radware

OPPORTUNITIES, THREATS AND SECURITY STRATEGIES FOR ONLINE BUSINESS

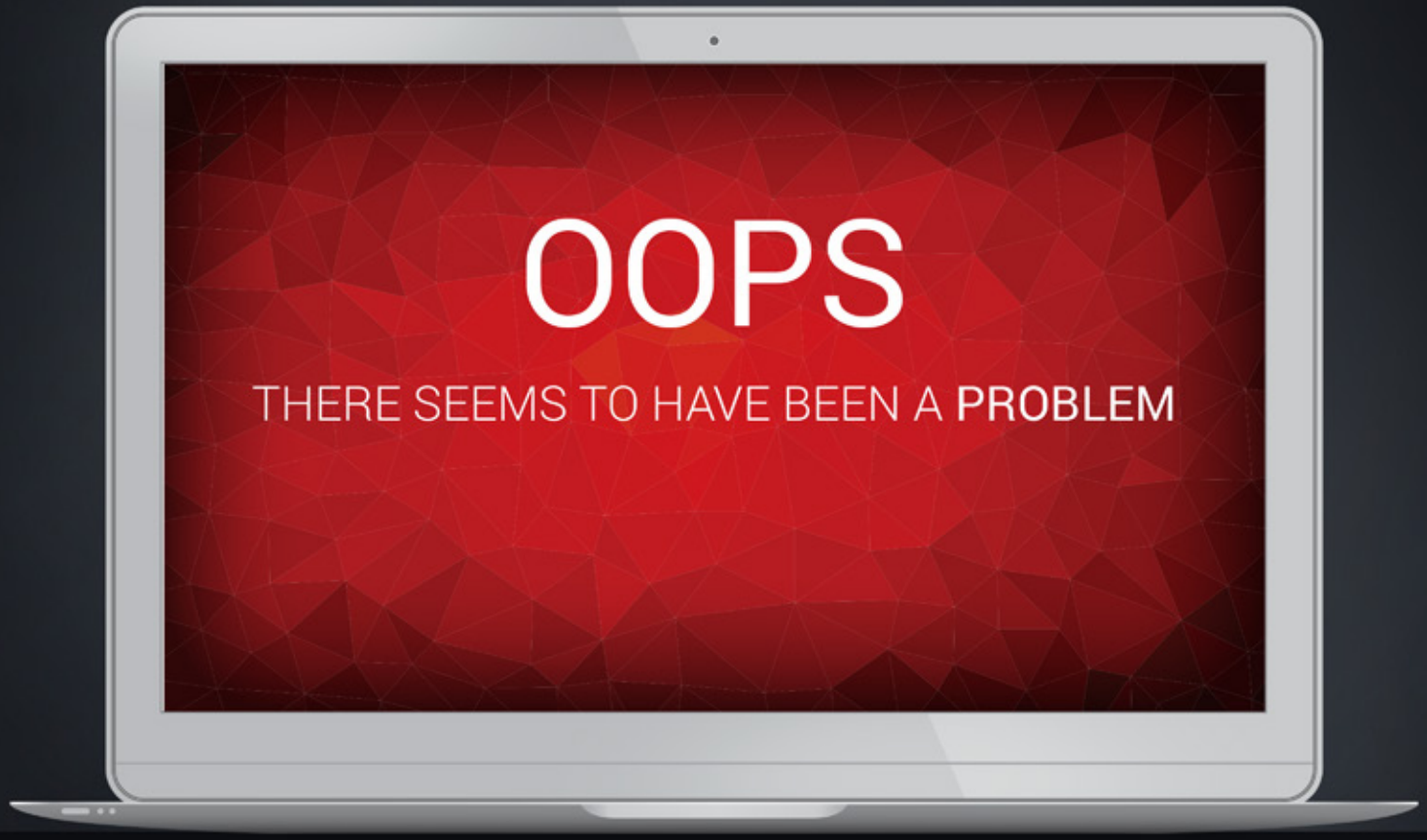


Table of Contents

01

Today, Every Business is an Online Business

Whether you are a Fortune 500 ecommerce company or a mid-sized organization delivering B2B services in a Software-as-a-Service model, one fact is undeniable: you rely on the Internet and many network-based services to operate. You are an online business.

