RADWARE SOLUTIONS FOR FINANCIAL SERVICES PROVIDERS

FINANCIAL SERVICES CONCERNS AND CHALLENGES

Financial services has historically been at the forefront of adapting to changes in technology, regulations and consumer behavior. Business challenges include digital transformation, mobile and cloud adoption, improvements in the quality of the user experience and compliance with evolving regulations and standards. Maintaining service availability and SLAs, keeping PII secure and protecting the organization from sophisticated attacks have become burdens for the IT department because it cannot maintain and develop in-house expertise to keep up with the latest cyberthreats.

Staying Open for Business (Protecting Service and Application Availability)

Customers expect applications and information to be available 24x7. Based on Radware's *2018–2019 Global Application and Network Security Report*, 73% of financial services organizations reported suffering cybersecurity attacks. Survey results show an increase in malware/bot, socially engineered and DDoS attacks. The significant drop in ransom threats is due to the increased focus on cryptomining. Businesses require integrated and automated application and security solutions that ensure business continuity and protection against advanced threats.

Protecting Sensitive Data

Compliance with evolving regulations and standards, such as PCI and GDPR, with requirements for protecting PII, is a constant concern in the financial world. Based on Radware's *2018–2019 Global Application and Network Security Report*, protecting sensitive data is the primary concern of organizations worldwide, with 35% citing data theft as the goal of the cyberattacks they experienced. In addition, although applications are targeted more frequently by application-layer DDoS attacks, 51% of respondents feel they are not prepared to handle these attacks.

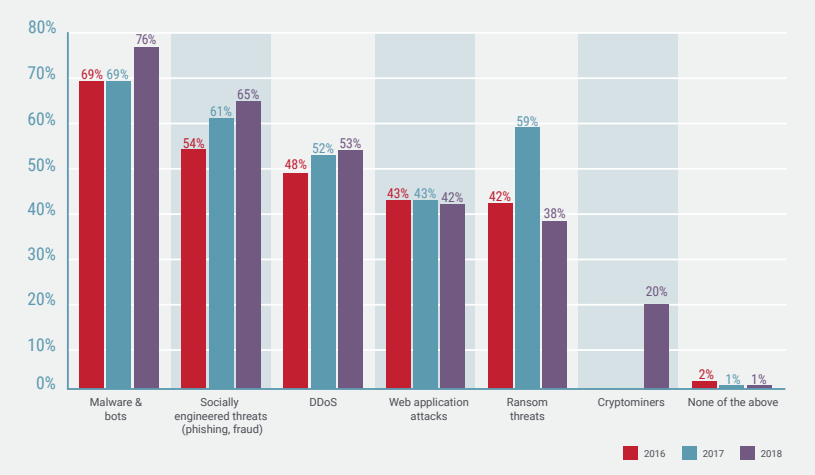

Figure 1. Types of attacks experienced (2016–2018).

Financial e-commerce operations are fertile grounds for malicious bots, including DDoS, account takeover, web scraping and denial of inventory. Bot traffic represents more than half (52%) the amount of internet traffic, exceeding 75% of the total traffic among some organizations based on Radware's *Web Application Security in a Digitally Connected World*. When 33% of businesses cannot make a clear distinction between legitimate and malicious bot traffic, they end up making large investments in additional capacity to accommodate this fictitious traffic, and this expense comes on top of the losses caused by faux buyers.

Cloud Migration

Migration to the cloud helps with cost savings and efficiency but results in multiple environments. Security solutions that use multiple technologies eliminate the ability to automate protection, limit scalability and increase management complexity. Even the most sensitive configurations must be accomplished from afar via remote connections. Putting internal resources in the outside world results in a far larger attack surface with long, undefined boundaries of the security perimeter. In other words, when your inside is out, then your outside is in.

Lack of Resources/Expertise to Manage Complex Protection

Protecting customer data is becoming increasingly complex and challenging. Although keeping websites, data and the network secure is critical, it is becoming increasingly difficult given the cybersecurity skills shortage and the rapidly increasing array of attack vectors. Based on Radware's *2018–2019 Global Application and Network Security Report*, 63% of security teams were exhausted after a 24-hour attack. Nearly one-half of respondents felt ill-prepared to defend against all types of cyberattacks despite having security solutions in place.

Automation can help. Eighty-six percent of businesses have explored machine-learning and artificial intelligence (AI) solutions, with almost half reporting quicker response times to cyberattacks or better security to be the motivation, according to the same report. One-third of respondents also felt that AI solutions would help them reduce costs or gain a competitive advantage.

