2019

Full Year DDoS Trends Report

corero

JUNIPER
NETWORKS

Table of Contents

2019 Full Year DDoS Trends Report

Executive Summary

INTRODUCTION

Organizations across the globe remain dependent on the Internet as a means to conduct business and deliver their services to other businesses and consumers alike.

This increasingly Internet-connected world grows more complex every year due to faster connections, the widespread adoption of Internet of Things (IoT) devices, and cloud services. Simultaneously, Distributed Denial of Service (DDoS) threats have become more sophisticated, frequent, and larger. Whilst unlawful in many countries, DDoS-for-hire services are commonplace and inexpensive.

Internet resilience can come down to a fraction of a second. When the Internet goes down, organizations that rely on that service go down with it. DDoS attacks are considered one of the most serious threats to Internet availability today. Downtime or latency can significantly impact brand reputation, customer trust and revenue. Within Europe, the introduction of the GDPR and NIS legislation has significantly increased the risk of punitive fines.

This report contains observations from DDoS attacks against Corero customers in 2019, as well as comparisons against previous years.

Key Trends

HIGHLIGHTS

Average number of attacks per customer per day remains steady year over year

Trend is shifting from smaller, sub 1Gbps attacks to larger 1Gbps-5Gbps attacks

Number of attacks over 10Gbps has increased by 35%

Continued trend toward attacks of less than 10 minutes

Approximately 1 in 4 victims of DDoS are attacked again within 24 hours

Continued increase in the use of multi-vector attacks

Other notable events within the reporting period include:

- In January of 2019 there was a report of a SYN DDoS attack which resulted in an overwhelming deluge of 500 million packets per second.
- National intelligence and law enforcement agencies took proactive, well publicized measures to take down DDoS-for-hire services.
- Governments became increasingly vocal about Nation State sponsored cyber-attacks and the threat these pose to critical national infrastructure.

Attacks Per Customer Remain Steady

KEY TREND

In today's "always-on" world, customers expect constant service availability in order to conduct their day to day business activities, or to simply communicate with colleagues and customers around the globe. Any downtime can be more than just an inconvenience. In some industries, such as financial trading, even seconds of downtime are incredibly disruptive and damaging. Even 0.01% downtime can dramatically affect a business' bottom line, as this equates to almost an hour of downtime over the course of a year.

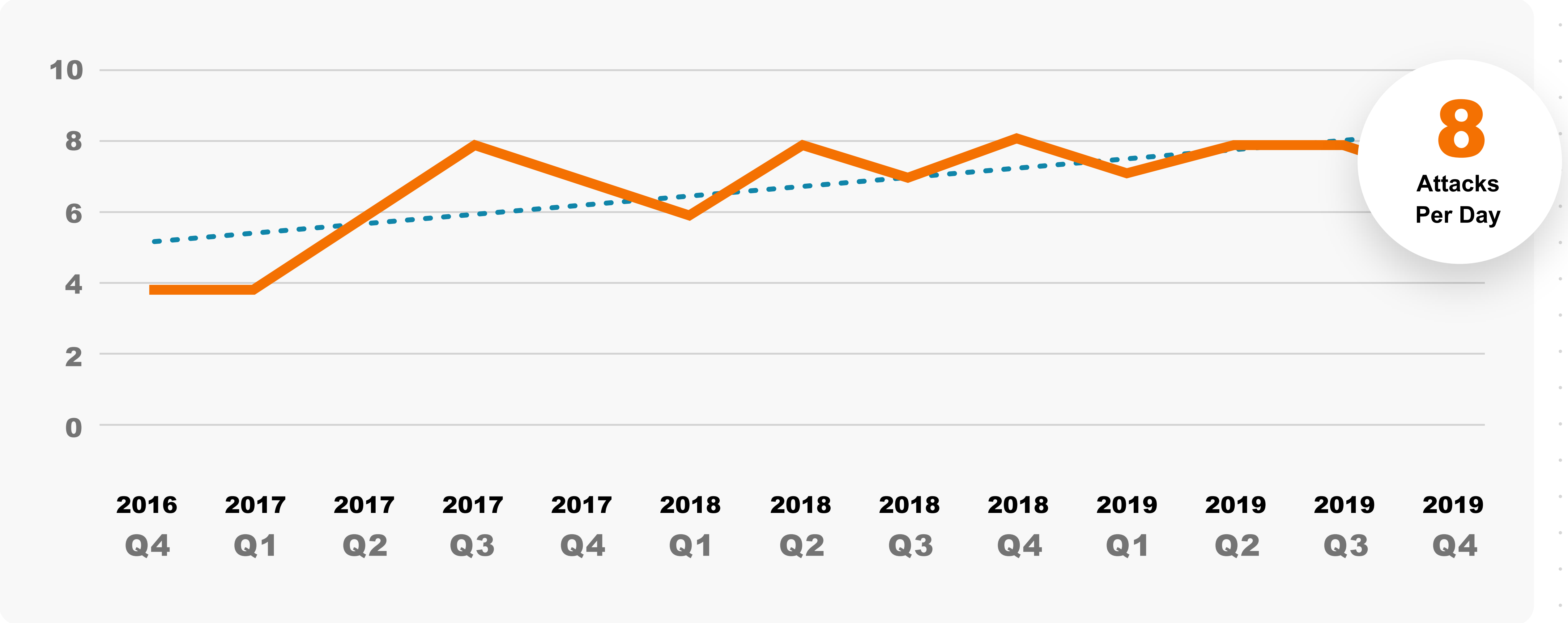
Frequent, modest-sized, short duration attacks continue to be the most common DDoS problem, as they are able to cause damage to more victims. It is these types of attacks that your organization is more likely to encounter.