The notion of the 'online business' was born in the mid-to-late 1990's largely as brick-and-mortar stores took to the new platform of the World Wide Web. In 1999, the online sales of products sold through physical stores totaled approximately $20 billion, or nearly two-thirds of all sales on the Web. Yet, a year prior, eBay became an early darling of the financial world when its stock climbed 163% in its first day of trading, largely paving the way for a new wave of ecommerce companies. Today, ecommerce sales in the U.S. alone are over $335 billion, and are projected to increase to $523 billion by 2020[1].

Soon, the notion of the online business would expand to those leveraging the Internet as not just an order taking system, but an actual delivery platform. Application Service Providers (ASP) would emerge and largely evolve into today's Software-as-a-Service. IDC estimates that by 2018, 27.8% of the worldwide enterprise applications market will be SaaS-based, generating $50.8B in revenue.

The motivations for creating new businesses online and shifting existing businesses to online models are clear. According to a recent study[2], companies that support their own online business channels enjoy nearly 20% higher profits than those that do not. In addition, online business models offer greater scale and flexibility to keep pace with shifting demands in products and services.

02

Attackers Know They Can Do Damage

It should come as no surprise that, across the board, there is an increase in the frequency and complexity of cyber security threats targeting online businesses. Each year, Radware compiles its *Global Application & Network Security Report*, which chronicles the changes seen by IT and security professionals to the threat landscape. This report also highlights that those businesses typically thought of in the online business realm (financial services, retail/ecommerce, online gaming, media/entertainment) remain among the most frequently attacked organizations.

The reasons behind the frequency of attacks against these industries is simple...these targets have a lot at risk and also represent large attack surfaces.

As evidence of the increased sophistication of attack, consider that over 50% of attacks Radware mitigates on behalf of customers include more than five attack vectors. Advanced application attacks and “smoke screen” attacks that use DDoS attacks to mask other tactics are becoming commonplace. Attacks leveraging encrypted traffic as an attack vector are on the rise, further challenging many of the cyber security solutions currently in place. Bots, crawlers and spammers crowd web assets, using new techniques to disguise malicious traffic, and zero day attacks swiftly exploit newly-discovered vulnerabilities.

The points of potential target, or ‘attack surface’ of online business also expand and evolve in ways that challenge security teams’ ability to provide protection. Cloud migration and DevOps are IT trends that are creating a proliferation of new applications, code changes to existing applications and hybrid environments hosting applications, all of which create complexity in managing security controls.

03

Impacts of Attack and Outage

Businesses of all sizes across a wide number of verticals now generate significant sales online, increasing their risk and exposure from outages and breach. Unfortunately, malicious actors understand this and target online businesses with this in mind. By and large, their efforts are successful in causing issues. According to the Radware 2015-*2016 Global Application & Network Security Report*, 62% of those attacked suffered downtime or degradation.

According to this same report, organizations now see more tangible financial impact from cyber-attacks. Over two-thirds (69%) of organizations say attacks cause revenue, customer, partner, and productivity loss (up from 45% last year). In our 2014 findings, respondents cited reputation loss and revenue loss as top business concerns vis-à-vis cyberattacks. This illustrates a shift in concerns related to cyber-attacks—that is, worrying less about reputation loss and more about serving customers and ensuring service level agreements (SLAs).

