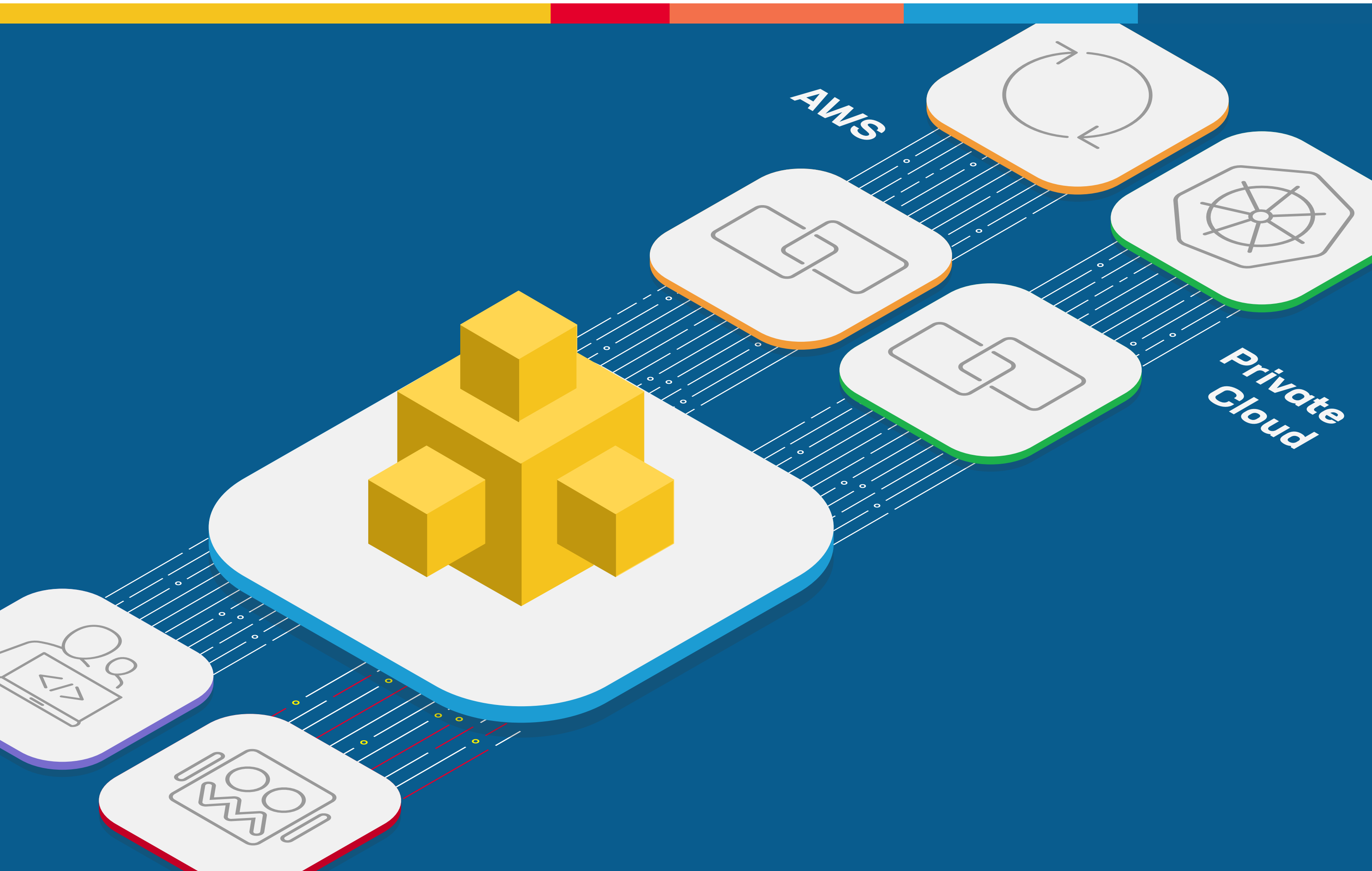
SOLUTION OVERVIEW

Distributed Cloud DDoS Mitigation

F5 Distributed Cloud DDoS Mitigation delivers DDoS and advanced security services to protect against L3-L7 attacks on enterprises and hosting and service providers.



KEY BENEFITS

Maximize uptime
Ensure the availability of critical applications and infrastructure against sophisticated volumetric and distributed attacks by leveraging F5's global network and support.

Reduce total cost of operations
Lower CapEx and OpEx by moving to cloud-based network perimeter security and reduce reliance on appliances and legacy architectures.

On-demand scalability
Dynamically expand capacity and deploy new services on demand without adding appliances or network capacity in your data centers.

Increase productivity
Empower your network and DevOps via a SaaS security platform and central pane of glass. Deliver more projects, new apps, and expanded capacity with existing resources.

Bold Attacks Require F5's Advanced, Multi-Layer DDoS Mitigation

The soaring volume and complexity of distributed denial of service (DDoS) attacks in the current decade warrant cause for concern, as well as finding the most sophisticated protection available. According to F5 Labs, DDoS attacks jumped by 55% in a 15-month period ending March 2021 and became increasingly more complex, with 54% of incidents leveraging multiple attack vectors.

The largest attack in that span measured 500 Gbps and used no fewer than five different attack vectors, according to the F5 report on DDoS attack trends. The technology sector was the most targeted, receiving 27% of all DDoS attacks over those 15 months.

Volumetric DDoS attacks, which attempt to consume critical network and application resources, accounted for 73% of all incidents.

But increasingly, threat actors also sought to exploit different layers of the network and application stack. Application attacks saw a sharp increase compared to previous years and were found in 16% of these DDoS attacks.

Today, DDoS mitigation is essential, and the quality and breadth of your solution matters. You need protection against attacks at multiple layers across your network and application ecosystem.

F5® Distributed Cloud DDoS Mitigation—a key offering in F5 Distributed Cloud Web App and API Protection (WAAP)—provides mitigation against a variety of denial-of-service attacks across L3-L7. It does this through multiple layers of protection, from custom DoS rules and edge firewalls prescreening traffic, to deep packet inspection with advanced scrubbing for enterprises, hosting, and service providers.

High-Capacity, SaaS-Based, and Hybrid DDoS Mitigation

INCREASINGLY, THREAT ACTORS SOUGHT TO EXPLOIT DIFFERENT LAYERS OF THE NETWORK AND APPLICATION STACK. APPLICATION ATTACKS SAW A SHARP INCREASE COMPARED TO PREVIOUS YEARS.

To protect customers against DDoS attacks, F5 Distributed Cloud DDoS Mitigation leverages a globally secured network with points of presence (PoPs) interconnected across a dedicated, multi-terabit redundant private backbone. F5's PoPs are built out with advanced network monitoring, analytics and security technology providing robust, SaaS-based app and infrastructure protection including DDoS mitigation with upstream router monitoring, L3-L4 firewall, machine learning for anomaly detection, deep packet inspection and WAF delivering layer 7 protection.

SaaS-Based DDoS Mitigation

Distributed Cloud DDoS Mitigation safeguards companies and service providers against DDoS for both their network infrastructure and their web application services. Running across F5's global network PoPs—it provides an intelligent mitigation solution for both network and

KEY FEATURES

Multi-layer global DDoS protection
DDoS mitigation tools and technology are distributed across F5's global network PoPs to provide filtering for volumetric, L3/L4, and advanced L7 application DoS attacks wherever protection is necessary.

Flexible service levels
Choose to deploy and manage elements of your DDoS mitigation solution on your own or let F5 deliver as a managed service—deployed, maintained and supported 24x7 by certified experts in our Security Operations Center (SOC).

High-capacity defense
Our secure global network and scrubbing infrastructure spanning 23 PoPs globally is designed to handle today's largest and most complex DDoS attacks with 13 Tbps of combined scrubbing capacity.

Centralized observability
F5 Distributed Cloud console provides extensive information on DDoS attack activity with customizable, single-pane-of-glass management for threat visibility and mitigation data.

Support for organizations of any size and level of sophistication
Get support during attacks of any size, with service options to suit any environment or business requirements, including BGP or proxy routing with on-demand or always-on service options.

Continuous attack monitoring and mitigation
F5 SOCs operate 24x7, leveraging our team of industry leading SOC engineers for technical assistance to obtain the highest level of protection and uptime for all your applications.

application traffic, and is deployed upstream from customers' Internet access. It autonomously protects against public-access DDoS attacks.

Thanks to F5's globally deployed and large-scale network infrastructure, Distributed Cloud Mesh supports direct Border Gateway Protocol (BGP) connections in addition to DNS proxies. The DDoS mitigation mitigation infrastructure is distributed across a spectrum of F5's PoPs worldwide to filter volumetric traffic, L3/L4 protocol threats and advanced L7 application attacks (via on-demand or always-on service) closest to the attack sources.

Hybrid DDoS Mitigations

Combining on-premises defense with F5's SaaS-based DDoS mitigation gives customers the control to defeat targeted network and application-layer attacks. This approach is logical when operating multiple IP transit providers; massive DDoS attack protection is necessary when on-premises appliances cannot handle the full attack volume.

In the event of a volumetric attack overwhelming the capacity of the on-premises appliance or Internet link, DDoS mitigation can be activated by an administrator with assistance from our SOC. The IP prefix under attack is then announced by F5 and mitigated. The scrubbed traffic is received from F5 Distributed Cloud Services either through GRE tunneling or authoritative DNS resolution.

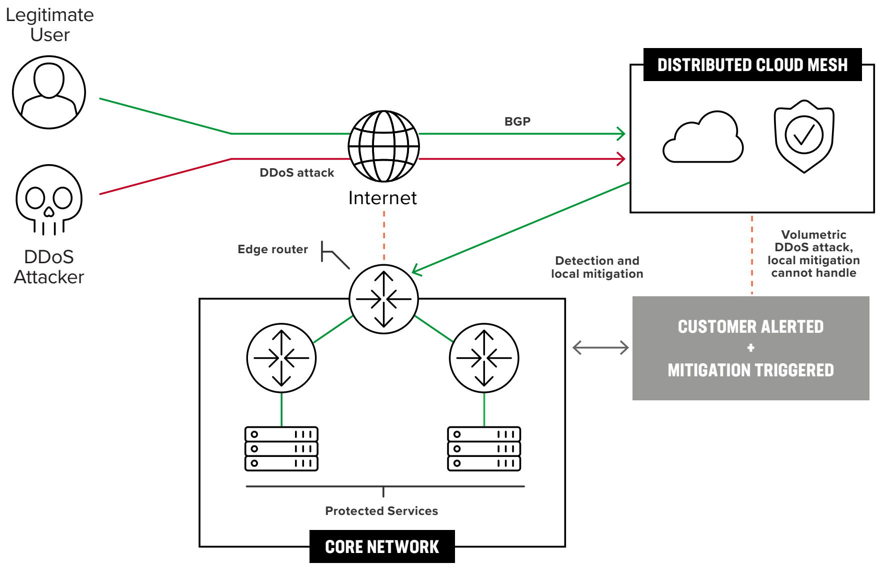

Legitimate User
DDoS Attacker
BGP
DDoS attack
Internet
DISTRIBUTED CLOUD MESH
Edge router
Detection and local mitigation
Volumetric DDoS attack, local mitigation cannot handle
CUSTOMER ALERTED + MITIGATION TRIGGERED
Protected Services
CORE NETWORK

Figure 1: Hybrid DDoS protection: cloud mitigation

How F5's Secured Backbone Protects Your Infrastructure

F5 Distributed Cloud's global, secured network is designed to handle today's largest and most complex DDoS attacks of more than 3 Tbps. When an attack begins, the F5 Global Network and Distributed Cloud DDoS Mitigation infrastructure perform the following actions:

F5 DDOS MITIGATION SYSTEMS ARE DISTRIBUTED ACROSS A SPECTRUM OF F5'S POPS WORLDWIDE TO FILTER L3/L4 AND ADVANCED L7 ATTACKS CLOSEST TO THE ATTACK SOURCES.

1. Cloud Detection

F5's cloud detection equipment and software detect the attack. Detection is based on a combination of static rules and personalized rules per customer:

- Coreprotect: network edge protection and DDoS mitigation using pre-defined global rule sets to block known bad traffic for all customers.
- Auto-mitigation: automatic identification and mitigation of basic and intermediate complexity attacks without intervention from customers.
- Custom Mitigations: flowspec-based mitigation for targeted attacks requiring SOC analysis for specific customers.
- L7 and Proxy Protection: if enabled, additional protection is provided by the Distributed Cloud WAF against application layer attacks including signature based protection, granular rate limiting, AI/ML-based anomaly detection and mitigation, Fast ACLs for internet VIPs, and other factors.

2. Customer Alerting and Reporting

Customers have access to DDoS Mitigation reporting at any time via the Distributed Cloud console, including reporting for attacks automatically mitigated on their behalf. When an attack is detected, our 24x7 SecOps Team (SOC) is alerted and will either notify you to trigger the mitigation or trigger the mitigation on your behalf.

3. Cloud-Based DDoS Scrubbing

Customers who are high value targets, dealing with more persistent, complex attacks may benefit from advanced mitigation with deep packet inspection. When specialized or advanced DDoS attacks are detected, the traffic may be diverted either continuously (if enabled) or by the SOC to regional mitigation network locations for full packet inspection, custom filtering, and other advanced countermeasures.

F5 Distributed Cloud DDoS Mitigation provides a variety of service and connectivity options depending on the location of apps, level of service, and protection needed. This includes always-on or always-available scrubbing options and several routing choices for diverting traffic to scrub—such as BGP route advertisement to the F5 global network or proxy via DNS-based redirection. Distributed Cloud Services steers the traffic to our scrubbing centers to block the attack, allowing only legitimate traffic to go through.

For more information about F5 Distributed Cloud DDoS Mitigation and the Distributed Cloud WAAP services, visit f5.com. Contact sales@f5.com to learn more or to schedule a demo.