Solution Brief

ARBOR NETWORKS
The Security Division of NETSCOUT

RETAIL SUCCESS TODAY IS MORE THAN eCOMMERCE

Expanding customer engagement requires protecting availability

Under the Covers of eCommerce

A Kleiner, Perkins Caufield & Byers's 2017 report shows U.S. ecommerce growth at 15% year-over-year[1]. By 2018 APAC's ecommerce will be $1,892 billion, and represent more than half the global total of $3,015 billion[2]. Global B2B ecommerce is expected to top $6.7 trillion by 2020[3].

Yet in today's highly competitive, digital environment the number one priority is customer engagement. And customer engagement is evolving well beyond the online shopping cart:

- Target plans to have in-store mapping beacons in more than 1,000 of its 1,800 stores
- Fastenal sees double digit growth in sales through its expanding network of over 66,577 of internet-connected vending machines
- Nordstrom has seen 45% YoY growth for its order online, pickup in-store options

There are the mobile innovations: push notifications, real-time parcel tracking, and mobile payment and mPOS options. There are the operational innovations that support better, digital customer engagement. And there are IoT innovations such as RFID merchandise tracking, smart shelves, perishable goods sensors, and more.

What Do These Strategies Have in Common?

They all require network availability and resilience. If your network is down so is your brand, and your connection to the customer.

54%

Of retailers said **the customer experience** is their most important area of focus.

WAY AHEAD OF

16% Cross-Channel Marketing
14% Data-Driven Marketing
11% Mobile
4% Programatic Buying/Optimization

Source: Adobe-eConsultancy study, "2017 Digital Trends in Retail"

Unfortunately, these very innovations can make you more vulnerable to cyber threats, including Distributed Denial of Service (DDoS) and ransomware attacks. Retails' hybrid (on-premise and cloud-based data centers), highly distributed infrastructure already presents a challenging security environment.

BOTTOM LINE: The attack surface is increasing as retailers continue with their digital transformations.

INDUSTRY

Retail

CHALLENGES

- Digital retail has expanded well beyond online purchasing, presenting new opportunities – and security challenges
- IoT-based botnets are increasingly being used to launch large and complex DDoS attacks – and retail organization's eCommerce sites are at risk
- It's not just about lost revenue – highly valuable personal information, service availability and brand are also at risk
- Misconceptions linger as older DDoS protection strategies struggle with increasingly sophisticated network environment and attacks

SOLUTION

- Arbor's intelligently automated combination of in-cloud and on-premises DDoS protection solutions provide the industry's most comprehensive protection from modern day DDoS attacks – so you can maintain service availability
- Leverage Arbor's ATLAS Intelligence Feed to automatically arm all Arbor solutions with global threat intelligence

BENEFITS

- **Reduce costs** associated with network and service downtime caused by DDoS attacks
- **Increase revenue and growth** by protecting availability of network and services from DDoS attacks
- **Gain compliance** by having an automated process in place for availability protection

[1] www.kpcb.com/internet-trends

[2] *e-Commerce Retailers: The Next Billion $ Opportunity, Are We Ready? 2016, Frost & Sullivan White Paper in Collaboration with CDNetworks*

[3] *17 B2B Ecommerce Companies Taking Advantage of a $6.7 Trillion Opportunity (+ How Your Brand Can, Too)*

DDoS Attacks Have Changed: Has Your Protection?

Cyber attackers have taken notice. Concurrent with innovations in digital retail, DDoS attacks have also evolved. Last year 90% of all security incidents in the retail sector involved denial of service (DoS), point-of-sale (POS) or web app attacks[4]. According to another survey report, 73% of retail organizations were hit with a DDoS in 2016, and 83% or those were hit more than one.

The risk equation is changing for retail organizations as some of the growth in frequency, size and complexity of DDoS attacks can be attributed to the weaponization of the Internet of Things (IoT) botnets. The vulnerability of any organization to the modern day DDoS attack was driven home by the Mirai IoT botnet attacks against DNS service provider Dyn when well-known brands such as PayPal, Twitter, GitHub, Amazon, Netflix, and Spotify went down as a result of the attacks and got the media's attention.