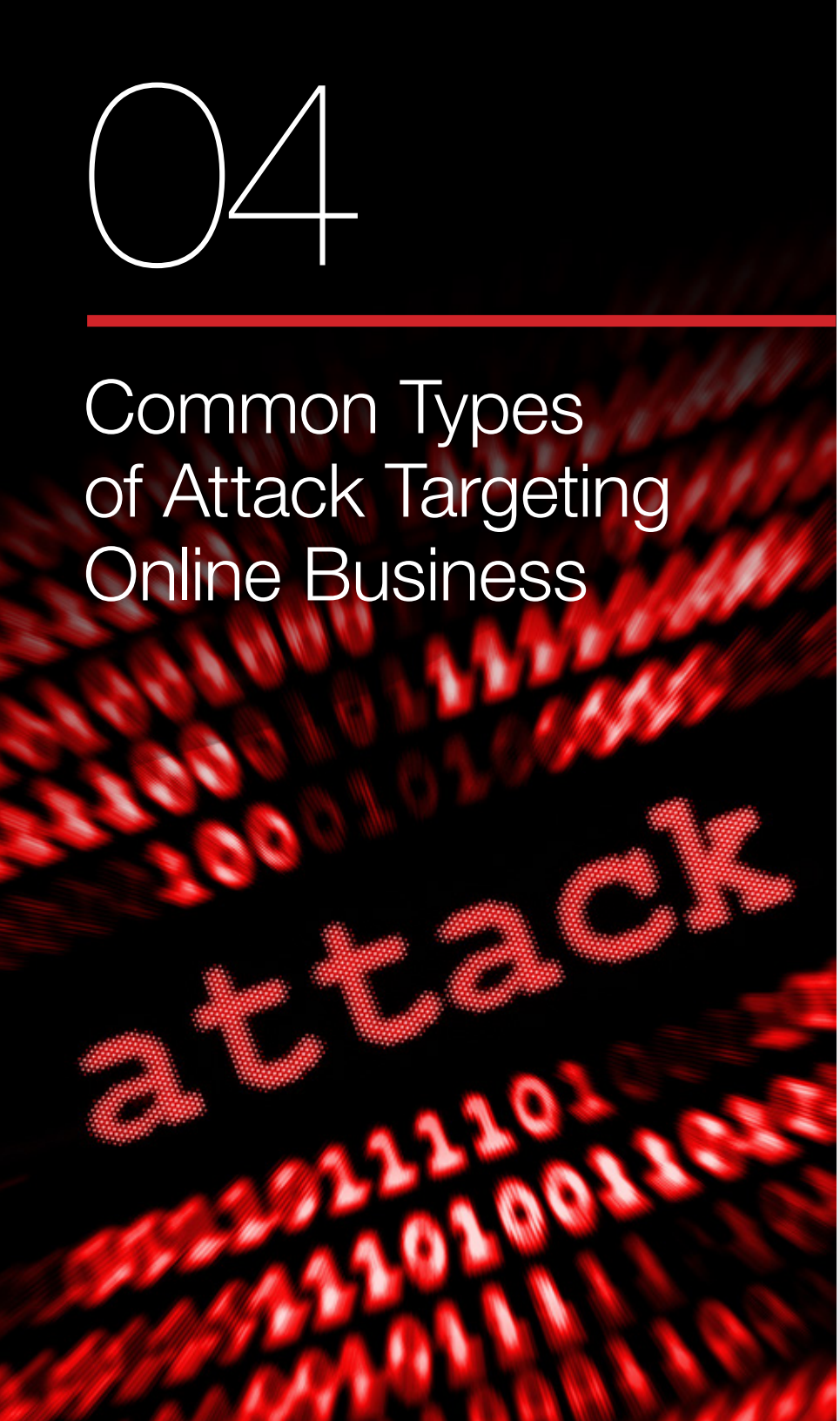
Attacks aren't just about outage or breach. Performance degradation caused by attacks are a growing problem. According to recent studies, 40% of customers now will wait 3 seconds or less before moving on to a competitor site, meaning the impact of performance loss is extremely tangible for online businesses.

According to recent studies, 40% of customers will wait 3 seconds or less before moving on to a competitor site.

As cyber threats continue to grow in size, they not only pose security risks but create unnecessary costs that go into processing unwanted data. Processing bad traffic into data centers or cloud hosting environments can result in significant cost, especially to online businesses with large scale networks. Conversely, dropping malicious activity at the border can avoid these unnecessary operational costs and improve overall operational efficiencies. By building strong security controls at all levels of the infrastructure, security teams can provide tools for infrastructure and operations teams to process only legitimate traffic and also ensure that investments are based solely on business-related traffic.

04

Common Types of Attack Targeting Online Business



In a recent report, Forrester Research[3] highlights four major threats to online business, all of which Radware can address (unplanned downtime, performance issues, transactional fraud, DDoS attacks).

Availability Attacks (including distributed denial of service)

For decades, information security has focused on the 'security triad' of confidentiality, integrity and availability. In many cases, investments in information security have focused much more on the first two of these principles much more than the third. However, as more critical aspects of business operations shift towards online models, availability becomes an equal tenant to the others. Attackers have become adept at exploiting remaining deficiencies however, largely through distributed denial of service (DDoS) attacks. DDoS attacks are consistently among the most frequently experienced attacks.

Transaction Fraud

Online transaction fraud costs an estimated $3.5 billion annually[4]. Much of this activity is attributed to the theft of consumer credit card information breached by application attacks that exploit online business applications. The impacts of transaction fraud also extend beyond the immediate transactions. Consumers consistently say that if their sensitive data is breached, they will likely no longer conduct business with that merchant. A common set of attacks references with regard to transaction fraud are those tracked by the Open Web Application Security Project as part of their OWASP Top 10 list. Among those, SQL Injection consistently ranks as a top threat targeting illegitimate access to applications and backend databases.

