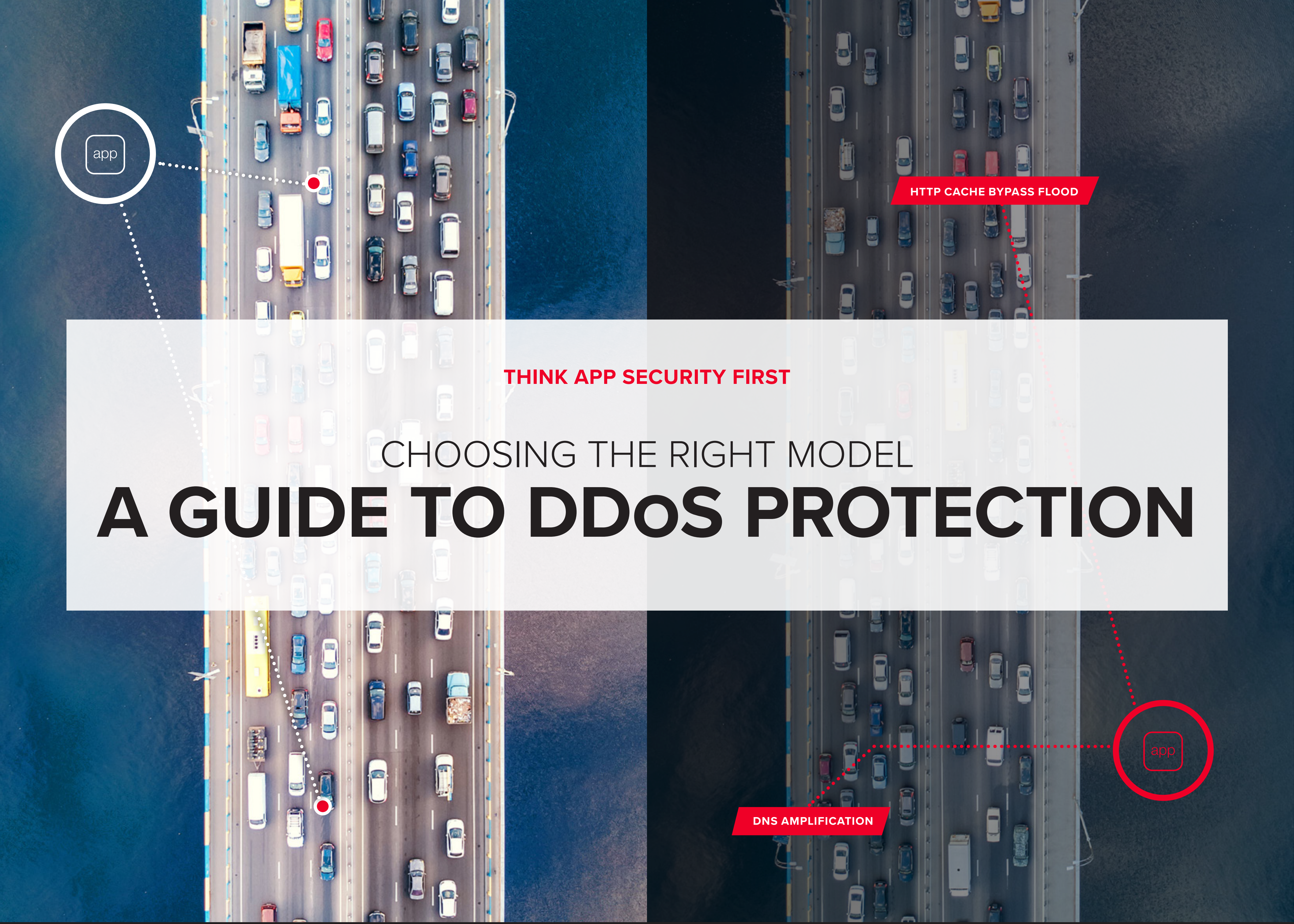


THINK APP SECURITY FIRST

CHOOSING THE RIGHT MODEL

A GUIDE TO DDoS PROTECTION

WE MAKE APPS GO SAFER

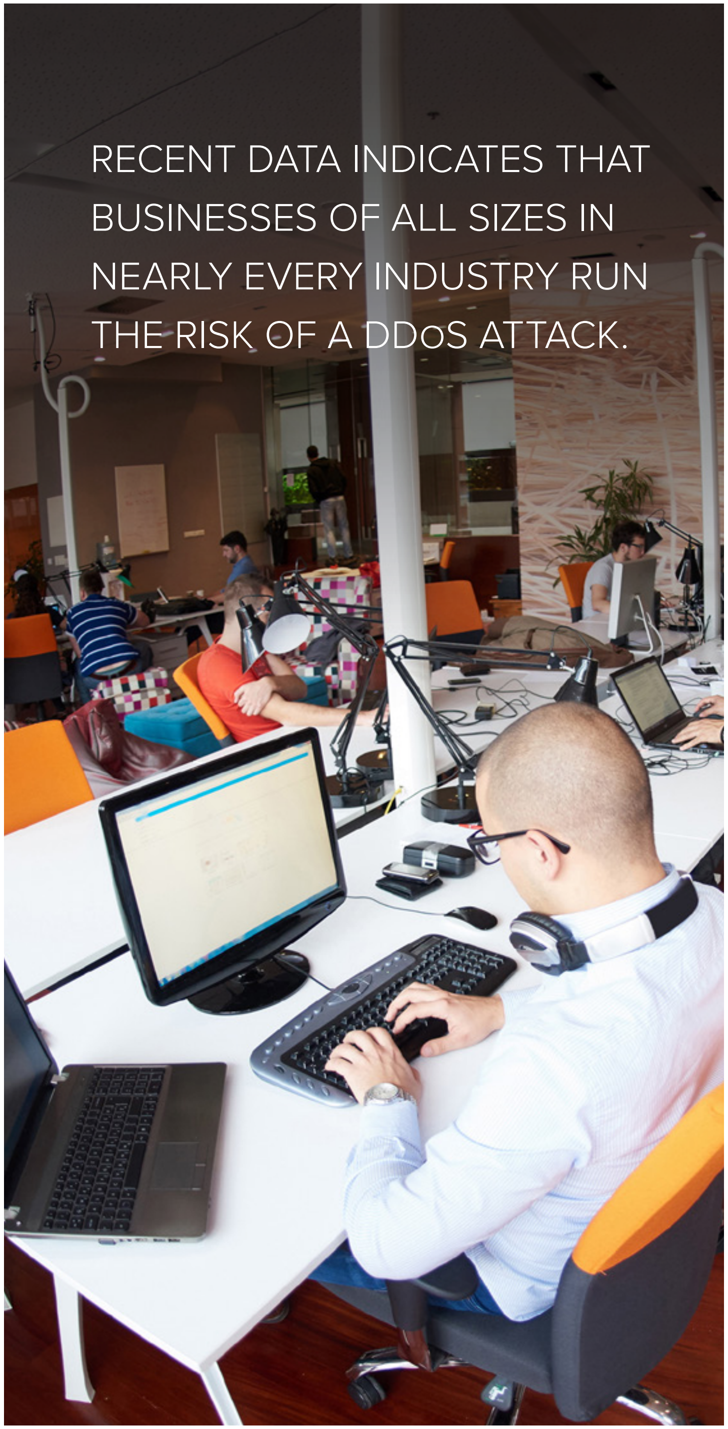
INTRODUCTION

By thinking proactively about DDoS defense, organizations can build a comprehensive strategy to mitigate attacks.

Until recently, security teams for organizations in many industries believed they didn't need to worry about DDoS attacks, but the latest data from the Verizon 2017 Data Breach Investigations Report indicates that businesses of all sizes in nearly every industry run the risk of being attacked.[1] IoT devices are increasingly compromised, recruited into botnets, and offered up by their creators as for-hire DDoS services. Additionally, there are numerous DDoS tools and services that are easily accessible and easy to use, even for the untechnical novice.

Modern denial-of-service attacks not only interrupt or bring down websites and applications, but also serve to distract security operations teams from even larger threats. Attackers combine a variety of multi-vector attacks—including volumetric floods, low-and-slow application-targeted techniques, and authentication-based strategies—in hope of identifying weak spots in an organization's defense.

Whether your organization has already been hit by a DDoS attack or you've witnessed a partner or another organization struggle to mitigate one, planning is the key to survival. Building a DDoS-resistant architecture can help your organization keep its critical applications available and mitigate network, application, and volumetric attacks. With options such as on-premises protection, cloud-based scrubbing services, and hybrid solutions, the question is not whether you should prepare for a DDoS attack, but which strategy best helps your organization ensure service continuity and limit damage in the face of an attack.



RECENT DATA INDICATES THAT BUSINESSES OF ALL SIZES IN NEARLY EVERY INDUSTRY RUN THE RISK OF A DDoS ATTACK.

