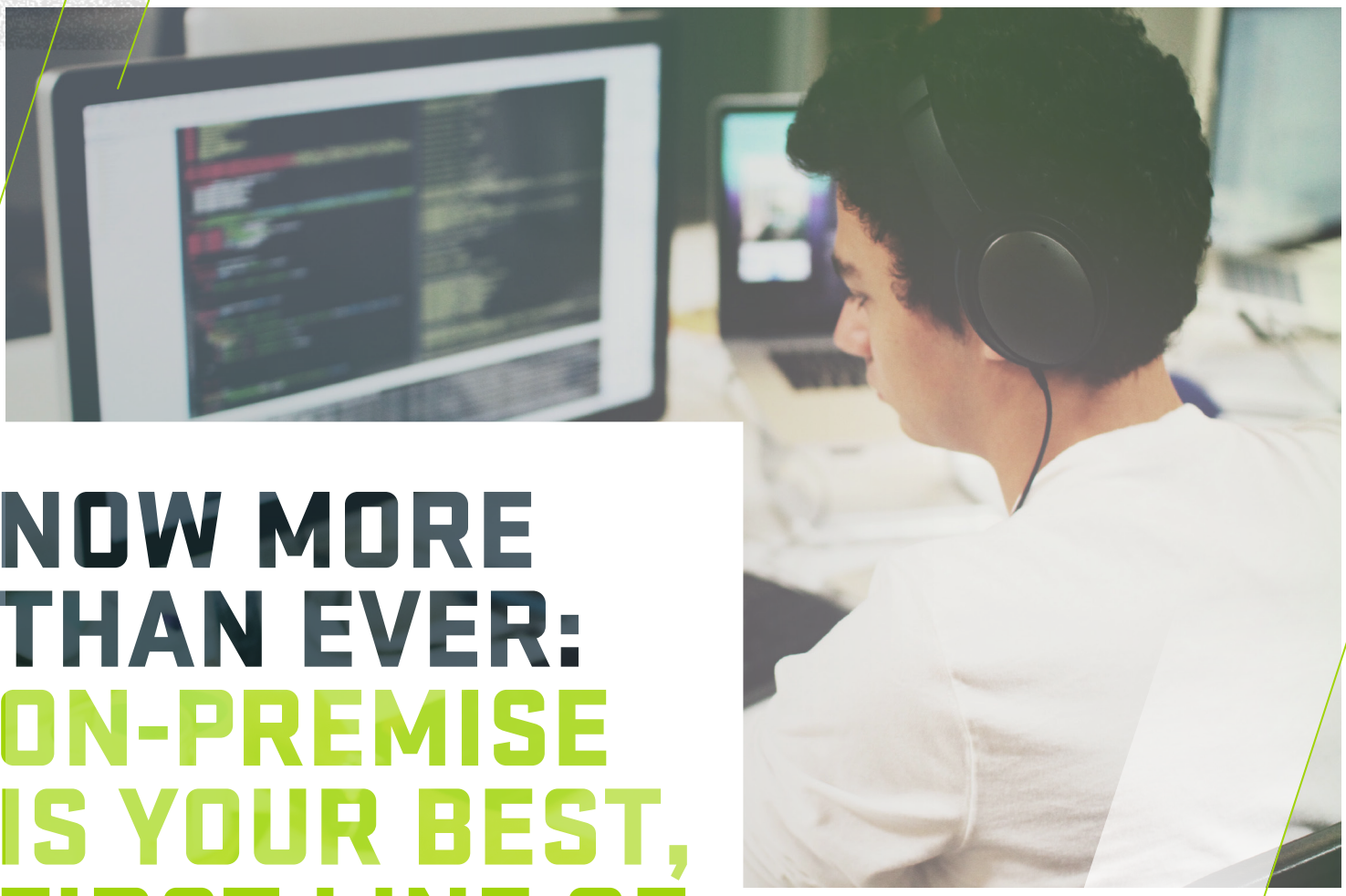

NOW MORE THAN EVER: ON-PREMISE IS YOUR BEST, FIRST LINE OF PROTECTION

Why? Because the business stakes have changed.

In this era of Digital Transformation we tend to think the cloud solves everything. That "on-premise" anything is old-school and part of a fading world of legacy systems. The fact is, in terms of operational control and minimizing time-to-mitigation, nothing beats on-premise DDoS protection. And today, that can be delivered in the form of a traditional appliance, or a virtualized solution.

The cloud has changed the business stakes by enabling SaaS-based applications for customers as well as web-based GUIs for internal users. Online service availability is as fundamental to enterprise success as electricity.

When customer-facing systems are down, revenue streams and brands are put at risk. Aberdeen Group estimates the average cost per hour of downtime across all businesses to be $260,000, a 60% increase over their data from two years earlier. Lack of application availability also disrupts employee productivity and supplier relationships.

As the costs and consequences rise, the threats have also changed. DDoS attacks continue to proliferate. Arbor Networks' Active Threat Level Analysis System (ATLAS), which collects data from more than 300 service provider networks, recorded 6.3 million attacks in 2016, or one every 6.3 seconds.

ARBOR® NETWORKS

The Security Division of NETSCOUT

Here are 3 simple reasons why on-premise protection is the best choice for your first line of DDoS defense.

REASON 1

Despite these headlines, the truth is the vast majority of DDoS attacks are not large.

Eighty per cent are less than 1Gbps. And unlike advanced threats which may dwell insider your networks for weeks, DDoS attacks occur without warning — thus the need for fast, on-premise, automated detection and mitigation.

REASON 2

Application layer attacks are increasingly the bad guys' strategy of choice, typically part of multi-vector campaigns that include volumetric, application and stateful attack components.

According to Arbor Networks' 12th annual *Worldwide Infrastructure Security Report* (WISR) 67% experienced multi-vector attacks and 25% experienced application layer attacks. These are extremely difficult for cloud-based DDoS protection solutions to mitigate. Industry best practices have shown that the best place to stop small, stealthier application-layer attacks is on-premise.

REASON 3

Increased reliance on cloud-based applications and third-party services present bad actors with more opportunities.

You have more threat surfaces to worry about than just your corporate website. Rather than rely solely upon your SaaS provider or ISP for DDoS protection you may need to take matters into your own hands. For example, virtual DDoS protection running in your own cloud environment to protect your critical services.

Perhaps you are thinking you are already covered by your existing on-premise security solutions: firewalls, load balancers, WAFs and IPS. Think again. The increasing sophistication of DDoS attacks makes these stateful devices themselves vulnerable to tactics such as TCP state exhaustion attacks. According to Arbor Networks' 12th annual WISR, 53% of Enterprises reported their firewalls/IPS failing during a DDoS attack.

On-premise protection provides a significant ancillary benefits. First, without sufficient network visibility, enterprises lack the information needed to understand whether poor service or application performance is a result of DDoS attack traffic, or a network misconfiguration. On-premise solutions provide the critical traffic visibility needed to quickly diagnose the issue, saving IT and network teams valuable time while improving performance.

Greater visibility on-premise is also essential to understanding when a DDoS attack is being used as a distraction as part of a targeted attack looking to exfiltrate data. Besides providing the best first line of defense, on-premise solutions can monitor both in-bound and out-bound network traffic to discover anomalies that indicate attacker reconnaissance activity, malware movement, and botnet command and control activity.

Wondering how prepared you are in the fight against DDoS?

Take this quick assessment. Then take a look at how on-premise solutions can keep you in control of your service availability and performance.

Learn more on Arbor's industry-leading portfolio of DDoS protection solutions.

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

AI/OPPROTECT/EN/0617-LETTER