Corero has observed the frequency of attack attempts against our customers holding steady over the past 24 months. The average customer is attacked approximately 8 times per day.

AVERAGE ATTACKS PER CUSTOMER (DAILY)

Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018	Q2 2018	Q3 2018	Q4 2018	Q1 2019	Q2 2019	Q3 2019	Q4 2019
4	4	6	8	7	6	8	7	8	7	8	8	7

> "We've seen daily attacks continue at a significant rate"



Continued Increase in DDoS Attacks Over 10Gbps

KEY TREND

The continuing trend is that the average size of attacks is increasing. There is a trend shifting from smaller sub 1Gbps attacks to larger 1Gbps-5Gbps attacks as a percentage of all attacks during 2019.

There is a measurable increase of 35% in the ratio of attacks over 10Gbps in 2019 compared to 2018 levels. This trend continues and is around double the 2016 levels.

> "We have seen a 35% increase in attacks greater than 10Gbps over the past year."

35%

Increase in DDoS Attacks Over 10Gbps

Average Size of DDoS

Size	2017	2018	2019
< 1Gbps	82%	82%	75%
1Gbps - 5Gbps	14%	13%	17%
5Gbps - 10Gbps	3%	3%	3%
> 10Gbps	1.5%	1.7%	2.3%

85%

Attacks Lasted Less Than 10 Minutes

Average Duration of DDoS Attacks

Minutes	2015	2016	2017	2018	2019
0 - 5	63%	54%	58%	65%	67%
6 - 10	17%	18%	13%	16%	18%
11 - 20	7%	8%	10%	8%	6%
21 - 30	8%	11%	7%	3%	2%
31 - 60	3%	4%	6%	4%	3%
> 60	2%	5%	6%	4%	3%

Short Duration, <10Gbps Attacks Continue to Dominate

KEY TREND

While the frequency has remained consistent, the size and duration of attacks remains the primary factor in organizations needing a DDoS Protection solution. As previously reported, the vast majority (98%) of mitigated DDoS attacks were less than 10Gbps in volume.

The continuing trend is for short attacks. In 2019, 85% of attacks lasted less than 10 minutes; up from 81% in 2018.

The long-term trend of a reduction in the percentage of attacks over 20 minutes continues with a further decline in average duration. In 2019, only 8% of attacks lasted longer than 20 minutes; down from 11% in 2018.

In summary, attacks below 10Gbps and short duration attacks continue to dominate with these attacks trending larger and shorter to evade traditional protection methods.

Probability of Repeat Attacks

KEY TREND

We continue to report the significant chance of repeat attacks.

There is a continuing trend that organizations have approximately a 1 in 4 chance of being attacked again within 24 hours.

During the remainder of the 90-day period, the probability of follow-up attacks rises to 1 in 3 (36%). We have excluded so-called “saw tooth” or “pulse” attacks from this data, which are characterized by attacks which switch-on for, say, 5 minutes and then reappear several minutes later in a similar or mutated form. Corero counts these as a single attack scenario that has presumably been designed to evade traditional redirection to scrubbing center defenses and/or to allow DDoS-for-Hire services to multiplex their attack resources between different victims and support more dark web customers paying for DDoS attacks.