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

A BRIEF OVERVIEW OF
DDoS ATTACKS TYPES

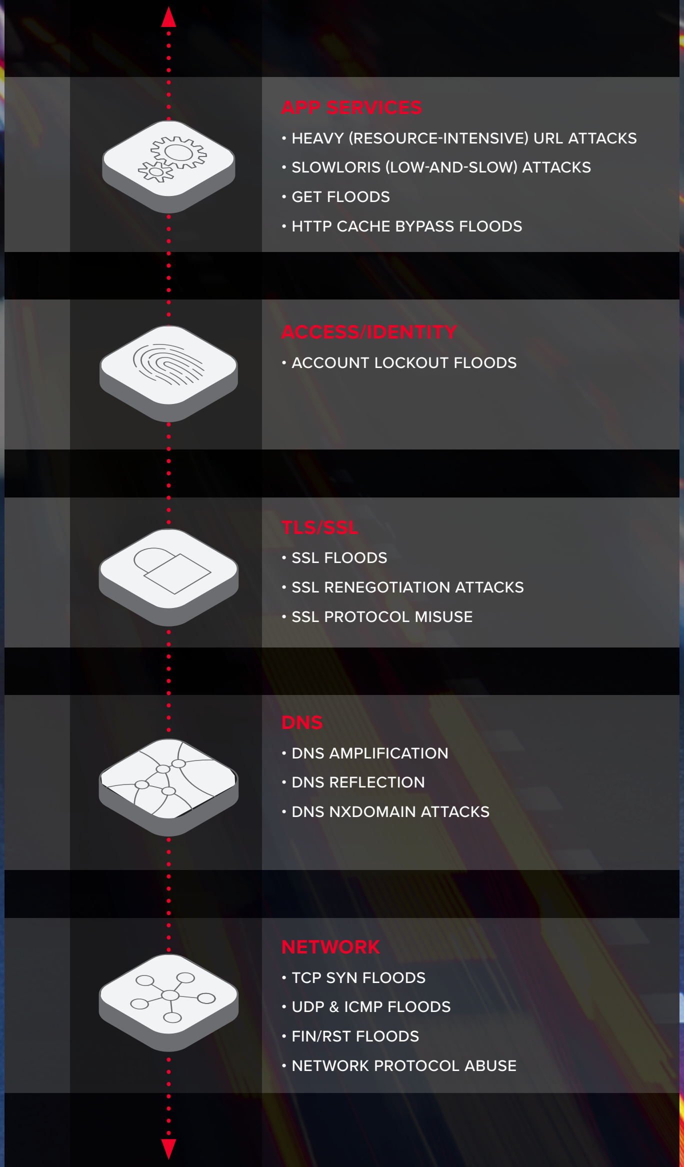
Before considering which DDoS protection strategy makes the most sense for your organization, consider the various types of DDoS attacks, which constantly change as attackers become more and more sophisticated. It helps to picture the components that make up the threat surface of an application and then match them to individual attack types.

While the type of attack(s) you experience will not solely determine which model is right for you, it's important to understand that a DDoS attack can take many forms. And remember that vast swarms of bots (botnets) are most often the delivery mechanism for the attacks. Recognizing bot activity on a per-component level makes it easier to recognize attacks, no matter the type.

It's possible, too, that an attacker might employ several of these attack types in concert, which means that organizations must develop a comprehensive—and flexible—DDoS protection strategy.

On the following pages, we'll explore your options, beginning with the standard on-premises solution.

DDoS IMPACTS ALL LAYERS OF THE APPLICATION STACK



APP SERVICES

- HEAVY (RESOURCE-INTENSIVE) URL ATTACKS
- SLOWLORIS (LOW-AND-SLOW) ATTACKS
- GET FLOODS
- HTTP CACHE BYPASS FLOODS

ACCESS/IDENTITY

- ACCOUNT LOCKOUT FLOODS

TLS/SSL

- SSL FLOODS
- SSL RENEGOTIATION ATTACKS
- SSL PROTOCOL MISUSE

DNS

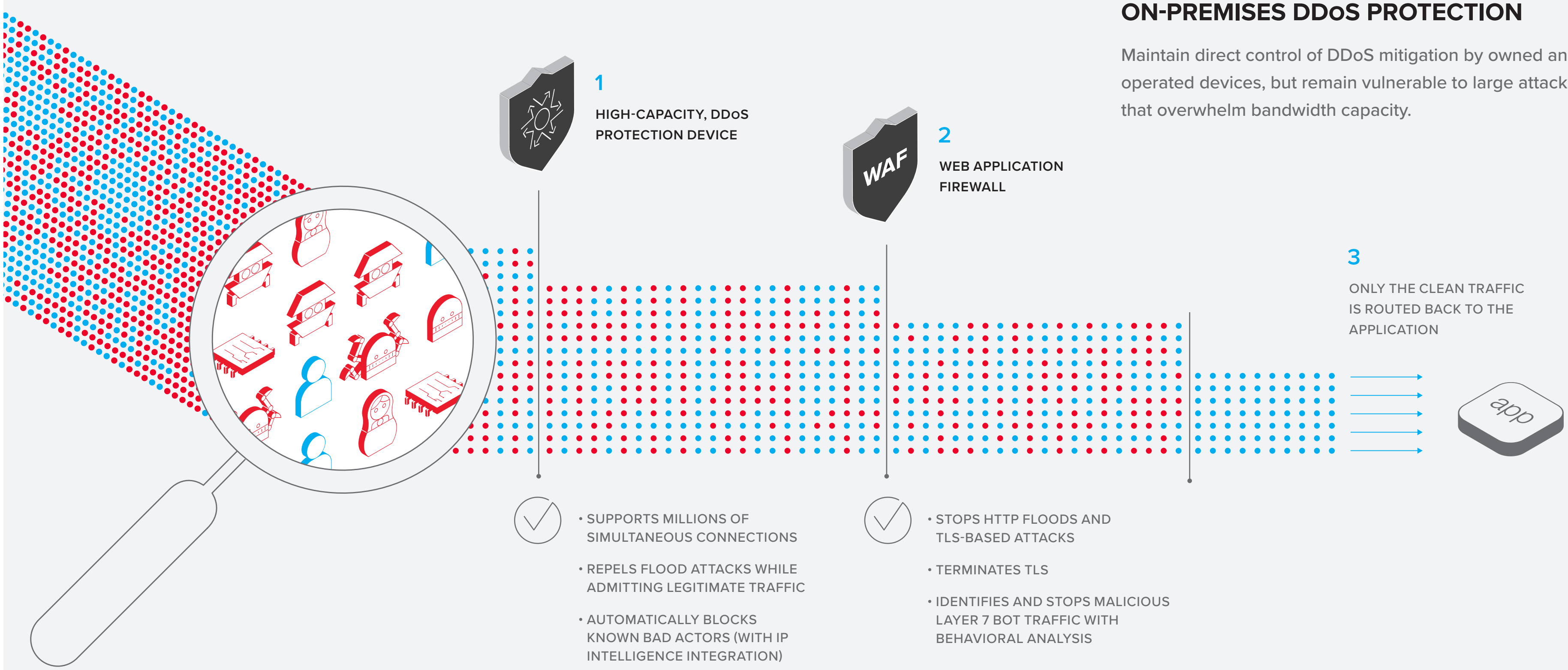
- DNS AMPLIFICATION
- DNS REFLECTION
- DNS NXDOMAIN ATTACKS