Risky Thinking About DDoS Protection

The uncomfortable truth: The modern-day DDoS attack is frequently a dynamic, complex, combination of volumetric, TCP state exhaustion and application layer attack vectors. In Arbor Networks' 13th Annual *Worldwide Infrastructure Security Report* (WISR 2018), 48% of respondents have experienced a multi-vector DDoS attack (20% more than prior year). According to Arbor's WISR 2018, there was a 30% increase in the number of application-layer DDoS attacks. A 'low and slow' application layer attack presents just as much risk as an 800 Gbps volumetric attack.

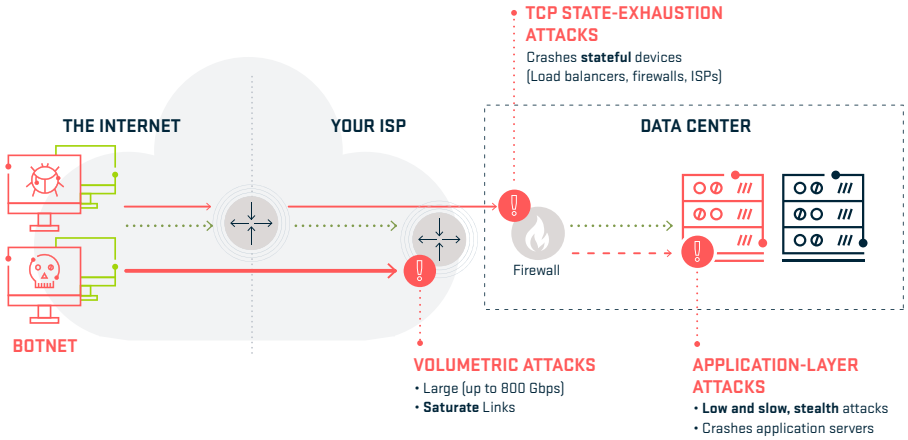

Figure 1 *The modern day DDoS attack is multi-vector*

The dramatic increase in the size, frequency and complexity of DDoS attacks, begs the question: When was the last time you reassessed your risk of a DDoS attack? Common misconceptions about what constitutes effective DDoS protection plague proper risk analysis. For example:

- Firewalls, load balancers, WAFs and IPS are not designed to protect against all DDoS attacks. These stateful devices are themselves vulnerable to TCP state exhaustion DDoS attacks — and routinely fail during attacks. According to Arbor's 13th annual WISR 51% of Enterprises reported their firewalls/IPS failing during a DDoS attack.
- Most on-premises protection can be easily saturated given DDoS attack techniques such as reflection/amplification or IoT botnets for hire. Even though 88% of attacks are less than 2Gbps, these can still overwhelm most retail organization's Internet circuits.
- Cloud-based managed DDoS protection services alone are required to stop large volumetric DDoS attacks — but they struggle to detect smaller, application layer attacks which are just as impactful.
- 74% of attacks last for less than 30 minutes; making automation vital for effective protection.

1 in 3

Retailers have already suffered revenue losses as a result of a cyberattack, and retail organizations perceive targeted attacks as the greatest risk facing their business, according to the Cisco 2017 *Annual Cybersecurity Report*.

52%

Of retail organizations consider their security infrastructure up-to-date and upgraded with the best technology tools (below other industries at 59%).