> **“Organizations have a 1 in 4 chance of being attacked again within 24 hours”**

Probability of Repeat DDoS Attacks by Elapsed Time

Days	Q1 2018	Q2 2018	Q3 2018	Q4 2018	Q1 2019	Q2 2019	Q3 2019	Q4 2019
< 1	20%	21%	22%	23%	23%	21%	24%	23%
2 - 7	7%	7%	7%	6%	6%	6%	5%	5%
8 - 30	6%	6%	5%	5%	5%	5%	5%	5%
31 - 90	3%	3%	2%	2%	2%	2%	2%	3%

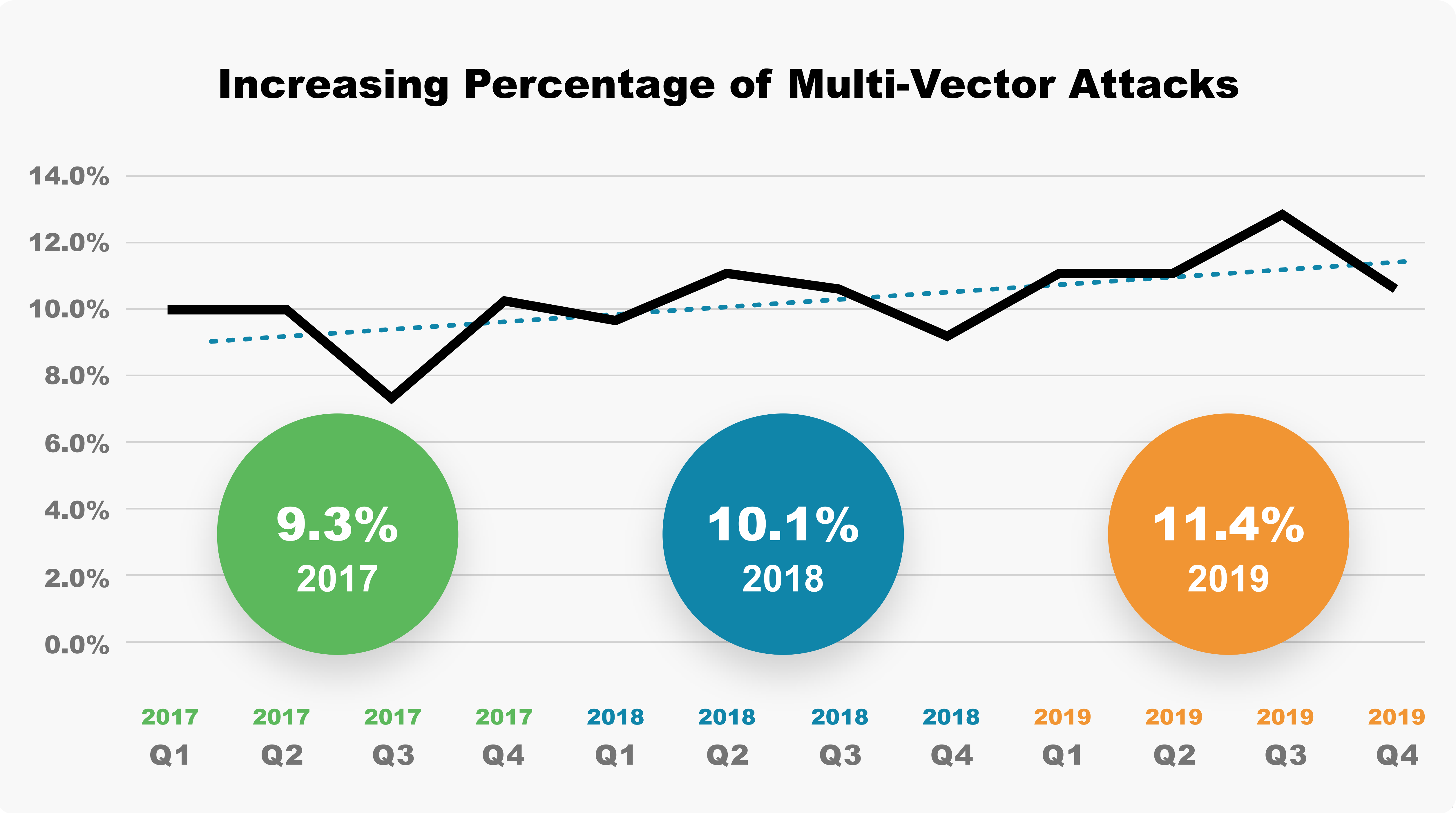
Increase in the Use of Multi-Vector Attacks