NETWORK

- TCP SYN FLOODS
- UDP & ICMP FLOODS
- FIN/RST FLOODS
- NETWORK PROTOCOL ABUSE

MODEL OPTION 1:
ON-PREMISES DDoS PROTECTION

The value of an on-premises solution is clear for many organizations. By deploying point products in your data centers, you can maintain direct control over your infrastructure, allowing you to update, change, add, or remove any piece of it at any time. You also reap the benefit of immediate mitigation of an attack through the instant response of your security devices followed by reporting on the details of the attack. Your in-house IT team can architect custom solutions that scale independently of each other. In addition, low-level DDoS attacks such as Slowloris, as well as exploits that target your applications, are much more efficiently identified and mitigated in your data center close to the application. Furthermore, many organizations—especially large financial institutions—are reluctant to share their private keys with outside vendors, such as a cloud-scrubbing DDoS service.


1
HIGH-CAPACITY, DDoS PROTECTION DEVICE
WAF
2
WEB APPLICATION FIREWALL
3
ONLY THE CLEAN TRAFFIC IS ROUTED BACK TO THE APPLICATION
app

ON-PREMISES DDoS PROTECTION

Maintain direct control of DDoS mitigation by owned and operated devices, but remain vulnerable to large attacks that overwhelm bandwidth capacity.

- SUPPORTS MILLIONS OF SIMULTANEOUS CONNECTIONS
- REPELS FLOOD ATTACKS WHILE ADMITTING LEGITIMATE TRAFFIC
- AUTOMATICALLY BLOCKS KNOWN BAD ACTORS (WITH IP INTELLIGENCE INTEGRATION)

- STOPS HTTP FLOODS AND TLS-BASED ATTACKS
- TERMINATES TLS
- IDENTIFIES AND STOPS MALICIOUS LAYER 7 BOT TRAFFIC WITH BEHAVIORAL ANALYSIS

ON-PREMISES DDOS PROTECTION, CONT.

By keeping DDoS mitigation in house, you always have optimal visibility and control over your protection strategy. The bottom line is that if your organization gets targeted repeatedly, you will save money and time by having an on-premises solution that's fine-tuned and ready to spring into action at the first sign of an attack.

1 TBPS

TODAY'S LARGE-SCALE DDOS ATTACKS ARE EXCEEDING 1 TBPS IN TOTAL THROUGHPUT, WHICH EASILY OUTCLASSES ALL BUT THE LARGEST ON-PREMISES ENTERPRISE DEFENSES.

On-premises solutions do have some limitations. For example, even the most robust on-premises DDoS solution would be overwhelmed by the size of some of today's large volumetric attacks. In addition, while there are many point products on the market, there are very few comprehensive DDoS solutions, which means that organizations must work with multiple vendors to develop a full-featured solution. Managing several products from several different vendors requires a lot of varying technical knowledge and can be a time-consuming process, which detracts from your security operations team's ability to focus on other threats. Furthermore, some of these individual solutions are not extensible and provide value only when you are attacked, which means that you've spent a large amount of money for something you might use only once or twice (if you're lucky).