3 TRENDS SHAPING RETAIL CYBERSECURITY IN 2017, JASON ANKENY, FEB. 13, 2017

THE ARBOR AVAILABILITY PROTECTION SYSTEM (APS)

Provides always on, in-line protection from network and application layer DDoS attacks and advanced threats

Provides in-bound and out-bound threat identification and mitigation

APS mitigation platforms and capacities range from 2U appliances (1 Gbps – 40 Gbps) to virtual machines (sub 100 Mbps)

THE ARBOR CLOUD DDoS PROTECTION SERVICE

Arbor Cloud is a fully managed DDoS protection service providing up to multi-Tbps of global protection

CLOUD SIGNALING

Arbor Cloud Signaling™ provides instant, intelligent communication between on-premise Arbor APS and Arbor Cloud for comprehensive, layered, DDoS protection

[4] *Verizon, 2016 Data Breach Investigations Report Retail*

To add fuel to the fire, the ease with which complex DDoS attacks and weaponized IoT bot-nets can be purchased, or services hired, puts serious attacks within easy reach of virtually any potential adversary.

And lastly, DDoS attacks are frequently used as cover for multi-part, long-running attack campaigns targeting personal information. And when DDoS is used as a diversion for fraud or stealing valuable information, you have a recipe for disaster.

Now is the time for retail organizations to reassess their risk from DDoS attacks and re-evaluate their protection strategies.

Protecting Your Brand and Customer Experience Requires Intelligently Automated, Layered DDoS Protection

To stop today's DDoS attack industry best practices, recommend a layered, automated protection strategy backed by continuous, timely threat intelligence.

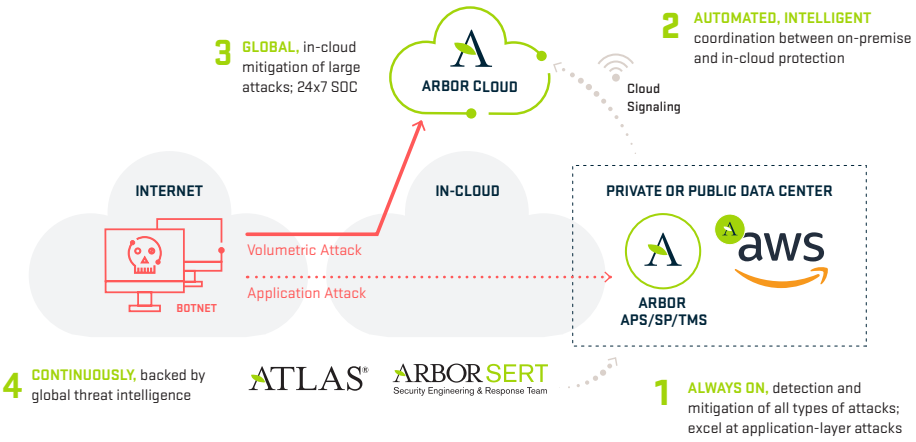

Figure 2 *Unified, intelligently, automated DDoS protection products and services: armed with global visibility and actionable threat intelligence.*

Arbor's DDoS Protection solution offers a fully integrated combination of in-cloud and on-premise DDoS attack protection products and/or services:

Arbor APS

In-line, always-on, installed in private or hosted data centers (e.g. Amazon Web Services), in front of firewalls and key communication gateways; can automatically stop in-bound network, application-layer and TCP-state exhaustion attacks

Cloud Signaling™

Automatically and intelligently link to Arbor Cloud, in-cloud mitigation before on-premise protection and internet circuits are overwhelmed with large attacks

Arbor Cloud

24/7 SOC to automatically mitigate volumetric attacks upstream before on-premises gateways and security systems are overwhelmed

ATLAS Intelligence Feed

Automatically and continuously feed all mitigation options to stay protected from the latest threats (e.g., Mirai botnet derivatives)

"As we progress through 2017, B2B buyers will increasingly expect a more consumer-like experience from the ecommerce systems they interact with – even for the more complex products, digital goods, and subscription-based products."

TOP 5 B2B ECOMMERCE TRENDS OF 2017, PATRICK WOLF, FEB 2, 2017

—

ARBOR ATLAS: GLOBAL VISIBILITY AND THREAT INTELLIGENCE

Over the past 16 years more than 400 ISPs have participated in ATLAS, providing Global Visibility and Threat Intelligence to businesses worldwide.

- Arbor's Security Engineering and Response Team (ASERT) leverages ATLAS to conduct threat research, help customers mitigate DDoS attacks and create ATLAS Intelligence Feeds (AIF).
- AIFs continuously arm all Arbor DDoS protection products and services.

Intelligent Automation is the key to effective protection.

It effects speed of mitigation, to minimize impact on revenue and brand; the efficient use of scarce resources, both investments in technology and talent; and capability to stay up-to-date on the latest threat tactics, techniques and procedures (TTPs).

BOTTOM LINE: Intelligent Automation not only protects you from cost of downtime, but also enables your digital transformation and growth.

Unique, Automated Global Threat Intelligence

DDoS is frequently part of larger attack campaigns that include planning long before a victim is even targeted. A campaign is an ongoing set of operations, much of it automated, against well-researched targets. And adversaries frequently circle back — particularly if they have been successful. The good news is that these TTPs have a history and leave a trail.

For over 16 years Arbor Networks has had unique visibility into global threats. The ATLAS Intelligence Feed (AIF) is built on data from over 400 ISPs providing global threat intelligence. About one third of all Internet traffic flows thru ATLAS or an Arbor product. (A current representation of some of this data came be seen on the Digital Attack Map) ASERT security experts augment this data with additional research and historical perspective, for example, the origins and trajectory of botnet malware to determine the 'reputation' of IPs and DNS.

The AIF continuously arms all Arbor on-premise and cloud-based solutions with actionable threat intelligence. Timely AIF threat intelligence aids more rapid, automatic mitigation of DDoS attacks — yet another example of Intelligent Automation

Quantifying the Risk of Cyber Attacks

There are a number of risk frameworks, from NIST, ISO, CERT, ISACA, and others. While all recognize the business need to asess risk, they for the most part leave quantification up to the organization. What is clear is a compliance based approach to enterprise security is not enough. For example, you could "meet" all the NIST guidelines and still be at significant risk from DDoS or other advanced attacks.

One emerging risk analysis methodology is Factor Analysis of Information Risk (FAIR). FAIR provides for the quantitative measurement, management and communication of information risk in terms of the value to the business. A practical understanding and analysis of information risk in terms of dollars and cents can enable more well-informed business decision making. To see an example of how to conduct a FAIR-based risk analysis of DDoS attack and how different Arbor solutions can reduce the risk refer to the "Additional Resources" in the side bar.

No matter what framework or risk analysis methodology you use, accurate results depend on three things: 1) knowledge of the latest DDoS attacks trends (i.e., size, frequency and complexity); 2) best practices in DDoS defense (i.e., an intelligent combination of in-cloud and on-premise protection backed by continuous threat intelligence) and 3) understanding that not all assets are equal in value and will have a different risk profile.

Summary

Digital retail continues to evolve beyond eCommerce. Successful retail organizations are enhancing the customer experience through multiple digital channels, including in the store. B2B eCommerce is taking note and adopting some similar strategies. Supporting these innova-tions such as mobile and IoT are placing an ever greater burden on security teams.

At the same time they also increase vulnerability. Adversaries have taken note and are evolving their tools, like using IoT based botnets to launch DDoS attacks. The risks and costs of a breach, service unavailability, incident recovery, ransomware and extortion are greater than ever. Now is the time to re-evaluate the risks to your operations and assets.

Arbor's integrated in-cloud and on-premise solutions represent the industry's most comprehensive, effective DDoS protection. Easy to deploy and armed with campaign intelligence from ATLAS, Arbor's complete solution enables you to more efficiently protect your revenue streams, customer relationships — and your brand.

ADDITIONAL RESOURCES

Overview of Arbor DDoS Protection Solution

ATLAS Attack Map

ARBOR NETWORKS

The Security Division of NETSCOUT

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 6664 3140

Latin & Central America
T +52 55 4624 4842

www.arbornetworks.com

SB/RETAIL/EN/0318-LETTER