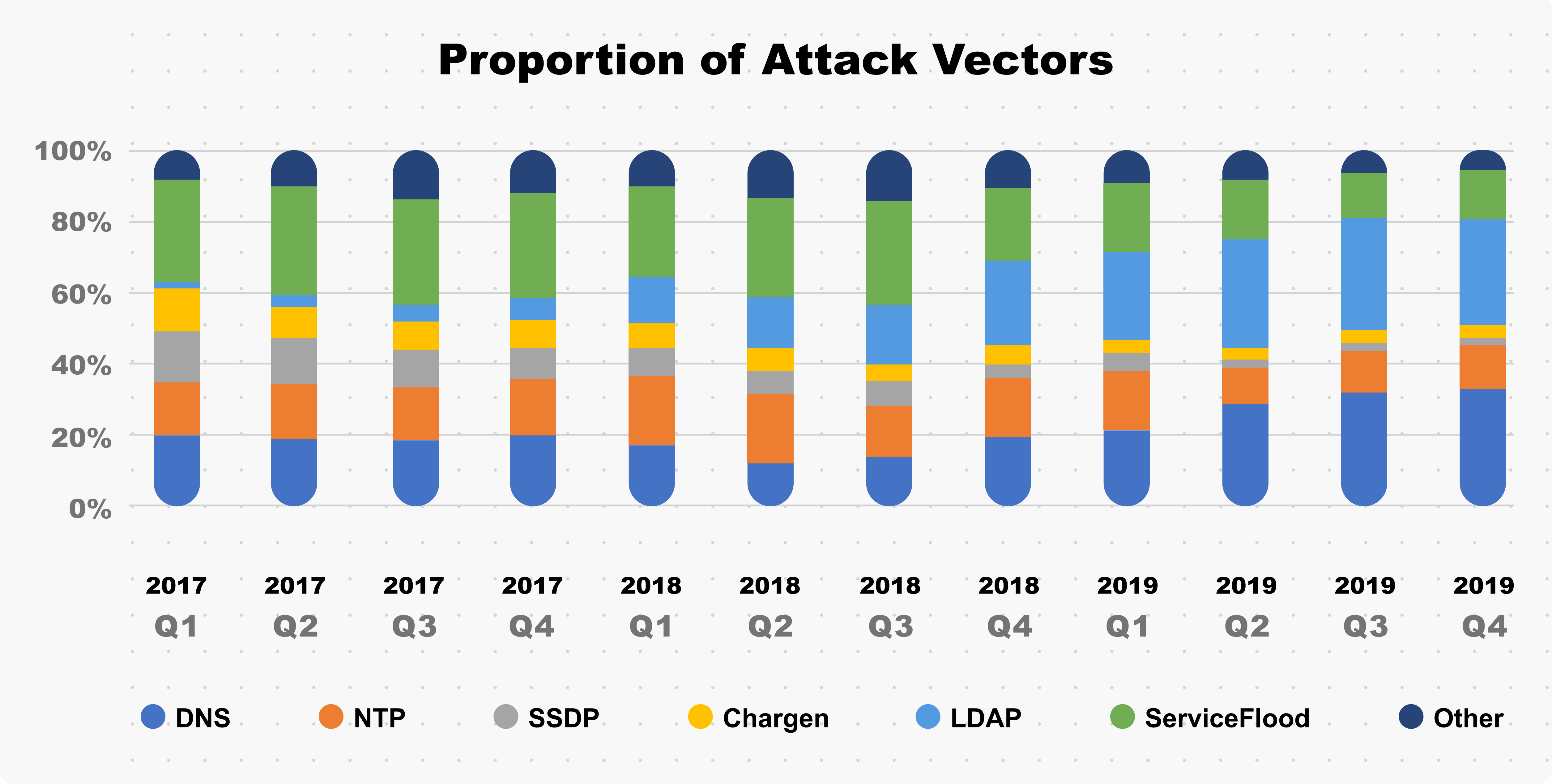
KEY INSIGHT 1

Multi-Vector vs. Single-Vector Attacks

We continue to see a gradual increase in the use of multi-vector attacks. In particular, the DNS and CLDAP vectors continue to dominate. During the reporting period we observed an 13% increase in the use of multi-vector attacks. Attacks present a significant challenge for both manual and legacy detection and mitigation solutions for the following reasons:

- For complete mitigation it is necessary to recognize each and every vector and respond with the appropriate mitigation without impacting legitimate traffic.
- Multi-vector attack rates are usually additive in terms of bandwidth and packet rate. The total attack rate will be the sum of vector1 + vector2 + vector3, etc.
- Multi-vector attacks often exhibit more variability in rate as different vectors join and leave. This presents challenges for many traditional detect and redirect DDoS solutions that typically provide partial mitigation capacity. Making a decision on the mitigation method (e.g. redirection vs. blackhole) based on the current attack rate is flawed as it can vary on a minute by minute basis.
- The most common contributors to multi-vector attacks continue to be volumetric UDP amplification vectors including DNS, CLDAP, NTP, Chargen, and SSDP.
- Attackers frequently mix resource exhausting TCP SYN floods from spoofed sources to make tracking and mitigation more challenging.
- These vectors and other variants may be added or removed multiple times during a typical 10 minute attack period. The aggregate attack amplitude often varies up to 10X during the attack as vectors surge and fade.





