Radware Solutions for Financial Services

Financial Services Concerns and Challenges

The financial services industry has historically been at the forefront of adapting to changes in consumer behavior, technology and regulations. Quality of user experience with 24x7 access to online financial services is even more important in a post-pandemic world. Financial business continuity plans did not anticipate this pandemic-driven shift, so new processes and technological measures have been implemented to allow financial service employees to work remotely while securing sensitive data to maintain regulatory compliance.[1] Based on Radware's *2020 C-Suite Perspectives: Accelerated Cloud Migration but Lagging Security*, the majority (58%) of financial service respondents expect 50% or more of their workforce to remain remote during 2021–2022.[2]

While these organizations recognize the advantages of moving to the cloud, they need the expertise of a trusted partner to help them with concerns of availability, visibility, data security and privacy. Due to the increase of online services, remote access and cloud computing adoption, financial organizations have reported a 30% increase in digital theft, according to a Radware's survey of C-suite executives.[3]

Financial services institutions are concerned about their service online availability, protecting sensitive data, migration to the cloud and their lack of expertise and resources to manage cybersecurity protection.

Staying Open for Business

Consumers expect banking and other financial applications to be available 24x7. Due to pandemic-related increases in network and application demand, financial services institutions have added network bandwidth and transit capacity to ensure availability for their clients and employees. However, the finance industry has a history of cyberattacks, especially ransom DDoS (RDDoS) attacks.

FS-ISAC, the financial services global cyber intelligence sharing community, reported in February that more than 100 financial services firms were targets of a wave of distributed denial-of-service (DDoS) extortion attacks. Dozens of institutions were hit within weeks by extortion notes threatening to disrupt the firms' websites and digital services. All types of financial services companies across Europe, North America, Latin America, and Asia Pacific were impacted. This included banks, payroll and payments companies, insurance companies and fin tech companies.[4]

Radware customers were also targeted by DDoS extortionists and required defense against RDDoS attacks. In both attack cases, organizations received a ransom letter, and a few hours later, they were hit by nine hours of DDoS attacks exceeding 200Gbps. If the volumetric DDoS attacks didn't work, the attackers attacked their targets' DNS servers, which can be more vulnerable if hosted by a third party.[5] Financial institutions must ensure their resources are safeguarded and no supporting services, such as DNS servers, can bring down public-facing assets.

1 https://www2.deloitte.com/us/en/insights/economy/covid-19/covid-19-crisis-management-in-financial-services.html

2 Radware 2020 C-Suite Perspectives Report

3 2020 Radware C-Suite Perspectives Report

4 https://www.fsisac.com/newsroom/globalleaders

5 Radware Cybersecurity Alert, Ransom DDoS Campaign: Circling Back, January 22, 2021

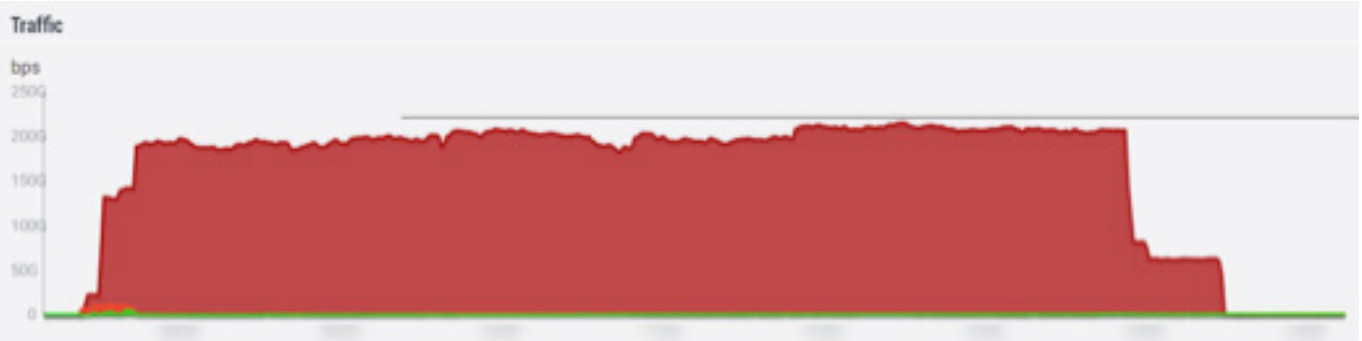

Figure 1. Second RDDoS attack in DDoS extortion campaign.

