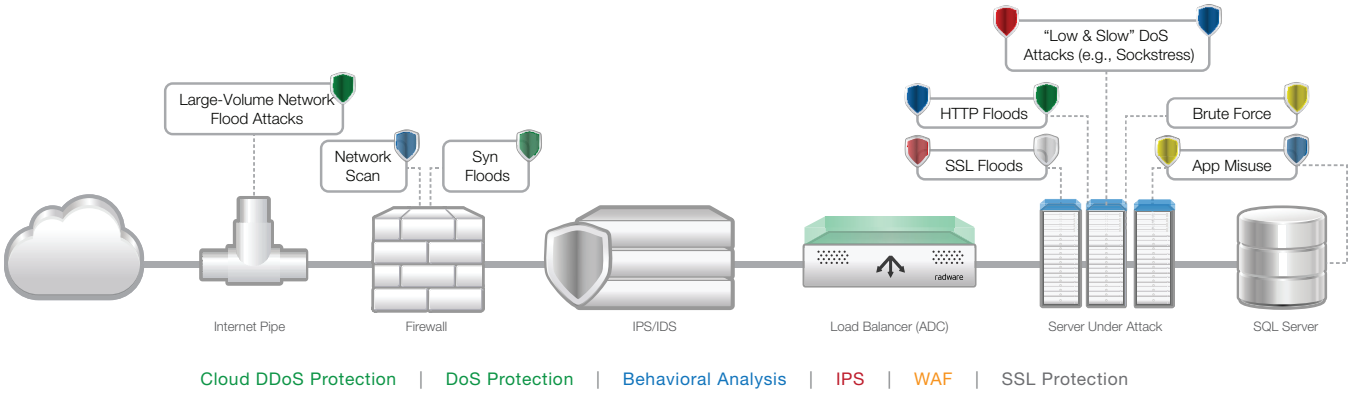

Figure 3: Attack vectors and the technology tools used to detect and mitigate

Cloud Migration

Organizations are transitioning to the cloud (either public, private or a hybrid model) and shifting the focus of their network environment from infrastructure to application. Migration to the cloud helps with cost savings and efficiency but results in mixed environments, thereby limiting control of the network. Security solutions using multiple technologies add to management and scaling complexity.

Cloud options provide application developers with easy means to build their own environments, making infrastructure managers less influential in the development phase but responsible to support environments that network teams cannot fully control.

Lack of Resources/Expertise to Manage Complex Protection

Protecting users' data is becoming increasingly complex. Although securing data, applications and network environments is critical, it's not the primary function of financial services businesses. Security operations teams are stretched to the max, and good engineers are hard to find.

Based on Radware's *2017–2018 Global Application and Network Security Report*, 48% of security teams aren't prepared to mitigate application DDoS attacks and over half are exhausted by a 24-hour attack. Not surprisingly, almost half of respondents prefer a managed security service.

The Solution

Radware can help you address financial sector challenges and secure your business with a comprehensive suite of advanced malware detection and prevention, DDoS protection and web application security solutions to protect digital assets both on-premise and in the cloud.

In addition, as financial services companies transition their services and applications to the cloud, Radware can offer secure application delivery and business continuity solutions to help with automation, availability and disaster recovery needs required in mixed environments.

Staying Open for Business (Protecting Availability)

In the online age, businesses need to maintain constant availability for customers. Radware helps organizations maintain and protect online availability with its stack of application delivery and security solutions.

Web App Acceleration

In an apps-driven world, a quality digital experience is critical. Both improving end-user quality of experience (QoE) and accelerating web application response time deliver several benefits to organizations. Radware's FastView helps companies improve online business metrics. Each second reduced with FastView immediately translates to improved online business metrics, including more page views, higher conversion rates, increased customer satisfaction and higher revenues.

Integrated and Automated Solutions

Today's standard defense technologies, including DDoS protection, anomaly and behavioral analysis, SSL protection and WAF, are often provided in point solutions. These systems are almost never integrated and require dedicated resources to maintain and synchronize.