Finally, not all on-premises solutions are designed to work with upstream cloud solutions—this is an important point to consider as your organization's needs change. Having a vendor that can provide seamless integration from on-premises defense to cloud scrubbing (when needed) helps you streamline your network architecture, reduce time from attack detection to mitigation, and avoid manual steps that can introduce errors.

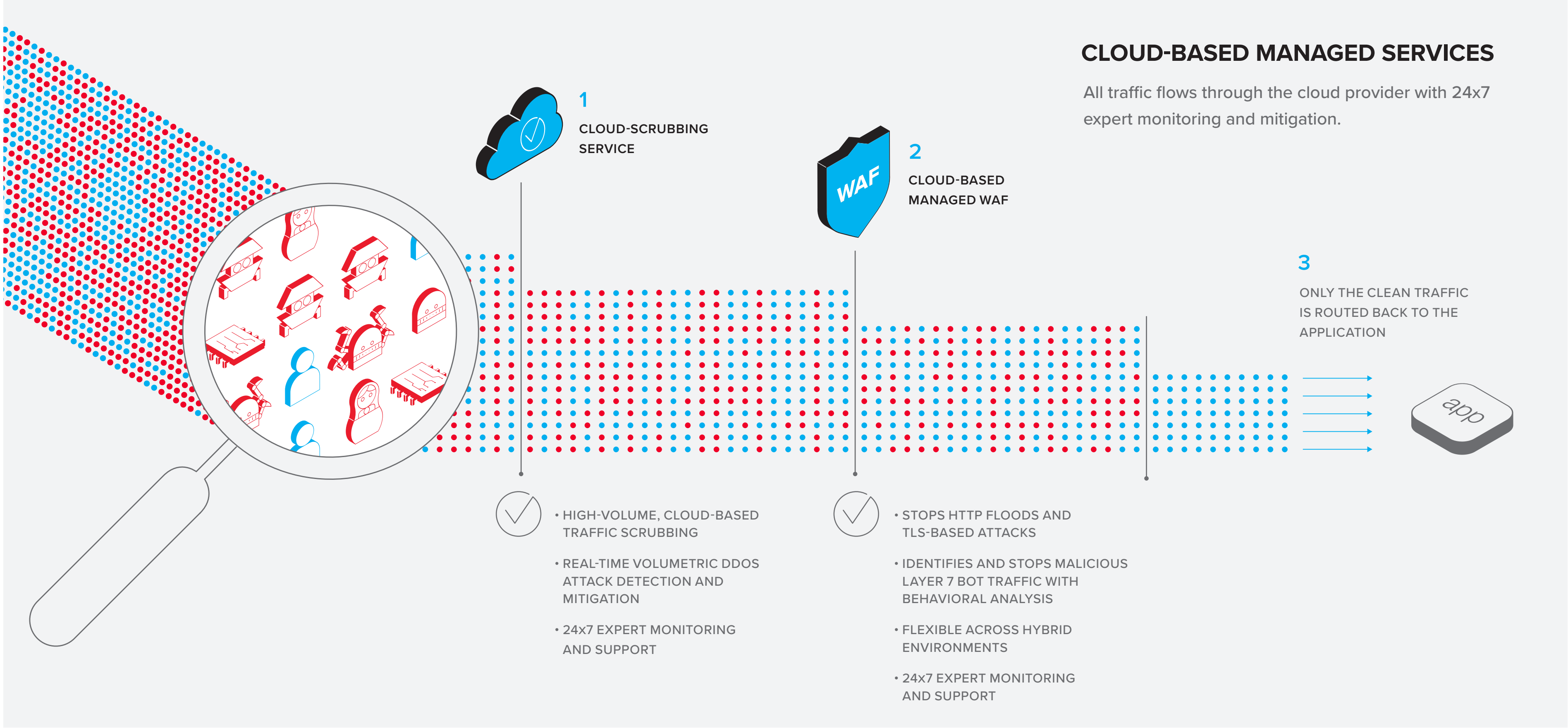
IF YOUR ORGANIZATION GETS TARGETED REPEATEDLY, YOU WILL SAVE MONEY AND TIME BY HAVING A FINE-TUNED ON-PREMISES SOLUTION.

MODEL OPTION 2:
CLOUD-BASED MANAGED SERVICES

For some organizations, employing a cloud-based scrubbing service and web application firewall (WAF) to outsource (or simply upgrade) your DDoS protection is the best strategy. If you're managing "born in the cloud" applications, you many not operate a traditional data center where on-premises security devices could be placed. In addition, you may not have the technical staff to deploy and manage an on-premises DDoS protection solution.

According to the F5 State of Application Delivery 2018 report, 87% of companies surveyed operate applications in multiple clouds.[2] Cloud-based DDoS solutions offer a centralized solution, no matter how many clouds you use. Whether operating in multiple clouds, an in-house data center, or a combination of both, a cloud-scrubbing service ingests your traffic; directs it to massive, globally

[2] https://interact.f5.com/2018_SOAD.html



CLOUD-BASED MANAGED SERVICES

All traffic flows through the cloud provider with 24x7 expert monitoring and mitigation.