Radware threat researchers note that RDDoS campaigns, which were traditionally seasonal, have become an integral part of the threat landscape for organizations across most industries. Instead of attacking once, threat actors are circling back to previous targets attempting to obtain additional payments.[6]

Protecting Sensitive Data

The financial services industry is extremely regulated with compliance requirements focusing on the management of risk and fraud. The protection of private data and evolving regulations and standards, such as SOX and GDPR, is a major concern for financial service organizations.[7] Based on Radware's *2019-2020 Global Application and Network Security Report*, protecting sensitive data is the primary concern of financial organizations worldwide, with 30% citing data theft as their highest concern if they are attacked.

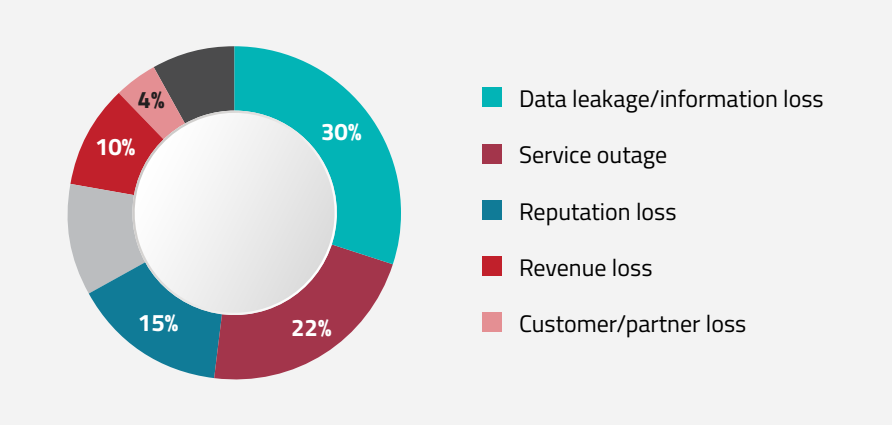

Figure 2. Biggest cybersecurity concerns for financial service companies

Financial applications are fertile grounds for malicious bots, which use attacks including DDoS, account takeover, web scraping and denial of inventory. According to Radware's *The State of Web Application and API report*, 90% of respondents have experienced an application attack.[8] Despite the availability of dedicated solutions to detect and fend-off illegitimate bot activity, only one-quarter of organizations use them. Considered a network-level attack, DDoS is the most common attack vector against applications and is frequently in the form of HTTP/S Floods. Eighty-nine percent of respondents have experienced such an attack that has targeted their web applications, one-third of which occur on a weekly basis.

6 Radware Cybersecurity Alert, Ransom DDoS Campaign: Circling Back, January 22, 2021

7 https://resources.infosecinstitute.com/topic/critical-security-concerns-for-the-financial-services-industry/

8 2020-2021 Radware Research: The State of Web Application and API Protection

Cloud Migration and Multi-Cloud Environments

Financial organizations are shifting application environments, migrating workloads between on-premise, private and public clouds and operating a hybrid application ecosystem spread across multiple environments. About half of the organizations who operate on the public cloud deploy applications on more than one cloud environment.[9] Moreover, many organizations continue to deploy applications either on-premise or on private clouds.

Financial service organizations need to handle the challenges of managing applications across a multi-cloud environment that include protecting applications and network resources against outside malicious traffic, securing remotely managed cloud infrastructure and managing evolving environments.

Improving Delivery of Applications

To create a quality customer experience, financial services organizations must ensure availability, performance and protection of their applications. Managing, scaling and securing applications across private cloud, public cloud and hybrid environments requires multiple tools. Without a single view and management tool for their assets, financial network teams lack visibility into application status, performance and security.

Although encrypted traffic keeps financial transactions more secure, cyberattacks can be hidden if the organization cannot inspect encrypted traffic. To maintain applications' SLAs, financial services organizations need an automated application delivery solution to pinpoint the source of their issues without requiring the expertise of an ADC or security engineer.