Radware's Attack Mitigation Solution not only combines the aforementioned technologies in a fully integrated, on-premise and cloud detection and mitigation solution, but it also provides machine-based learning algorithms, real-time signature creation and auto policy generation that automate the attack life cycle process to shorten the time to mitigation, overcome hacker sophistication and automatically respond to attacks.

Radware's secure application delivery and load-balancing solutions allow financial services businesses to simplify operations while ensuring resilience and SLA. Radware's Alteon ADC ensures availability and disaster recovery for local and globally dispersed applications at all times and provides scalable architecture and automation across multiple environments.

Advanced IoT Botnet Detection

Radware offers a multivector attack detection and mitigation solution, handling attacks at the network layer, server-based attacks, malware propagation and intrusion activities. The solution includes protection against volumetric and nonvolumetric attacks, SYN Flood attacks, Low & Slow attacks, HTTP Floods, SSL-based attacks, Burst attacks, and more. As the solution analyzes the traffic, it builds traffic baselines that are customized for the deploying organization.

The solution provides the industry's most advanced automated protection from fast-moving threats from recent IoT-based attacks. It is uniquely built to overcome both the complexity and scale of today's sophisticated IoT-based botnets. Radware DDoS protection includes both behavior-based algorithms to protect from known and unknown DNS Flood attacks and a positive DNS security model to protect against DNS Water Torture attacks.

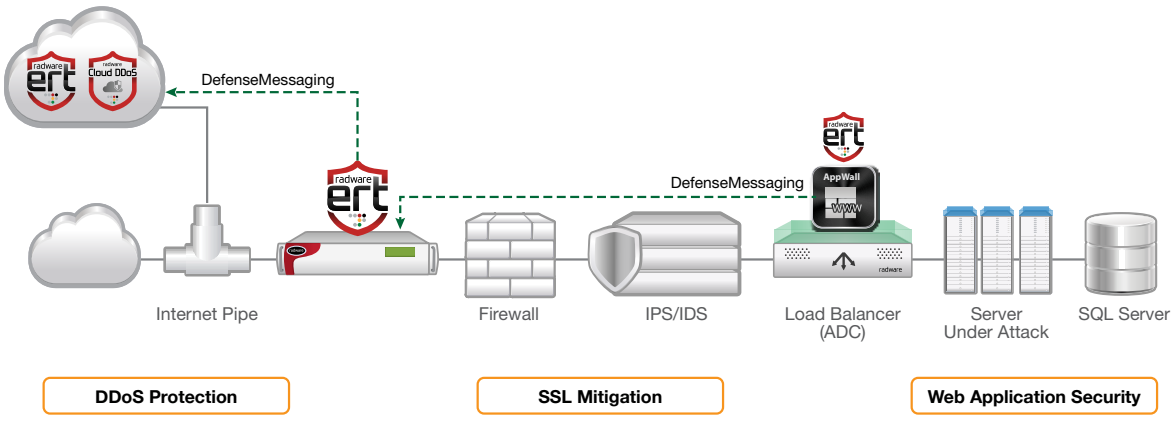

Figure 4: Radware's Attack Mitigation Solution

Protecting Against Data Breaches

Data theft is a key threat to the financial services sector, its customers and its business operations. It leads to massive fines, loss of reputation and loss of business. Radware helps organizations prevent data breaches via its suite of cloud-based security services to protect sensitive data and applications.

Web App Protection with Full Visibility

Radware offers an integrated security solution, which provides multivector web application protection with centralized management and reporting. The portal provides full visibility during peacetime and attacks, including real-time monitoring data, comprehensive alerting and periodical reporting tools, rich self-service frameworks, and full integration to external SIEM systems.

Web Application Security

Radware's WAF solutions ensure fast and secure delivery of mission-critical web applications for organizations worldwide. Radware's WAF technology, available via an on-premise appliance or as a cloud service, is recommended by NSS Labs and is ICSA Labs certified and PCI compliant.

Radware's WAF provides leading web application security by combining both a negative security model and a positive security model based on machine-learning technologies to provide comprehensive protection coverage against the OWASP Top 10 threats and other vulnerabilities. It provides patent-protected technology to create and maintain security policies in real time for the widest security coverage with the lowest false positives and minimal operational effort. Advanced automation capabilities facilitate seamless, risk-free onboarding and implementation of new application services. For organizations that have limited resources, Radware offers its Cloud WAF Service as well as a fully managed WAF solution.

Data Protection from Evasive Malware

Radware's Cloud Malware Protection Service defends against zero-day malware not blocked by traditional anti-malware defenses. It eliminates evasive threats with machine-learning analysis by studying the malware and host's unique communication patterns and blocking malware activity to prevent data breaches and protect PII.

Companies suffer from malware entering and remaining in the network (average of 200 days). The Cloud Malware Protection Service works with web security gateways, IPS/IDS, SIEM or endpoint security to prevent and clean malware from the network.

Compliance and Protecting PII

Financial services organizations are required to comply with regulations and security standards, such as PCI, GDPR and others. Radware's security network has one of the industry's most extensive lists of certifications and compliance credentials, so customers' private user data is always protected.

- Radware has the industry's most expansive set of compliance certifications, including PCI, HIPAA, GDPR and advanced ISO regulations deal specifically with private data security in the cloud.
- Radware's SSL inspection is able to discern between legitimate traffic containing PII and legitimate traffic that does not, so only non-PII traffic is decrypted and inspected. This allows companies to be compliant with regulations around PII, but at the same time does not compromise security visibility.
- Radware's DDoS and WAF solutions provide protection against attacks and security incidents and the unauthorized disclosure of PII. In addition, Radware's WAF keeps sensitive data safe by securing inbound and outbound traffic from web servers, inspects all web application output, and masks or blocks PII data.

- Radware's Cloud Malware Protection Service helps customers meet compliance requirements, such as PCI, HIPAA and GDPR, by blocking key vectors for data theft. It includes powerful auditing tools tested against some of the latest zero-day malware currently in circulation.

- Radware helps organizations meet GDPR requirements by securing web applications against data breaches and provides automated tools to simplify security compliance-related tasks.

Encrypted Traffic Challenges

Radware enables organizations to deliver and inspect SSL traffic and protect against SSL-based attacks.

Visibility into Encrypted Traffic

Websites, enterprise applications and web services are mandating the use of encryption. New ciphers and key-exchange mechanisms that deliver higher levels of security are available, but they also increase IT infrastructure loads.

Radware provides an industry-leading solution that addresses all the aforementioned challenges for offloading the processing of encrypted traffic from servers. Its software is optimized to handle the latest traffic encryption protocols and ciphers, including elliptic-curve cryptography (ECC) and perfect forward secrecy (PFS), and its embedded dedicated hardware is based on the latest industry chipset for processing traffic encryption and decryption. It provides an unmatched price-performance ratio for an application of any size.

Smart Protection from Encrypted Attacks

With approximately 50% of all inbound and outbound traffic being encrypted, SSL-based attacks are on the rise. Radware offers a patent-protected SSL attack mitigation solution, which supports all common versions of SSL and TLS and protects from all types of encrypted attacks, including TCP SYN Floods, SSL Negotiation Floods, HTTPS Floods and encrypted web attacks.

Radware's SSL solution is deployed using Radware-patented SSL protection technology to enable the SSL decryption agent to be deployed out of path and triggered only when suspicious activity starts. The solution mitigates SSL-based attacks using challenge-response mitigation techniques. SSL decryption and challenge-response mechanisms are enforced only against suspicious traffic. The result is the lowest latency SSL mitigation solution in the industry, as legitimate traffic is not affected by the mitigation efforts.

