IP Intelligence Service

DATA SHEET

What's Inside

Defend Against Malicious Traffic

Organizations today are exposed to a variety of potentially malicious attacks from rapidly changing IP addresses. Inbound and outbound botnet traffic such as distributed denial-of-service (DDoS) and malware activity can penetrate security layers and consume valuable processing power.

F5® IP Intelligence incorporates external, intelligent services to enhance automated application delivery with better IP intelligence and stronger, context-based security. By identifying IP addresses and security categories associated with malicious activity, the IP Intelligence service can incorporate dynamic lists of threatening IP addresses into the F5 BIG-IP® platform, adding context to policy decisions. IP Intelligence service reduces risk and increases data center efficiency by eliminating the effort to process bad traffic.

Key benefits

Ensure IP threat protection
Deliver contextual awareness and analysis to block threats from a dynamic set of high-risk IP addresses.

Improve visibility into threats from multiple sources
Detect malicious activity and IP addresses with help from a global threat-sensor network and IP intelligence database.

Enable granular threat reporting and automated blocking
Reveal communication with malicious IP addresses to create more effective security policies.

Optimize protection with real-time updates
Automatically refresh the threat database as often as every five minutes to keep the organization safe.