Encrypted Attacks

In the same way, SSL and encryption protect the integrity of legitimate communications, they equally effectively obfuscate many attributes of traffic used to determine if it malicious versus legitimate. Identifying attack traffic within encrypted traffic flows is akin to finding a needle in a haystack...in the dark. Most cyber security solutions struggle to identify potentially malicious traffic from encrypted traffic sources and isolate that traffic for further analysis (and potential mitigation).

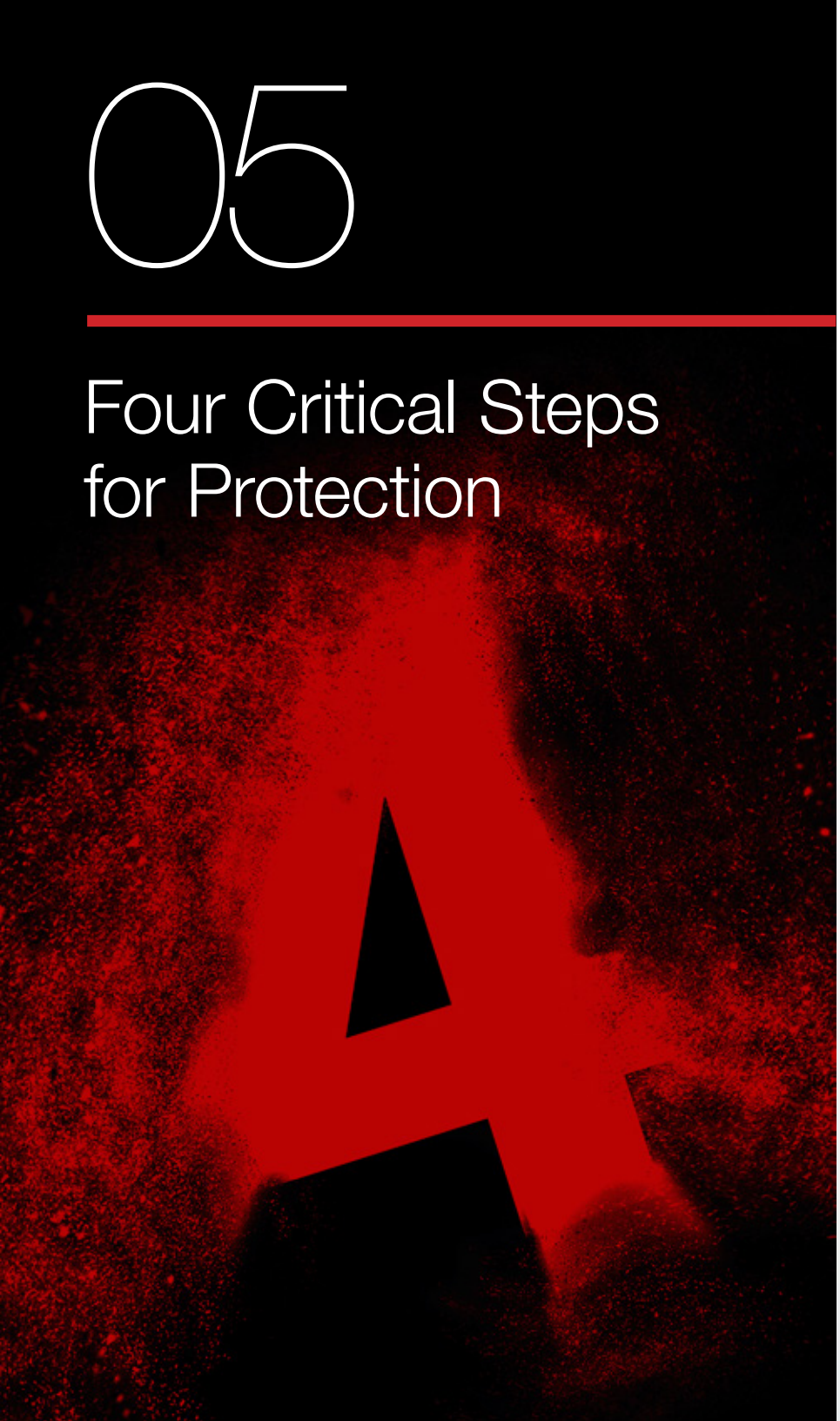
The other major advantage that SSL attacks offer to attackers is the ability to put significant computing stress on network and application infrastructures they target. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic, in many cases beyond the functional performance of devices used for attack mitigation.

