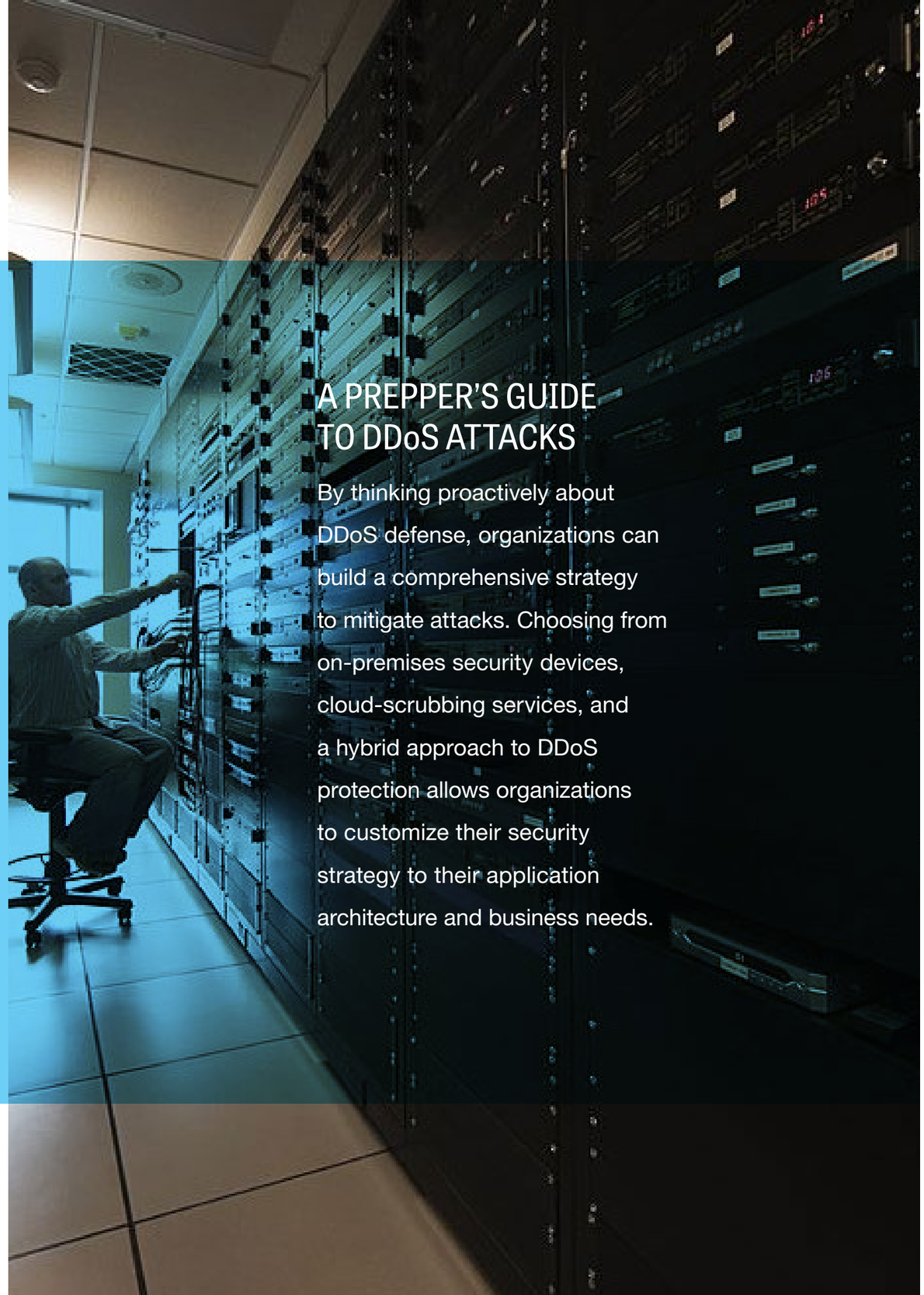
DDOS PROTECTION STRATEGIES: CHOOSING THE RIGHT MODEL



A PREPPER'S GUIDE TO DDoS ATTACKS

By thinking proactively about DDoS defense, organizations can build a comprehensive strategy to mitigate attacks. Choosing from on-premises security devices, cloud-scrubbing services, and a hybrid approach to DDoS protection allows organizations to customize their security strategy to their application architecture and business needs.

Businesses around the world find themselves in a constant struggle against the threat—and reality—of DDoS attacks. 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 hopes of identifying weak spots in an organization's defense.

While the primary purpose of DDoS attacks is to disrupt service to a website or web application, the consequences of a successful attack can be wide-ranging. From the simple loss of revenue (due to a downed site or service such as VPN) and regulatory fines and legal costs resulting from an attack, to a decrease in customer confidence and damage to your organization's reputation, the fallout from a single attack may affect your business for years.

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 2016 Data Breach Investigations Report indicate that businesses of all sizes in nearly every industry run the risk of being attacked.[1] Nearly half of all organizations experienced a DDoS attack at least once in 2014, at an average cost of $200,000–$500,000 per hour.[2] And keep in mind that many DDoS attacks are not even reported publicly. With those sobering facts in mind, every organization is coming to understand the need to implement a comprehensive strategy for mitigating DDoS attacks.

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.

[1]Verizon 2016 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[2]"Understand the Business Impact and Cost of a Breach," Forrester, January 12, 2015, https://www.forrester.com/report/Understand+The+Business+Impact+And+Cost+Of+A+Breach/-/E-RES60563.

WHICH DDoS MITIGATION MODEL IS RIGHT FOR ME?

Before considering which DDoS protection strategy makes the most sense for your organization, here's a quick refresher course on the types of DDoS attacks, which constantly change as attackers become more and more sophisticated.

TYPES OF ATTACKS

While the kind of attack(s) you experience will not solely determine which model is right for you, it's helpful to understand that a DDoS attack can take many forms. Today's attacks fall within four types: volumetric, asymmetric, computational, and vulnerability-based.

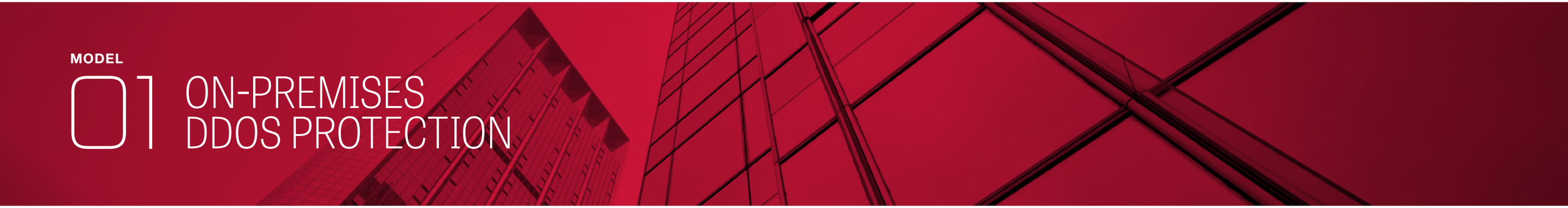
It's possible, too, that an attacker might employ several of these attack types in concert, which means that organizations must develop a comprehensive—and flexible—DDoS protection strategy. Let's explore your options, beginning with the standard on-premises solution.

VOLUMETRIC flood-based attacks that can take place at layer 3, 4, or 7

COMPUTATIONAL attacks designed to consume CPU and memory, such as GET floods long-running queries, and SSL attacks

ASYMMETRIC attacks designed to invoke timeouts or session-state changes

VULNERABILITY BASED attacks that exploit application-software vulnerabilities



MODEL

01 ON-PREMISES DDOS PROTECTION

BENEFITS

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. By keeping DDoS mitigation in house, organizations always have optimal visibility and control over their protection strategy.

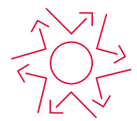
The bottom line is that if your organization gets targeted repeatedly, you will save money and time by having an on-premises solution that's fine-tuned and ready to spring into action at the first sign of an attack.

CONSIDERATIONS

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 largest 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 certain amount of technical knowledge and can be a time-consuming process, which detracts from your security operations team's ability to protect your website and services.

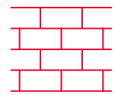
In addition, most of these individual solutions are not extensible and provide value only when you are attacked, which means that you've spent a large amount of money for something you might use only once or twice (if you're lucky). Finally, not all on-premises solutions are designed to work with upstream 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.

ON-PREMISES COMPONENTS



HIGH-CAPACITY, DDOS-AWARE NETWORK FIREWALL

- Supports millions of simultaneous connections
- Repels SYN floods while admitting legitimate traffic



WEB APPLICATION FIREWALL
with integrated DDoS protection

IP REPUTATION DATABASE

MODEL

02 CLOUD-SCRUBBING SERVICES

BENEFITS

For some organizations, employing a cloud-scrubbing service 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, an organization may not have the technical staff to deploy and manage an on-premises DDoS protection solution. Finally, for organizations that do operate an in-house data center, a cloud-scrubbing service can provide a set of high-bandwidth data centers that can scrub your traffic clean before passing it along securely to your data center.

The prime selling point of some of these cloud-scrubbing services is that they are located completely off-premises, so DDoS attacks may never reach your network depending on the subscription level you choose. Real-time volumetric DDoS-attack detection and mitigation in the cloud can keep the bad traffic out of your network, while allowing legitimate users to continue to use your site and services.

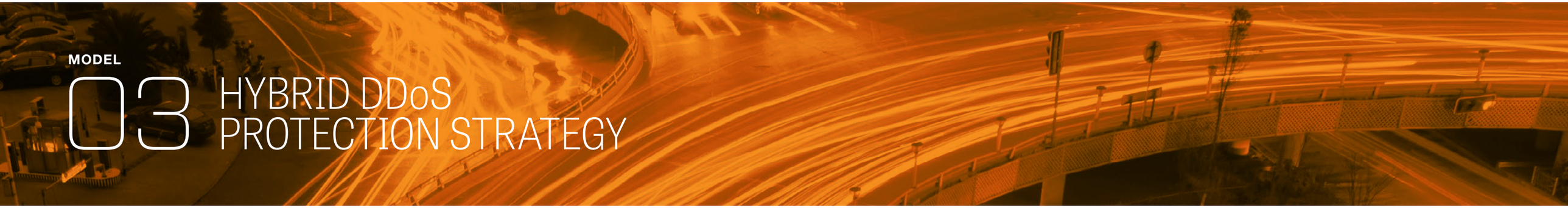
The multiple data centers operated by these cloud-scrubbing services mean that your organization has extra protection from worldwide attacks. Employing DNS Anycast to spread the attack across many global data centers means that attackers cannot focus all their firepower on a single site, even if they are all targeting the same IP address. In addition, having multiple data centers reduces latency and better ensures the high availability of your services and your site.

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

CONSIDERATIONS

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.

Finally, most of these services concentrate on layers 3 and 4 and are not optimal for combatting certain types of attacks, such as layer 7 application attacks and heavy URL resource attacks, including complex database queries, that quickly overwhelm your network. If you are considering a cloud-scrubbing service, look for one that also offers a web application firewall option for application attacks.



MODEL

03 HYBRID DDoS PROTECTION STRATEGY

BENEFITS

While both on-premises solutions and cloud-scrubbing 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 DDoS attacks are mitigated at the network tier with firewalls and IP reputation databases. The application tier handles high-CPU security functions such as SSL termination and web-application firewall functionality. And a cloud-based scrubbing tier protects against large volumetric attacks by filtering the 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.

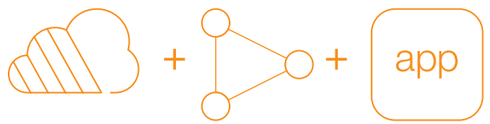
A hybrid approach to DDoS protection can also lead to cost savings and greater efficiency. Automatically shifting large attacks to the cloud requires fewer in-house technical resources, while boosting mitigation speed, which results in less downtime. There's also the benefit of ony paying only for your cloud-scrubbing service when you use it instead of having it turned on all the time. 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.

Perhaps the biggest benefit of the hybrid model is that it prepares your organization for a future when you can use a visual dashboard to manage the entire range of your on-premises and off-premises solutions. As this vision becomes a reality, you can focus less on where the attack should be mitigated and more on managing the combined solution to ensure the high availability of your site and services, as well as continued business growth.

CONSIDERATIONS

Managing a hybrid solution does require some in-house technical resources, while completely outsourcing your DDoS protection needs to a cloud-scrubbing service is the simplest way to achieve a fairly high degree of protection. On the other hand, 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.

HOW A HYBRID SOLUTION WORKS



CLOUD

High-volume, cloud-based traffic scrubbing

Real-time volumetric DDoS attack detection and mitigation

Supporting 24x7x365 expert security services

NETWORK

Layer 3 and 4 network firewall services

Mitigation of transient and low-volume attacks

Simple load balancing to a second tier

IP reputation database

APP

Application-aware, CPU-intensive defense mechanisms

Mitigation of asymmetric and SSL-based attacks

SSL termination

Web application firewall

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-scrubbing services deliver protection from those large attacks, but can be expensive if used exclusively. 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 to 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.

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

RPRT-DDOS MYTHS