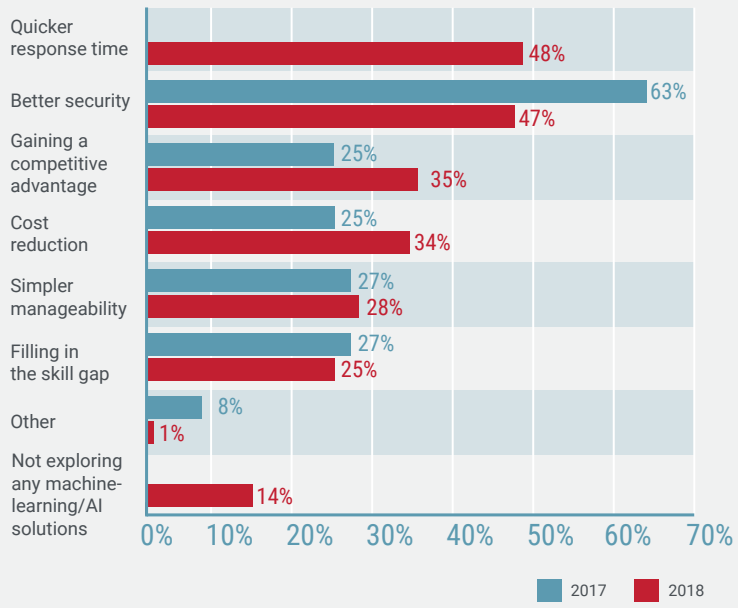

Figure 2: Motivations for exploring machine-learning and AI solutions.

Radware has an array of solutions that allow financial services companies to overcome unique challenges:

- A hybrid DDoS attack mitigation solution that provides the widest security coverage and fastest time to mitigation
- Machine-learning algorithms that ensure the most accurate protection against internet of things (IoT) botnets
- A scalable architecture and automation across heterogeneous environments that ensure business continuity and availability
- Web application firewalls (WAFs) that leverage a positive security model and machine-learning algorithms to provide comprehensive protection against API attacks, IoT botnets, the OWASP Top 10 and other threats
- An SSL attack mitigation solution that protects from all types of encrypted attacks without impacting legitimate traffic
- A fully managed network and application security service that is available 24x7 and provides the industry's fastest SLA (10 minutes) for access to a security expert
- Integrated reporting that includes both on-premise and cloud-based mitigation reporting and analysis

THE SOLUTION

Radware addresses these challenges via a comprehensive suite of application delivery and cyberattack mitigation solutions to protect digital assets hosted across on-premise and cloud-based infrastructures.

In addition, as financial services companies transition services and applications to the cloud, Radware can offer application delivery and business continuity solutions to assist with automation, scalability, availability and disaster recovery.

Staying Open for Business (Protecting Service and Application Availability)

Radware's application delivery and load balancing solutions allow financial services companies to simplify operations while ensuring business continuity and availability. Radware's ADC ensures availability and disaster recovery for local and globally dispersed applications at all times while providing a scalable architecture and automation across heterogeneous environments.

To ensure the availability of applications and make the business resilient to cyberattacks, Radware's Attack Mitigation Solution (AMS) offers a wide range of on-premise and cloud-based security solutions. Radware offers a hybrid attack mitigation service that integrates on-premise detection and mitigation with cloud-based volumetric attack scrubbing. Radware also offers a patent-protected SSL attack mitigation solution that protects from all types of encrypted attacks without impacting legitimate traffic. The solution combines detection and mitigation tools from a single vendor and provides maximum coverage, accurate detection and the fastest time to protection.

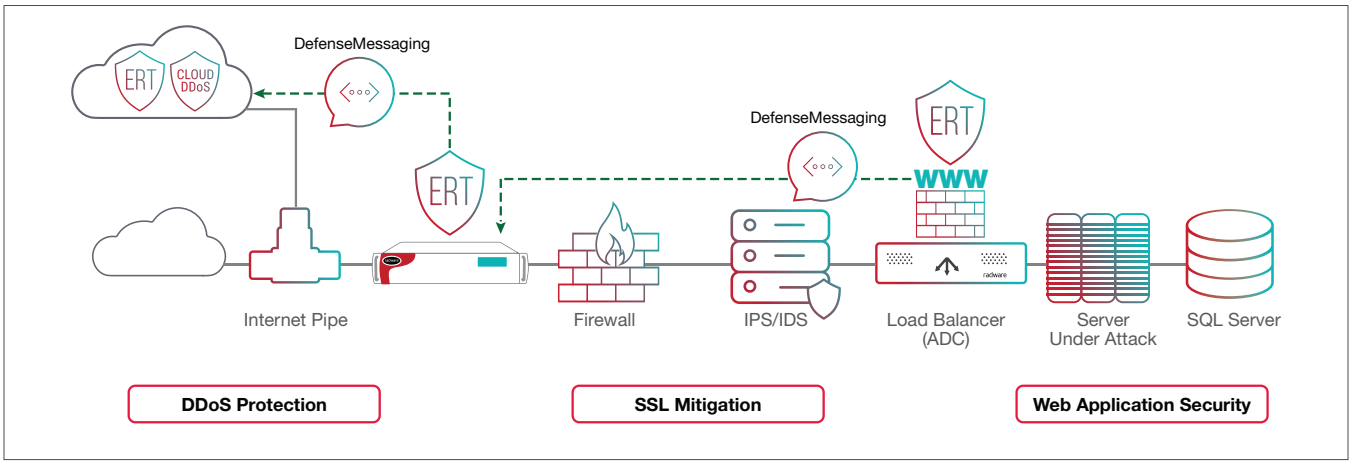

Figure 3: Radware's Attack Mitigation Solution

Protecting Sensitive Data

Financial services organizations are required to comply with a variety of regulations and security standards. Radware solutions and cloud services have the industry's most expansive set of compliance certifications, including PCI, HIPAA, GDPR and advanced ISO regulations, to address data security in the cloud, including application and malware protection and encrypted traffic inspection.