Dynamic Content and CDN-based Attacks

As online businesses mature and build global web properties, they often turn to Content Delivery Network (CDN) providers to support site performance. CDNs provide a particularly insidious cover for bad actors as they cannot be blocked by origin servers as accepting transactions and requests from their IPs is the basis for use of their content distribution capabilities. Malicious actors have made an art form out of spoofing IP addresses to not only obfuscate their identity but also to possibly masquerade as seemingly legitimate users based on geolocation or positive reputational information about IP addresses they are able to compromise. Dynamic content attacks further exploit CDN-based protection by overloading origin servers with requests for non-cached content that the CDN nodes simply pass along.

05

Four Critical Steps for Protection



A growing array of threats poses serious risk to data confidentiality, transactional integrity and platform availability. Below are four important steps that can help online businesses focus on the threats most commonly targeting these industries.

Address the Availability Threat

For online businesses, downtime means lost revenue and productivity, making it critical to protect against availability threats, such as DDoS. By and large, there is no longer any debate over the ideal security architecture for providing protection from the wide array of threat vectors related to denial of service attacks. Leading analysts agree that the best solution is hybrid attack protection, a combination of on premise and cloud-based mitigation technology that delivers immediate mitigation of non-volumetric attacks with the availability of additional mitigation resources in the event an attack threatens to saturate the internet pipe of the attack victim.

Guard Against Advanced Bots

Any business that conducts a high volume of online transactions can be a target of bots that exhaust application resources, illegitimately scrape sensitive information from websites and seek vulnerabilities by abusing application logic. To protect applications from advanced bots, operators need more advanced technologies that can track and precisely detect malicious end-user devices regardless of the source IP address. Device fingerprinting generally uses dozens of device characteristics in a unique way to identify

and distinguish it from all others. Using this proprietary tracking, a company can generate device reputational profiles that include historical behavioral information to aid in the detection and mitigation of threats.

Protect Customers from Fraud

Protecting online business platforms from fraudulent activity has short-term and long-term benefits in terms of transactions and customer retention. Since many attacks that lead to transactional fraud target application logic vulnerabilities, advanced web application firewall (WAF) technologies should be a critical part of protection strategies. In looking for a WAF that can address more advanced threats, ensure they provide full protection from the OWASP Top 10 threats, use positive and negative security models to keep up with quickly evolving attacks, and minimize manual policy tuning through automation.

Plan for Migration to the Cloud

If your organization hasn't already started to shift its IT and application environment to the cloud, chances are it soon will. According to recent studies[5], over 88% of enterprises are leveraging public cloud resources. While the benefits are obvious, sometimes the security implications are not. Adoption of cloud (both public and private clouds) creates distributed network and application environments that complicate management and orchestration of security policies. Additionally, reliance on a variety of cloud hosting providers creates inconsistency of levels of security being provided to various applications. By leveraging technologies that deliver coordinated policy management across hybrid environments and establish a strong baseline of protection, organizations can progress down the path of cloud migration without compromising their security posture.

06

About Radware Online Business Protection

To support online business protection, Radware offers a hybrid solution that integrates on premise, real-time attack detection and mitigation with on-demand cloud-based protection to block volumetric attacks. The solution includes all the different technologies needed, including DDoS protection, behavioral analysis, IPS, encrypted attack protection and web application firewall (WAF).

Radware's Online Business Protection solution ensures the integrity and availability of your network-based business by providing protection from today's advanced cyber-security attacks. The solution helps business and IT executives reduce the risk of lost revenue, customer churn, employee and partner productivity by protecting networks and applications from threats to availability and data breach.

To learn more about Radware's solutions for Online Business Protection, visit www.Radware.com.

1 https://www.internetretailer.com/2016/01/29/online-sales-will-reach-523-billion-2020-us
2 http://ecommerce-news.internetretailer.com/retailing/Average-Profit-Margin
3 https://www.forrester.com/report/Seven+Steps+To+Protect+Your+eCommerce+Website+In+2016/-/E-RES128006
4 http://www.pymnts.com/news/2015/2014-fraud-spike-cost-u-s-retailers-32-billion/
5 http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey