GDPR HAS CHANGED THE STAKES FOR NETWORK AVAILABILITY

Much of the discussion about GDPR focuses on the sticker shock of potential fines, which are only part of the significant changes this regulation introduces for businesses that collect or process personal data.

Overshadowed by this discussion is a key provision at the heart of GDPR, Article 32, the Security of Processing:

"(b) the ability to ensure the ongoing confidentiality, integrity, ***availability*** *and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;"*

And if the meaning of availability is not clear enough, GDPR Recital 49 specifies that a legitimate interest of the data controller in protecting their networks is "stopping ***'denial of service' attacks*** *and damage to computer and electronic communication systems."*

Avoiding 20,000,000 EUR or 4% of your annual turnover in fines is a surefire motivator. And protecting the availability of your network is part of GDPR. Availability has also become a business imperative — above and beyond regulatory compliance.

Organizations from commercial banks to online gaming, from retail operations to utilities increasingly rely upon the consistent, always on connections to their customers, partners and supply chain. Furthermore, the digital transformation of virtually any business looking to the future is predicated on network availability and reliability.

That availability is under increasing threat from more frequent, larger and more sophisticated distributed denial of service (DDoS) attacks. According to Arbor's 13th Annual *Worldwide Infrastructure Security Report*, the number of attacks increased significantly in 2017. Arbor's ATLAS observed 7.5 million DDoS attacks in 2017 (vs. 6.8 million in 2016). That equates to over twenty thousand DDoS attacks per day or 850 attacks per hour.

Part of this is due to low cost, attack for hire services. In fact, with cheaper services and widely available attack tools, launching a DDoS attack has been democratized. In GDPR-speak, this is significant to controller and processor organizations because it means anyone with an internet connection and a grievance can attack your availability.

ARBOR® NETWORKS

The Security Division of NETSCOUT

Attack size is also a factor. In Arbor Networks' 13th Annual *Worldwide Infrastructure Security Report* (WISR 2018) about one third of respondents reported peak attack sizes over 100 Gbps. The largest attack reported was 600 Gbps. This year, the percentage of attacks over 1 Gbps has increased to 22 percent, growing three years in a row.

To make matters worse, the modern DDoS attack is frequently a sophisticated combination of volumetric, TCP state exhaustion and application-layer attack vectors.

It seems that attackers are realizing that size doesn't matter, but stealth does. According to Arbor's WISR 2018 the percentage of volumetric attacks dropped from 60% in 2016 to 52% in 2017. However low and slow, harder to detect application layer attacks rose from 25% in 2016 to 32% in 2017. The top applications being targeted were HTTP/S, DNS and new comers email and VOIP.

It is a common misconception that devices such as firewalls, WAFs, load balancers, and IPS/IDSs can mitigate DDoS attacks and keep you GDPR compliant. The fact is these stateful devices can become part of the problem. TCP state-exhaustion attacks exploit TCP protocols: SYN, FIN, and RST floods, with much smaller attacks than volumetric but enough to consume the device's available memory. Commonly targeted devices include firewalls, IPSs, load balancers and servers. According to Arbor's WISR 2018 report 52 percent reported their firewalls or IPS/IDS devices experienced or contributed to a network outage during a DDoS attack.

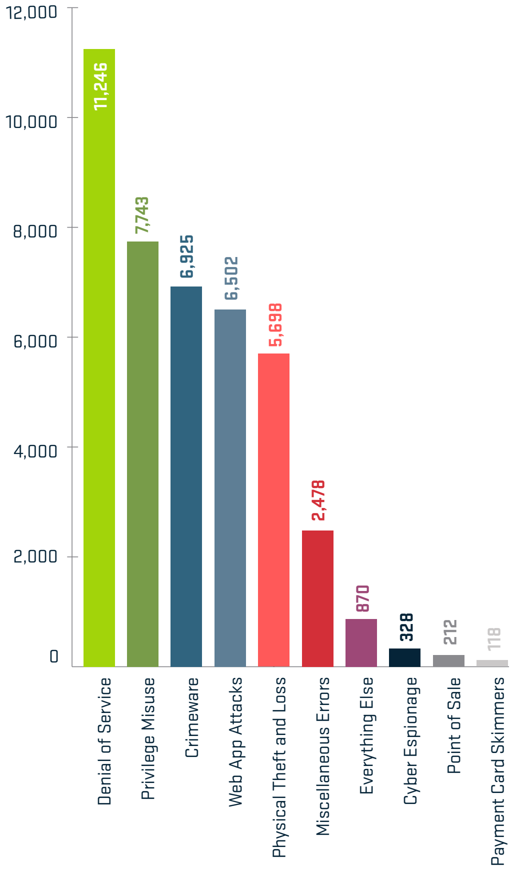
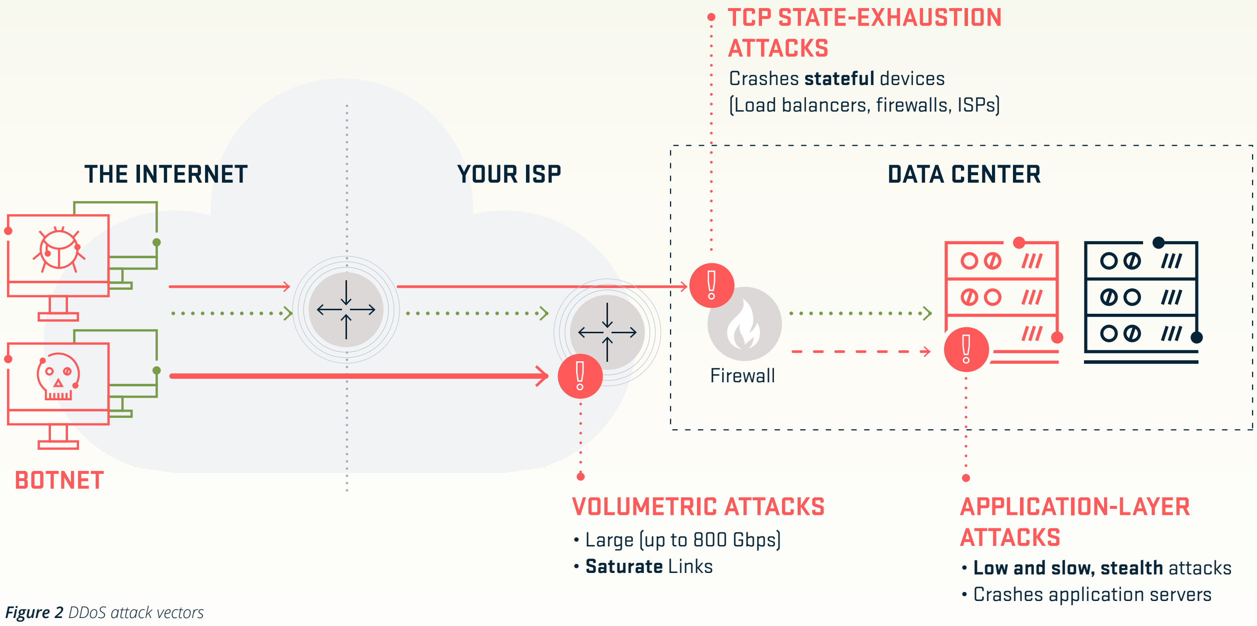
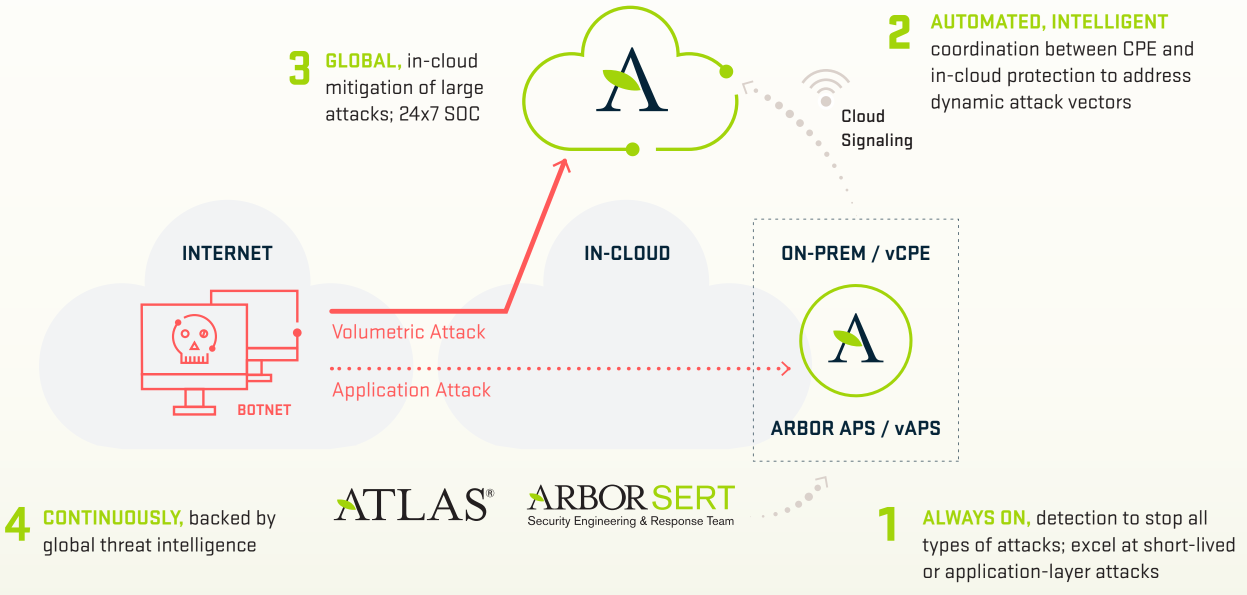