Lack of Resources To Manage Protection

Financial services IT teams have limited resources and numerous priorities. Although protecting customer data and keeping their company applications, data and network secure is a priority, IT teams lack the security expertise to defend against advanced cyberattacks. They are overwhelmed by the multiple tools and resources it takes to manage advanced network and security configurations.

FINANCIAL SERVICES CASE STUDY

Liberty is a pan-African financial services company in business for over 60 years. The company's network was being overwhelmed by DDoS attacks, impacting their customer experience and business by taking their customer portal, applications and network offline. The Liberty team assumed their ISP was providing protection but discovered their ISP would not assume that responsibility. Although they increased their network bandwidth, the network outages, some lasting for hours, never went away.

Liberty selected Radware as a vendor partner based on Radware's service strategy driven by research on future threat trends and technology. To protect both of their data centers, Liberty purchased Radware's DefensePro. DefensePro provides premise-based DDoS attack protection using behavioral algorithms to recognize attacks and generate real-time signatures.

The company saw results as soon as they implemented the DefensePros inline, discovering that 40% of their network traffic was malicious traffic, which impacted their network and business performance and caused them to pay more for unnecessary bandwidth capacity.

"When the Radware team turned on traffic inspection based on policies, everything became much cleaner on the routers and traffic was reduced by 40%"

–Preston Soobramoney, Head of Cyber Security

9 Radware State of Web Application and API Protection

Solution Summary - What You Should Consider

Financial services providers can struggle keeping financial data available and secure and ensuring cloud-based applications are protected with limited resources that aren't focused on security. Radware has more than 20 years of experience leveraging cybersecurity research to provide solutions that solve business and technology challenges. Radware solutions have the industry's most expansive set of compliance certifications, including PCI, SOX and GDPR, to address data security in the cloud, including application and malware protection and encrypted traffic inspection.

Radware has also won a number of prestigious analyst awards. For DDoS protection, Radware was named a Leader in the 2021 Forrester Wave™ for DDoS Mitigation Solutions, and a Leader in the 2019 IDC Marketscape for Global DDoS Prevention. For web application protection, Radware was ranked #1 by Gartner in API and High Security (2020), named a Strong Performer by Forrester in the 2020 WAF Wave and was most recently chosen as a Gartner WAF Peer Insights Voice of the Customer, Customers' Choice.

To ensure availability of financial applications and services, Radware offers a behavioral-based hybrid DDoS protection service, which combines on-premise detection and mitigation with cloud-based volumetric attack scrubbing, as well as a fully managed cloud-only attack protection service. It uses machine learning, real-time signature creation and auto-policy generation to shorten time to mitigation. In addition, keyless SSL attack protection defends against encrypted attacks without adding latency and impacting legitimate traffic.

To protect sensitive account data as well as mission-critical financial applications, Radware's web application firewall (WAF) solution, available on-premise or managed in the cloud, uses a positive security model and machine-learning algorithms to provide adaptive defense against the OWASP Top 10 and other threats. Radware's WAF integrates with the hybrid DDoS protection solution and Radware's Bot Manager, which provides precise bot mitigation and management in addition to API protection.

For security and control over assets in multiple public cloud environments, Radware provides 360-degree cloud application protection for the application infrastructure and application surface. Cloud Native Protector provides multi-layered protection for application infrastructure and workloads hosted in public cloud environments to identify exposed assets and remove excessive permissions, detect misconfiguration issues and detect and defend against data breaches. Radware's solutions also protect the application surface against web application attacks (WAF), bad bots (Bot Manager), API abuse (API protection) and Layer 3-7 DDoS attacks (DDoS protection).

Radware's application delivery controller ensures application delivery and disaster recovery for local and globally dispersed financial services applications while providing scalable architecture and automation across public, private and hybrid cloud environments. Radware's ADC also integrates with WAF, Bot Manager and API protection to ensure application availability.

Radware's Emergency Response Team (ERT) offers a fully managed network and application security service 24x7, which includes immediate response, onboarding, consulting, remote management and reporting. The ERT offers threat intelligence subscriptions designed to provide actionable, real-time data for immediate protection against active suspicious attacks and attackers.

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.