1 CLOUD-SCRUBBING SERVICE

- HIGH-VOLUME, CLOUD-BASED TRAFFIC SCRUBBING
- REAL-TIME VOLUMETRIC DDOS ATTACK DETECTION AND MITIGATION
- 24x7 EXPERT MONITORING AND SUPPORT

2 CLOUD-BASED MANAGED WAF

- STOPS HTTP FLOODS AND TLS-BASED ATTACKS
- IDENTIFIES AND STOPS MALICIOUS LAYER 7 BOT TRAFFIC WITH BEHAVIORAL ANALYSIS
- FLEXIBLE ACROSS HYBRID ENVIRONMENTS
- 24x7 EXPERT MONITORING AND SUPPORT

3 ONLY THE CLEAN TRAFFIC IS ROUTED BACK TO THE APPLICATION

CLOUD-BASED MANAGED SERVICES, CONT.

dispersed scrubbing centers; blocks malicious traffic; and then delivers clean traffic to your on-premises or cloud data center(s). And for the attacks aimed at layer 7, application security experts provide continuously updated WAF policies to ensure only legitimate traffic reaches your application.

Cloud-based DDoS protection solves the problem that no on-premises solution can: pipe-saturating DDoS events. Cloud-based DDoS protection services work to block attacks closest to the source of the attack, ensuring that attack traffic never reaches your data center(s) and application(s). In today's world of massive DDoS attacks generated from global IoT botnets, it is imperative to block those attacks as close to the origination point as possible.

IF YOU'RE CONSIDERING A CLOUD-SCRUBBING SERVICE, LOOK FOR ONE THAT ALSO OFFERS A WEB APPLICATION FIREWALL OPTION.

While the majority of the attacks seen today are volumetric attacks aimed at layers 3 and 4, the application layer (layer 7), is seeing an increase in attacks. A cloud-based managed WAF can augment your protection against application-level DDoS attacks. You'll have a solution for the many variations of HTTP floods or heavy URL resource attacks, including complex database queries that can quickly overwhelm your app. With the average salary of an application security engineer in the U.S. now up to $138,000 a year[3], it's expensive to build a team that can be available during nights, weekends, and holidays to fine-tune policies and stay on top of alerts. While this will round out your complete DDoS solution in the cloud, you'll also get many more benefits to your application security, such as defense against OWASP top 10 threats, credential stuffing, and API protection just to name a few.

Managed cloud-based security services can often improve operational efficiency and decrease IT overhead as they can be deployed in minutes. In addition, the best services offer 24x7 attack support from security experts, which can free your security team to focus on other issues. These services protect many customers, so the overall equipment cost is shared among a pool of customers. And because your organization only pays for the services it uses, you often reap significant CapEx savings.

However, if all your network traffic is being scrubbed—and you are bound by the terms of the service agreement you sign with the cloud-scrubbing service—there's less flexibility in customizing your solution. If you are considering a cloud-scrubbing service, look for one that also offers a web application firewall option for application attacks so you can remove the chance of conflict between multiple vendors. Lastly, to effectively protect an application with a managed WAF, your provider will need to terminate TLS which will require them to host your private key.

33%

IN 2017, 33% OF ALL ORGANIZATIONS FACED AT LEAST ONE DDoS ATTACK.[4]

[3] https://www.glassdoor.com/Salaries/applications-security-engineer-salary-SRCH_KO0,30.htm

[4] https://www.techrepublic.com/article/33-of-businesses-hit-by-ddos-attack-in-2017-double-that-of-2016/