Cloud Migration Made Easy

More financial services are transitioning their applications and services to the cloud and finding themselves operating mixed environments across physical, software-defined and public data centers. Using a single-technology security solution that provides flexible, secure application delivery helps businesses close network management gaps. Radware helps financial services to cost-effectively deliver and scale services while remaining protected with solutions that work seamlessly on or off the cloud.

Flexible, Manageable, Scalable and Secure Application Delivery

Radware's Alteon ADC provides automated application delivery across any digital environment or physical location. Alteon comes with native automation to allow organizations to instantly configure, license and provision new ADC services across multiple environments. Organizations implement new ADC devices where and when they need them using one elastic global license to move ADC services and instances to the cloud (and back) when needed and without investing in separate ADC licenses for each environment.

Radware's Alteon provides out-of-the-box automation for life cycle management of ADC services and integrates them with your organization's network automation systems. It also allows organizations to reuse existing investments in automation across hybrid deployment.

Single-Technology Security Solution

To protect your applications across data centers and cloud environments, Radware offers fully managed, integrated WAF and DDoS protection that is based on a single-technology stack with identical protections at every level. Radware provides full, flexible deployment options with on-premise, cloud (on-demand and always-on) and hybrid deployments, suiting any customer use-case or network topology.

Lack of Resources/Expertise to Manage Complex Protection

Many financial services businesses lack the time, budget, skills and staff to fully leverage their security and application delivery solutions. Working with a security business partner with customized automation and managed security services will help plug the resource gap, boost security and lower overhead. Leverage Radware's team of battle-hardened security experts to help your business meet these demands.

Security Protection Services

ERT Under-Attack Service

ERT Managed Service

Threat Intelligence Subscriptions

ERT Security Update Service

ERT Active Attackers Feed

Radware's Emergency Response Team (ERT) is a group of security experts available 24x7 for proactive security support services for customers facing a broad array of application- and network-layer attacks. The ERT features experienced security engineers for immediate response and escalation, as well as reputable threat researchers, who have brought to market discoveries such as the BrickerBot and JenX IoT botnets. They leverage a global threat-detection network to provide real-time threat intelligence to organizations around the globe.

Radware's ERT provides an extended scope of value-added services, including the industry's fastest SLA for access to a security expert. Radware's ERT also offers a fully managed network and application security service, which includes immediate response, onboarding, consulting, remote management and reporting. Finally, Radware's ERT offers threat intelligence subscriptions designed to provide actionable real-time data for immediate protection against active suspicious attacks and attackers.

Case Studies:

- A Germany-based international financial services corporation suffered a massive SSL-based DDoS attack. Radware was able to successfully provide emergency mitigation by separating the encrypted attack from legitimate traffic, keeping the company in business.

- An EMEA-based multinational bank and leading provider of financial services to organizations throughout the region was experiencing ransom extortion threats and attacks as well as burst and APDoS attacks impacting their business. Radware was selected for its machine-learning capabilities to automatically create attack signatures and security policies. In addition, it was one of the few DDoS mitigation vendors that offered a fully integrated hybrid offering that combines on-premise and cloud-based protection.

- One of the largest U.S. bank holding companies needed visibility to the encrypted traffic handled by its perimeter devices. Radware's simple and consistent solution handled SSL traffic interception of both transparent and explicit security devices.

Summary — What You Should Consider

Financial services organizations face many security challenges. Radware would like to be your business partner to deliver the following benefits:

- Protect your digital business by using an integrated hybrid security solution that uses machine learning to automate threat detection and mitigation
- Keep your customers happy with a fast and safe online experience that is always available and protects their PII
- Protect your organization from data-stealing malware
- Enable your cloud migration by using a solution that enables automated application delivery across any digital environment or physical location
- Manage all of your security solutions easily with a portal that provides full visibility during peacetime and attacks with automated self-service tools

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 on DDoS attack tools, trends and threats.