Figure 1 *Percentage and count of incidents per pattern; Source: 2017 Verizon Data Breach and Incident Report*



TCP STATE-EXHAUSTION ATTACKS
Crashes **stateful** devices
(Load balancers, firewalls, ISPs)
THE INTERNET
YOUR ISP
DATA CENTER
Firewall
BOTNET
VOLUMETRIC ATTACKS
• Large (up to 800 Gbps)
• **Saturate** Links
APPLICATION-LAYER ATTACKS
• **Low and slow, stealth** attacks
• Crashes application servers

Figure 2 *DDoS attack vectors*



1 **ALWAYS ON,** detection to stop all types of attacks; excel at short-lived or application-layer attacks

2 **AUTOMATED, INTELLIGENT** coordination between CPE and in-cloud protection to address dynamic attack vectors

3 **GLOBAL,** in-cloud mitigation of large attacks; 24x7 SOC

4 **CONTINUOUSLY,** backed by global threat intelligence

Figure 3 *Arbor Intelligently Automated DDoS protection*

Best Practice DDoS Defense

To stop the modern day DDoS attack consisting of a dynamic combination of volumetric, TCP state exhaustion and application layer attack vectors, industry best practices recommend a layered, intelligently automated protection strategy backed by continuous, timely threat intelligence.

The heart of Arbor's approach to DDoS protection is global threat intelligence. With 400 customers sharing traffic data, we have visibility into approximately 1/3 of all internet traffic.

This gives us a unique position to monitor botnets and IoT compromise activities that drive DDoS attack activity. ATLAS intelligence is derived from the infiltration of these botnets, watching their development, monitoring their C&C infrastructure, malware campaigns, and current vertical and regional targeting.

Arbor's DDoS Protection solution offers an intelligently automated combination of this global threat intelligence with in-cloud and on-premise DDoS attack protection products and/or services:

- Arbor APS to stop in-bound network, application-layer and state exhaustion attacks on-premise, in front of firewalls and key communication gateways.
- Cloud Signaling™ to intelligently link to in-cloud mitigation before on-premise protection and internet circuits are overwhelmed with large attacks.
- Arbor Cloud and 24/7 SOC to mitigate volumetric attacks upstream before on-premises gateways and security systems are overwhelmed.
- ATLAS Intelligence Feed to continuously feed all mitigation options to stay protected from the latest threats. (e.g., Mirai botnet derivatives).

So, with all the attention on protecting personal information, don't forget one of the basics of GDPR compliance: keeping your systems available and resilient. After all, it would be hard to demonstrate compliance — and avoid those fines — if your systems were down.

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