MODEL OPTION 3

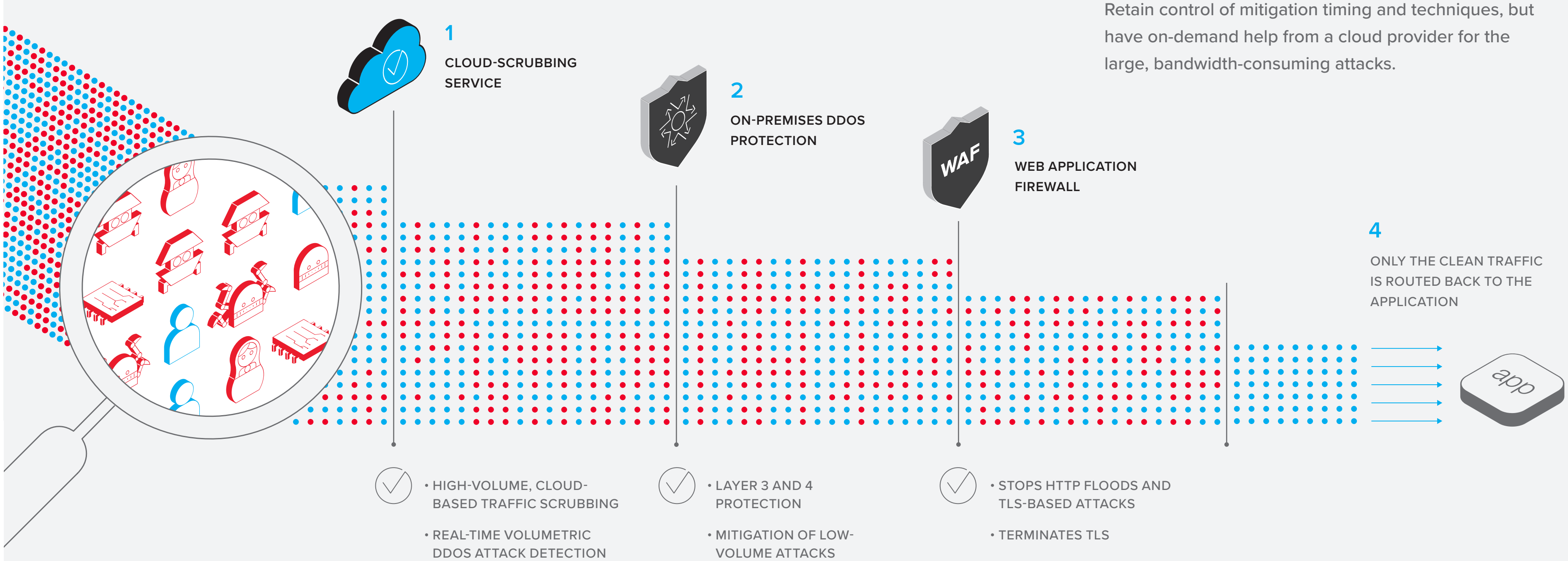
HYBRID DDoS PROTECTION STRATEGY

While both on-premises solutions and cloud-based services offer protection from DDoS attacks, many organizations will want to consider the benefits of a hybrid strategy that employs combined on-premises and cloud protection to stop all varieties of DDoS attacks. Once architected, a hybrid solution delivers a closed feedback loop between on-premises and cloud components, which allows for fine-tuned mitigation as well as granular reporting of attack details.

Perhaps the strongest approach to hybrid DDoS protection involves a multi-tiered architecture where layer 3 and layer 4 attacks are mitigated at the network tier with robust firewalls and IP reputation database integration. The application tier handles high-CPU security functions such as SSL termination and web application firewall functionality. And a cloud-based tier protects against large volumetric attacks by filtering the

HYBRID DDoS PROTECTION

Retain control of mitigation timing and techniques, but have on-demand help from a cloud provider for the large, bandwidth-consuming attacks.



1 CLOUD-SCRUBBING SERVICE

- HIGH-VOLUME, CLOUD-BASED TRAFFIC SCRUBBING
- REAL-TIME VOLUMETRIC DDOS ATTACK DETECTION AND MITIGATION
- 24X7 EXPERT MONITORING AND SUPPORT

2 ON-PREMISES DDOS PROTECTION

- LAYER 3 AND 4 PROTECTION
- MITIGATION OF LOW-VOLUME ATTACKS
- IP REPUTATION DATABASE

3 WEB APPLICATION FIREWALL

- STOPS HTTP FLOODS AND TLS-BASED ATTACKS
- TERMINATES TLS
- IDENTIFIES AND STOPS MALICIOUS LAYER 7 BOT TRAFFIC WITH BEHAVIORAL ANALYSIS