> “If you are attacked, there is a 23% chance the same IP address will be attacked again in the next 24 hours."

Traditional Detect, Redirect, Mitigate Solutions May Be Ineffective

KEY INSIGHT 2

DDoS attacks target victims for various reasons. Whatever the motivation, current data suggests that there is a 23% chance of a repeat attack to the same victim within 24 hours and a 36% chance of a repeat attack within 90 days.

When combined with the data indicating that the majority of attacks are also less than 10 minutes, these findings call into question the efficacy of traditional detect, redirect and mitigate solutions that may need up to ten minutes or more to initiate mitigation.

Clearly for the vast majority of the attacks described in this report this would be ineffective. The only way to avoid repeat outages as a result of these repeat attacks is to deploy active real-time protection against DDoS that can detect and mitigate in seconds or less.

Majority of DDoS Attacks Do Not Saturate Uplinks

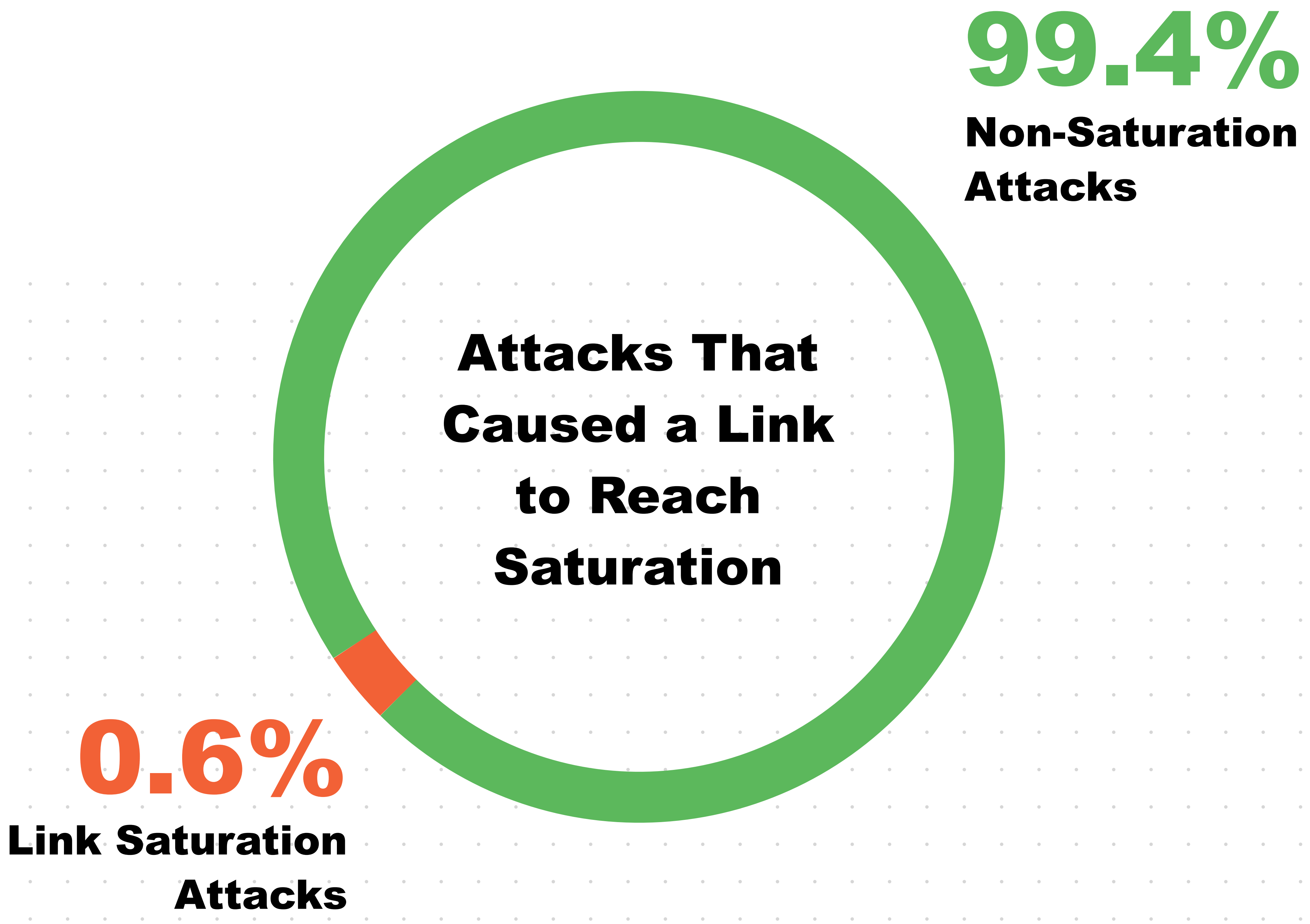
KEY INSIGHT 3

A new insight for this report is the tracking of link saturation by DDoS attacks. Corero analyzed hundreds of thousands of attacks during the period and found that less than 0.6% resulted in one 10Gbps link being saturated, which is judged as more than 95% utilization, also known as “full pipe”.

99.4% of attacks do not reach 95% link saturation levels.

Furthermore, of those 0.6% of attacks that caused a link to reach saturation of 95% utilization, the large majority (>95%) of those saturated attacks lasted less than 10 minutes.

> “Over 99% of attacks do not reach 95% link saturation levels."



Recommendation 1

Understand the Evolving Threat Landscape

The DDoS threat landscape continues to evolve just as it has for the last couple of decades. **We continue to see an increase in attack attempts against our customers year over year.**

The sophistication of DDoS also continues to develop, with multi-vector attacks being used more frequently each year. These attacks often present a more challenging detection and mitigation task due to their varying amplitude, ports and protocols.

The average attack is short with the majority now lasting less than 10 minutes. Real-time detection and mitigation are an essential requirement to provide comprehensive protection.

With the increased number and average size of DDoS attacks we're seeing, even if it's targeted to another customer of your service or hosting provider, you may still be impacted without the latest generation of "always on "protection.

> "The sophistication of DDoS attacks continues to develop, with multi-vector attacks being used more frequently in the past year."

Recommendation 2

Talk DDoS with Your ISP

Organizations that once had DDoS protection projects on the back burner are now re-prioritizing their security strategies to place DDoS mitigation at the forefront.

This shift in precedence means that Internet and Cloud Providers are increasingly enabling this protection for their customers to eliminate DDoS threats closer to the source. As a result, providers are now also accepting a greater responsibility for defending their customers and networks against DDoS attacks.

This approach allows for new security service offerings that protect and increase customer satisfaction.

There are various ways to protect your network from attacks, so an organization must weigh the advantages and disadvantages of each defense method, according to its needs, risks, and budget. In short, an organization has three options; a completely on-premises solution, a cloud-based mitigation service, or a hybrid combination of on-premies with cloud scrubbing for attacks that exceed link capacity.