The growth in application-layer attacks underscores the need for fast, reliable and secure delivery of mission-critical web applications and APIs. Radware's WAF solution uses a positive security model and leverages machine-learning algorithms to provide adaptive defense against the OWASP Top 10 and other threats. An auto-policy-generation engine tracks changes to the application and adjusts security policies with minimal human intervention. Radware's WAF technology, which is available as an on-premise appliance (inline or out-of-path) or a cloud service, is recommended by NSS Labs and is ICSA Labs certified and PCI compliant.

In addition, Radware's WAF solution integrates into Radware's Layer 3-7 Attack Mitigation Service and is enhanced by market-leading DDoS protection and bot management solutions. Radware's Bot Manager provides precise bot mitigation and management, combining device fingerprinting, collective bot intelligence and behavioral modeling to protect against account takeover, carding fraud, denial of inventory and other bot attacks on web, mobile and API platforms.

Zero-day malware can bypass legacy malware protection solutions and can exist in a company's network for months before being discovered. Radware's Cloud Malware Protection Service integrates with enterprise web security gateways, IPS/IDS, SIEM or endpoint security to prevent and clean malware from the network. It leverages big data analytics to find new malware and eliminates evasive threats using machine-learning analysis and anomaly detection by studying the malware and the host's communication patterns to block malware activity, prevent data breaches and protect PII.

Finally, financial institutions must protect their hosted services and applications with encrypted traffic inspections. This can be a challenge due to the amount of inbound traffic that is encrypted (as high as 90%) along with new encryption standards, which increase processing loads on the IT infrastructure. Radware offers an industry-leading ADC solution that provides visibility into encrypted traffic and options for offloading its processing.

Cloud Migration Made Easy

As businesses transition their applications and services to the cloud, they have to manage heterogeneous environments that include private and public clouds. Radware helps financial services organizations cost-effectively deliver and scale services while remaining protected with solutions that work seamlessly within cloud, physical or virtual/software-defined environments.

To protect your organization's data centers, Radware offers fully managed, integrated WAF and DDoS protection solutions that leverage identical protection models at every level. Radware provides flexible deployment options for on-premise, cloud (on-demand and always-on) and hybrid deployments to fulfill the network topology of any customer.

To gain control over assets in multiple public cloud environments, Radware's Cloud Workload Protection Service helps customers reduce this attack surface by identifying exposed assets and removing excessive permissions. It detects suspicious activity and prioritizes the highest risks based on context for faster investigation and response. Radware provides smart hardening recommendations, applying the principle of least privileges to fortify the security posture and reduce the attack surface.

Assistance with Managing In-House Resources/Expertise for Comprehensive Protection

Radware builds automation into its solutions to help IT teams manage application delivery and security. Radware's ADC solution configures, licenses and provisions new ADC services and applications across multiple environments. Organizations can implement new ADC devices where they are required and when they are needed, leveraging one flexible license across all environments.

Radware's Attack Mitigation and WAF solutions use machine-based learning, real-time signature creation and auto-policy generation to automate the attack protection life cycle to shorten time to mitigation by automatically mitigating attacks.

Radware's Emergency Response Team (ERT) provides an extended scope of value-added services, including the industry's fastest SLA for access to a security expert: 10 minutes. Radware's ERT offers a fully managed network and application security service 24x7, which includes immediate response, onboarding, consulting, remote management and reporting. Finally, the ERT offers threat intelligence subscriptions designed to provide actionable, real-time data for immediate protection against active suspicious attacks and attackers. Radware's researchers have discovered the BrickerBot and JenX IoT botnets, Stresspaint malware targeting Facebook credentials and more.

SUMMARY—WHAT YOU SHOULD CONSIDER

Financial services companies face many operational and security challenges. Radware has more than 20 years of experience leveraging cybersecurity research to provide technology that solves business and technology challenges. Radware's mission is to help businesses deliver compliant, highly available and secure services and applications against a backdrop of advanced cyberthreats and technological change.

CASE STUDY:

- This multinational banking group was experiencing rapid growth, increased visibility and success. As a result, it became the target of an increasing array of Burst attacks, multivector campaigns and ransom-based attacks. Radware's on-premise DDoS mitigation appliance, DefensePro, was selected for a multitude of reasons in addition to a series of other products and services, including Cloud DDoS Protection Service, DefenseSSL and ERT Active Attackers Feed.

  Radware was selected primarily for its machine-learning capabilities that allow attack signatures to be created automatically. In addition, it was one of the few DDoS mitigation vendors that offered a fully integrated hybrid offering, which combined on-premise and cloud-based protection. Over the past year, this financial services company has successfully maintained 100% business continuity and service availability despite experiencing a four-fold increase in cyberattacks.

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.