4 ONLY THE CLEAN TRAFFIC IS ROUTED BACK TO THE APPLICATION

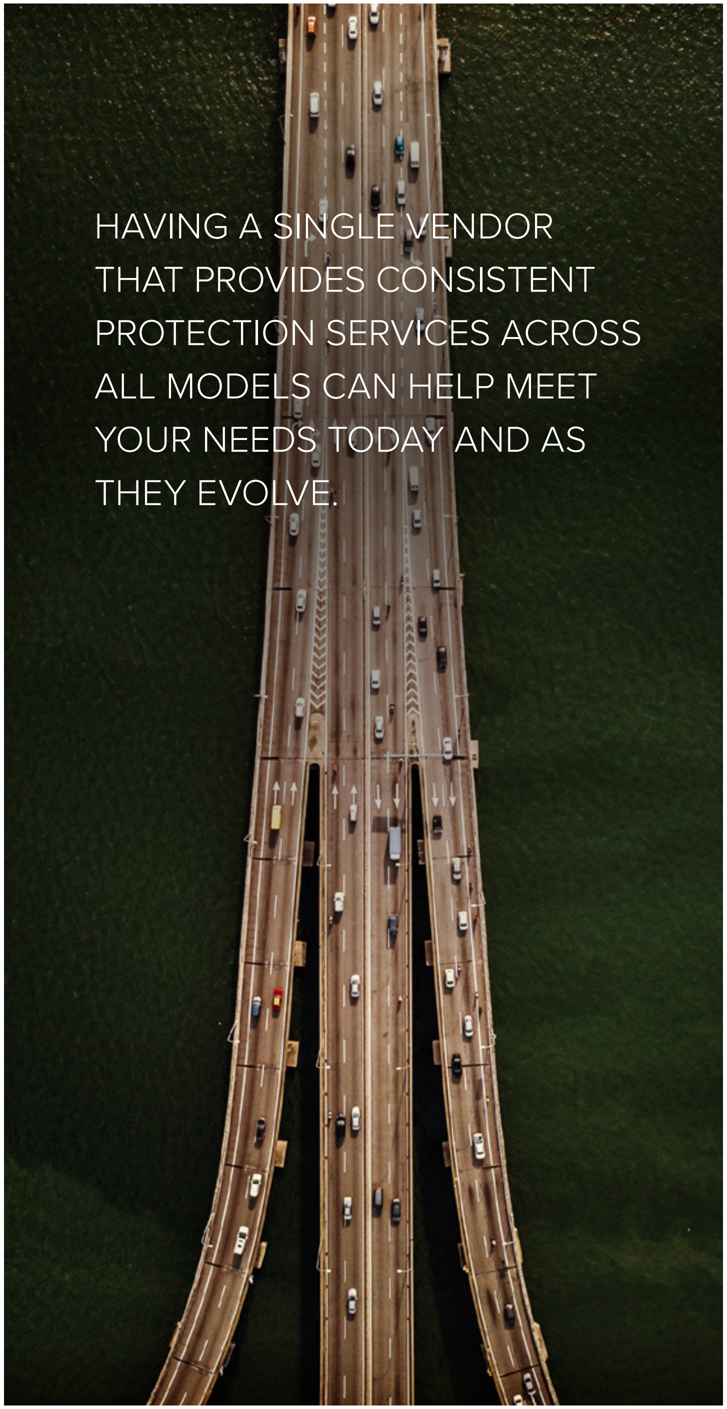
HYBRID DDOS PROTECTION STRATEGY, CONT.

traffic generated by the attacker while returning legitimate traffic to your data center. This true hybrid solution delivers DDoS defense at all layers, protecting protocols (including those employing SSL and TLS encryption) as well as stopping DDoS bursts, randomized HTTP floods, cache bypass, and other attacks that can disrupt application behavior.

A hybrid approach to DDoS protection can also lead to cost savings and greater efficiency. Automatically shifting large attacks to the cloud requires fewer in-house technical resources, while boosting mitigation speed, which results in less downtime. There are also benefits to only engaging the cloud-scrubbing service when you need it, instead of sending traffic through it continuously. This "always-available" architecture allows traffic to flow normally to your data center(s), which reduces complexity, until engagement of cloud-based protections is needed. A true hybrid solution offers expedient cloud-engagement to reroute traffic through the cloud-scrubbing platforms. And, ideally, both parts of your hybrid solution can share a combined fabric that controls whether attacks are handled on-premises or in the cloud—thus enabling the optimal balance for any given attack or series of attacks.

Completely outsourcing your DDoS protection requirements to a cloud-based service is the simplest way to achieve a high degree of protection, while managing a hybrid solution does require some in-house technical resources. In addition, some businesses have spent considerable time and money architecting strong volumetric solutions on-premises, which works well as long as your in-house devices aren't overwhelmed by the growing size of DDoS attacks. The last caveat about a hybrid solution is that your organization may need to employ multiple incident managers to address attacks on-premises and in the cloud.

A HYBRID APPROACH TO DDOS PROTECTION CAN ALSO LEAD TO COST SAVINGS AND GREATER EFFICIENCY.



HAVING A SINGLE VENDOR THAT PROVIDES CONSISTENT PROTECTION SERVICES ACROSS ALL MODELS CAN HELP MEET YOUR NEEDS TODAY AND AS THEY EVOLVE.

IS THERE AN IDEAL SOLUTION?

In today's climate of ever-evolving DDoS attacks, it's increasingly clear that every organization needs to consider and adopt a DDoS protection strategy.

Integrated on-premises solutions offer tight control and flexibility, but can be quickly overwhelmed by a large volumetric attack. Managed cloud-based services deliver protection from those large attacks, but can be expensive if used for all traffic, all the time. By using a combination of on-premises security devices and a cloud-based scrubbing service to handle volumetric attacks, organizations maintain control, while spinning up cloud-protection services as needed to handle the largest volumetric floods.

In choosing how to best protect your organization from DDoS attacks, you should weigh the likelihood of experiencing an attack against the ability of your organization to effectively mitigate it. Having a single vendor that provides consistent protection services across all models to meet your needs today and as they evolve can be a key advantage.

Whatever you decide, be proactive in your DDoS defense. Ensure the continuity of your site and your services by putting your solution in place—before you experience an attack.

For more information about protecting your organization against DDoS attacks, visit f5.com/security.

THINK APP SECURITY FIRST

Always-on, always-connected apps can help power and transform your business–but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com