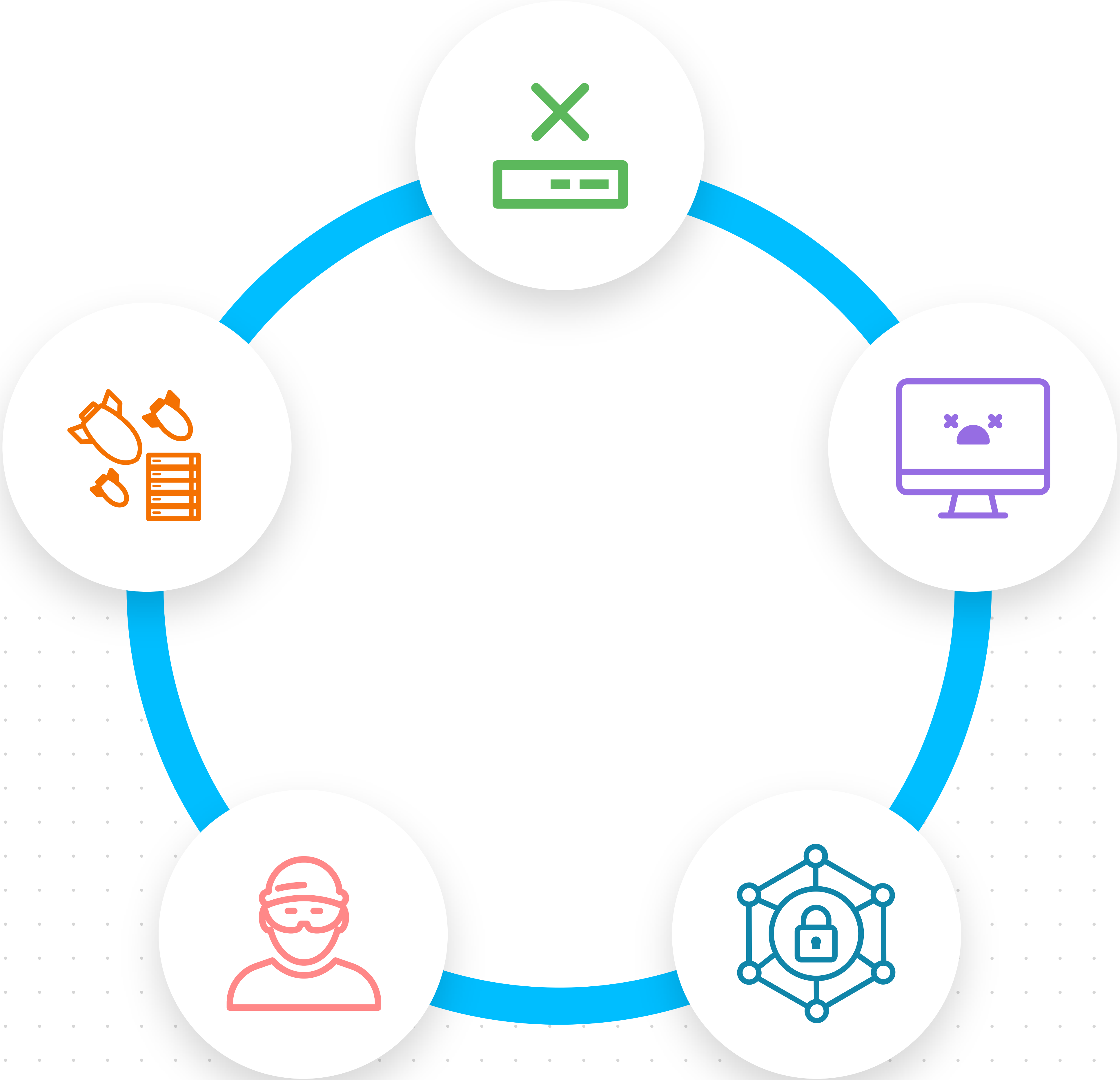
Recommendation 3

Enable Real-Time Threat Protection

To keep up with the growing sophistication of well-equipped and well-funded threat actors, it's essential that organizations maintain comprehensive visibility and automated mitigation capabilities across their networks in order to instantly detect and block any potential DDoS attacks as they arise.

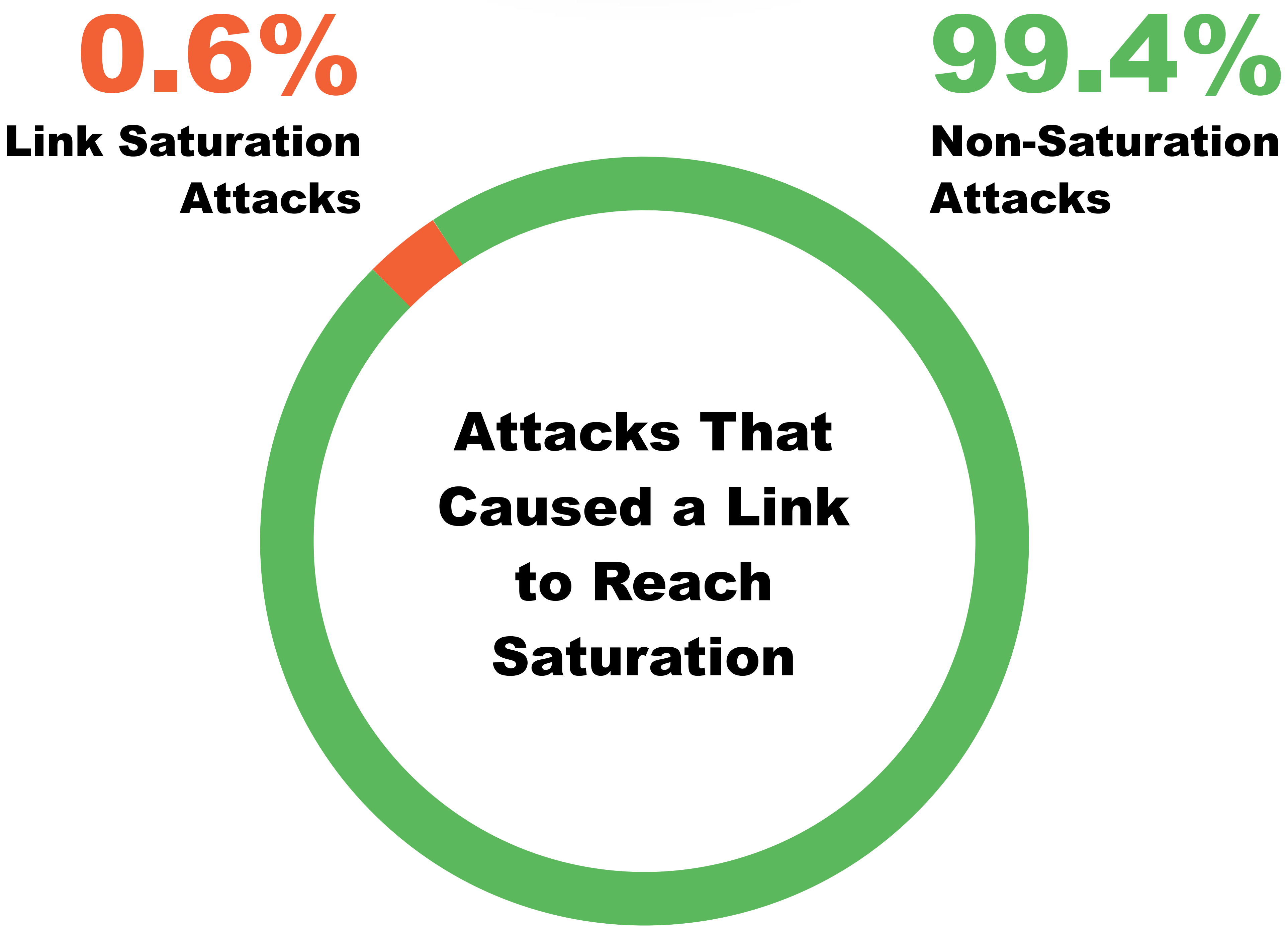
Proactive DDoS protection is a critical element in proper cyber security to protect against loss of service availability and data breach activity. The everyday DDoS attacks that we have highlighted in this report cannot be properly defeated with traditional Internet gateway security solutions such as firewalls, Intrusion Prevention Systems and the like. Similarly, cloud-based DDoS scrubbing alternatives cannot achieve successful mitigation of the frequent, short duration attacks that are impacting organizations every day.

