IP Intelligence Service

DATA SHEET

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.

What's Inside

Contextual Awareness and IP Threat Protection

Using a frequently updated list of threat sources and high-risk IP addresses, IP Intelligence delivers contextual awareness and analysis of IP requests to identify threats from multiple sources across the Internet. The service draws on the expertise of a global threat-sensor network to detect malicious activity and IP addresses. Even when the BIG-IP device is behind a content delivery network (CDN) or other proxies, the IP Intelligence service provides protection by looking at the real client IP addresses as logged within the X-Forwarded-For (XFF) header. You can easily configure alarms or block traffic from a CDN with threatening IP addresses.

Deliver key contextual awareness

IP Intelligence:

- Updates the list of threatening IP addresses as frequently as every five minutes.
- Identifies and blocks the sources of known bad IP addresses.
- Identifies and blocks communications with new threatening IP addresses.

Protection Categories

The IP Intelligence service identifies and blocks IP addresses associated with a variety of threat sources, including:

Windows exploits: Includes active IP addresses offering or distributing malware, shell code, rootkits, worms, or viruses.

Web attacks: Includes cross-site scripting, iFrame injection, SQL injection, cross domain injection, or domain password brute force.

Botnets: Includes botnet command and control channels and infected zombie machines controlled by the botnet controller.

Scanners: Includes all reconnaissance, such as probes, host scan, domain scan, and password brute force.

Denial of service: Includes DoS, DDoS, anomalous SYN flood, and anomalous traffic detection.

Reputation: When enabled, denies access to IP addresses currently known to be infected with malware or to contact malware distribution points.

Phishing: Includes IP addresses hosting phishing sites or other kinds of fraud activities, such as click fraud or gaming fraud.

Proxy: Includes IP addresses providing proxy and anonymization services, as well as The Onion Router (TOR) anonymizer addresses.

Granular Threat Reporting and Automated Blocking

Armed with the latest intelligence and predictive risk analyses, IP Intelligence reveals inbound and outbound communication with malicious IP addresses and enables granular threat reporting and automated blocking. This increased visibility can reveal IP-based threats such as phishing attacks, attackers using anonymous proxies, the TOR network for online attacker anonymity, and even outbound communication with botnet command and control channels, exposing malware residing within the enterprise. Once identified, these threats can be mitigated by automatically blocking traffic through selected IP categories.

Sophisticated Threat Detection and Analysis

IP Intelligence incorporates a data set of threatening IP addresses and assigns threat categories. Network traffic and behavioral data from all IP addresses is also collected, analyzed, and assigned to threat categories, providing visibility into threats based on IP addresses as they evolve.

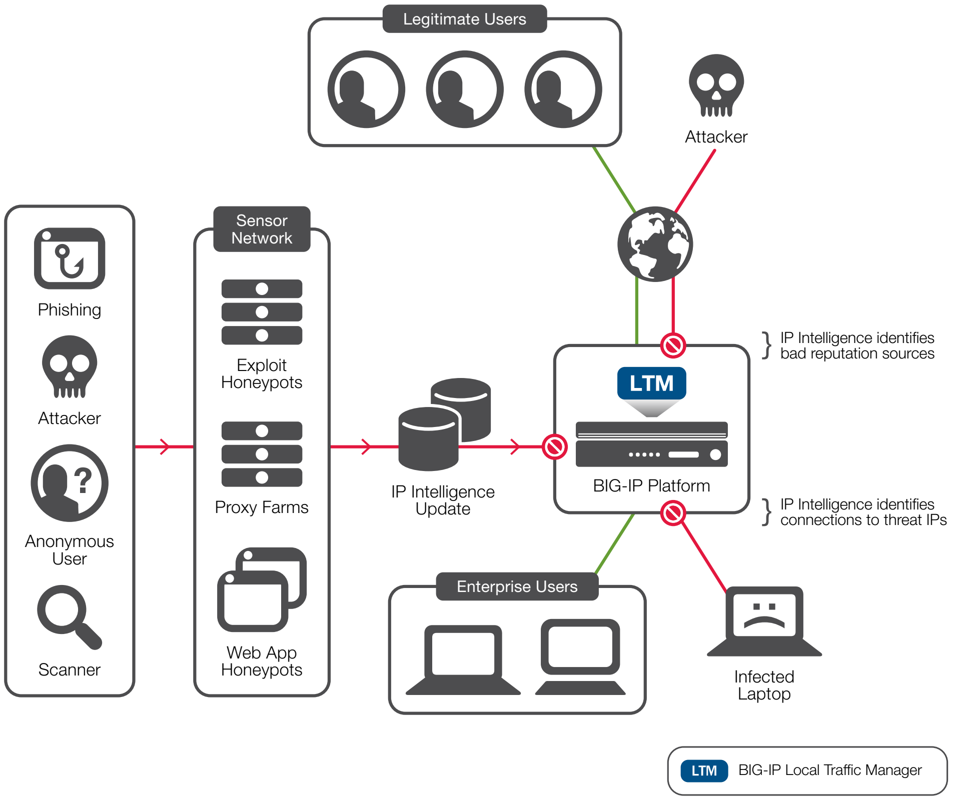

Figure 1: IP Intelligence identifies IP addresses, compares them to the global IP Intelligence database, and allows or blocks connections based on current known risks.

Threat Expertise from an Evolving IP Intelligence Database

When deployed on the F5 BIG-IP system, IP Intelligence uses insight about the Internet's most threatening IP addresses to block connections to and from those addresses. This evolving database of addresses is refreshed from the cloud as frequently as every five minutes to keep threat data current, minimize the threat window, and protect the organization and its reputation.

By detecting and blocking undesirable traffic, IP Intelligence offloads a significant percentage of the server workload. Emerging threats are continuously captured and published, while IP addresses that are no longer a threat are removed from the threat data. IP Intelligence augments visibility for all BIG-IP platforms without compromising access to legitimate IP addresses.

Real-Time Updates for Continuous Protection

Authenticated access to global threat data in the cloud enables IP Intelligence to update the BIG-IP system as frequently as every five minutes. BIG-IP products are easily configured to receive these real-time updates, delivering convenient security management while providing additional context during IP requests.

BIG-IP Platforms for Flexible Deployment

IP Intelligence is a subscription-based service that may be configured with the BIG-IP® Application Security Manager™ (ASM) user interface or incorporated into any BIG-IP platform with the F5 iRules® scripting language. For instance, IP Intelligence can be deployed with BIG-IP® Local Traffic Manager™ (LTM) in front of an e-commerce or financial website to mitigate phishing attacks. Add IP Intelligence to BIG-IP ASM to increase contextual awareness of Internet sites and protect requested applications from IP addresses with known malware or viruses. See the BIG-IP Platform Data Sheet for hardware details.

VIPRION Platforms

The IP Intelligence service is also available on the modular F5 VIPRION® system. The IP Intelligence service may be configured with the BIG-IP ASM user interface or incorporated with iRules into any BIG-IP product on the VIPRION platform. See the VIPRION Data Sheet for hardware details.

F5 Services

F5 Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Services can help you achieve IT agility. For more information about F5 Services, contact consulting@f5.com or visit f5.com/services.

More Information

To learn more about IP Intelligence, use the search function on f5.com to find this and other resources.

Data sheets

BIG-IP Platform

VIPRION

White paper

IP Intelligence

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.