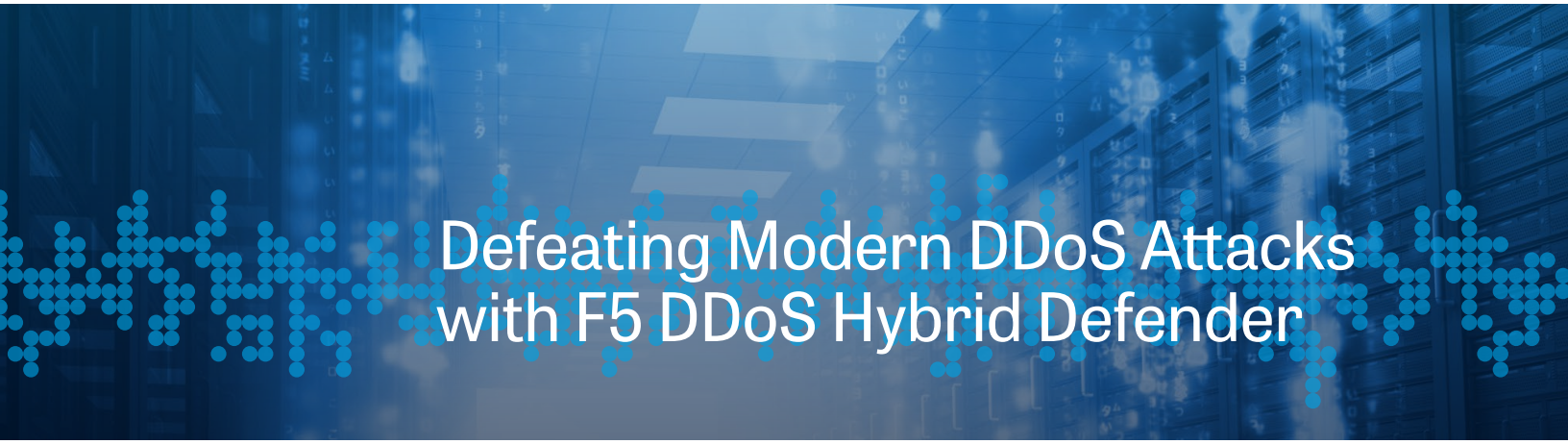

Defeating Modern DDoS Attacks with F5 DDoS Hybrid Defender

KEY BENEFITS

Ensure business continuity by quickly discovering and mitigating attacks.

Reduce time to mitigation with automatic and contextual traffic monitoring.

Protect services for legitimate traffic with on-demand cloud-based scrubbing.

Defend and secure applications and infrastructure.

Ensure availability of your applications with a next-generation distributed denial-of-service (DDoS) defense that blocks today's multi-vector threats, including attacks that target applications and the underlying infrastructure. F5® DDoS Hybrid Defender™ integrates on-premises DDoS protection with optional cloud-based scrubbing for rapid mitigation and a low total cost of ownership (TCO).

Challenge

DDoS attacks are rapidly evolving in severity, complexity, and sophistication, threatening businesses with losses in revenue, customer confidence, and industry credibility. Modern denial-of-service (DoS) attacks are not only interrupting or bringing down services, but distracting security operations teams with a mix of threats that have varying effects on the infrastructure. Attackers also combine volumetric, partial saturation, authentication-based, and application-level attacks until they find a weak point. These threats, which are becoming more difficult to defend against, are often a precursor for advanced persistent attacks. How quickly your organization can discover and stop these threats is key to ensuring service continuity and limiting damage.

Solution

As a high-performance appliance that is easy to deploy and manage, DDoS Hybrid Defender guards against even the most aggressive and targeted DDoS attacks. Its unique, multi-pronged design defends the data center and application infrastructure with:

- The industry's only true, multi-layered defense providing DDoS protection for applications, protocols, and the network.
- Sophisticated application attack defense with in-depth behavioral analytics.
- Full SSL decryption capabilities.

Organizations gain more comprehensive anti-DDoS functionality with controls that enable a flexible hybrid defense without impeding legitimate traffic. DDoS Hybrid Defender also delivers leading scale and high performance with line rate capabilities.

Comprehensive attack coverage

DDoS Hybrid Defender delivers immediate protection against complex vectors, saturation attacks, reflective and amplification attacks, and simultaneous application-layer events. This full-proxy solution offers DDoS protection 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.

Seamless hybrid defense

DDoS Hybrid Defender reduces mitigation times and enables you to implement more granular DDoS rules and policies by automatically collecting and analyzing data across deployments—data that includes SSL inspection, behavioral analytics, bandwidth usage, health monitoring, and other statistics. This capability ensures that attacks can be discovered sooner and mitigation activated swiftly and accurately via hardware, upstream, or across cloud-based services.

Designed to integrate with the F5 Silverline® cloud-based scrubbing service, F5 DDoS Hybrid Defender ensures fast activation of on-demand cloud-based scrubbing, seamlessly re-directing attack traffic to prevent even the largest volumetric attacks from saturating in-bound pipes. In addition, get immediate access to advanced technical expertise from dedicated F5 Silverline Security Operations Center engineers, who are available 24/7.

Unlike other hybrid DDoS approaches, the F5 solution is seamless, transparent, and managed to reduce errors and IT overhead. It enables a smooth and immediate transition back to on-premises protection once attack traffic has subsided to normal levels.

Features

DDoS Hybrid Defender protects the most complex infrastructures, enabling organizations to improve data center and application level security, protect customer data and access, and enhance overall security postures.

Features	Details
Protocol anomaly detection	Including SYN/ICMP/ACK/UDP/TCP/IP/DNS/ARP/SIP
DoS and DDoS protection	L3, L4, L7, SSL, DNS, HTTP, floods, sweeps
Remotely triggered black hole filtering (RTBH)	Using BGP protocol
Accelerated blacklist enforcement	Automatically blacklist IPs in violation of DDoS policies
IP reputation and geolocation	Drop or block traffic from known suspicious IPs
SNMP reporting	Included
Cloud mitigation off-load	Requires F5 Silverline DDoS Protection license
Out-of-box protection	Auto sizing and auto configuration of DDoS protection features

To learn more, contact your F5 representative.

OV-SEC-92998339-ddos 0616