As organizations develop their DDoS resiliency plans and choose their methods of DDoS protection, time-to-mitigation is a critical factor to consider.



85%

Attacks Lasted Less Than 10 Minutes



Recommendation 4

Consider Hybrid DDoS Protection

Depending on your risk tolerance in regard to business continuity, you should consider enhancing existing Cloud-based DDoS protection with on-premises DDoS detection and mitigation to create a hybrid solution. This hybrid solution will handle the majority of attacks in real time without swinging attack traffic to the cloud.

Cloud-based mitigation is necessary to defend against DDoS attacks that are larger than your internet bandwidth—the kind that result in the infamously huge, overwhelming, floods of traffic to an unsuspecting organization. However, on-demand cloud mitigation is not, and can never be, truly real-time, so cannot deliver protection without at least some degree of downtime. This can be from minutes, to tens-of-minutes, depending on the chosen provider. Corero research also shows that the vast majority of DDoS attacks are short (less than ten minutes) and sub-saturating (over 75% are less than 1Gbps) so the typical time to swing traffic to cloud DDoS protection means the attack is often already over and the damage may be done.

A key benefit of the hybrid DDoS protection approach is that the on-premises solution significantly reduces the number of times an organization engages the cloud protection. This lowers costs while delivering a real-time, comprehensive and consistent defense. Another benefit is that during the minutes, to tens of minutes, that the cloud service activation is in process, the attack will still be stopped by the on-premises solution.

2019 DDoS Trends

SUMMARY

13%

Increase In Use Of Multi-Vector Attacks

35%

Increase In Number Of Attacks Over 10Gbps

85%

Of Attacks Lasting 10 Minutes Or Less

23%

Chance Of Repeat Attack On Same Victim Within 24 Hours corero

Corero Network Security is a leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and digital enterprises rely on Corero's award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, with comprehensive visibility, analytics and reporting.

This industry leading technology delivers flexible protection that scales to tens of terabits, with a dramatically lower cost of ownership than previously possible. For more information, visit **www.corero.com**

US Headquarters
293 Boston Post Road West, Suite 310
Marlborough, MA 01752
+1 978-212-1500
info@corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford Road,
Uxbridge, England UB8 1HR, UK
+44 (0) 1895-876579

JUNIPER NETWORKS

Juniper Networks is leading the revolution in networking, making it one of the most exciting technology companies in Silicon Valley today. Juniper's sole mission has been to create innovative products and solutions that meet the growing demands of the connected world.

At Juniper Networks, we believe the network is the single greatest vehicle for knowledge, understanding, and human advancement that the world has ever known.
For more information, visit
http://www.juniper.net

US Headquarters
1133 Innovation Way
Sunnyvale, CA 94089