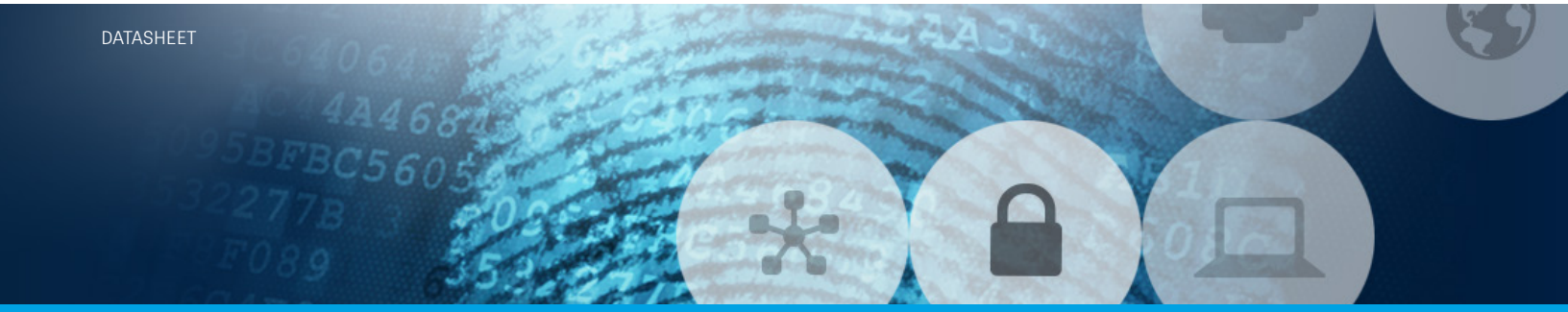
F5® Silverline®
Threat Intelligence

DATASHEET



What's Inside

Defend Against Malicious Traffic

Organizations today are exposed to a variety of malicious attacks from rapidly changing IP addresses. Inbound botnet traffic, such as distributed denial-of-service (DDoS) and malware activity, can penetrate security layers and consume valuable processing power slowing down networks and applications. According to a 2015 Threat Brief, 85,000 new malicious IPs are launched every day.*

F5® Silverline® Threat Intelligence is a cloud-based service incorporating external IP reputation and reducing threat-based communications. By identifying IP addresses and security categories associated with malicious activity, this managed service integrates dynamic lists of threatening IP addresses with the Silverline cloud-based platform, adding context-based security to policy decisions. Silverline Threat Intelligence is available only as an add-on managed service to either Silverline® DDoS Protection or Silverline® Web Application Firewall. All services are managed with 24x7x365 support from F5 Security Operations Center (SOC) experts, reducing risk and increasing network and application efficiency by eliminating the effort of processing threat-sourced traffic.

Key benefits

Ensure IP threat protection
Deliver contextual awareness with SOC-designed threat mitigation from a set of high-risk IP addresses.

Improve threat visibility
Learn malicious activity and threat sources based on selected categories using a global threat-sensor network and threat database.

Automate blocking and granular reporting
SOC experts design policy that automatically blocks new IP threats. Silverline Threat Intelligence reveals communication from malicious IP addresses.

Optimize real-time threat security
Automatic threat database updates are refreshed in real time to mitigate malicious communication.

*Threat Brief Report, Webroot, May 2015

Contextual Awareness and Threat Protection

Using a frequently updated list of threat sources and high-risk IP addresses, Silverline Threat Intelligence delivers contextual awareness and analysis of IP requests to identify threats from multiple sources across the Internet. F5 SOC experts draw on the capabilities of a global threat-sensor network to detect malicious activity and IP addresses. Even when Silverline Threat Intelligence is behind a content delivery network (CDN) or other proxies, it provides protection by analyzing the real client IP addresses as logged within the X-Forwarded-For (XFF) header. This allows the SOC to easily configure alarms or block traffic from a CDN with threatening IP addresses.

Protection Categories

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

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

Botnets: Botnet command and control channels and infected zombie machines controlled by the bot master.

Cloud provider networks: Detects cloud-based IP addresses used in malicious threats.

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

Illegal websites: Denies access to illegal IP addresses for sites on regulatory or compliance block lists due to unapproved content.

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

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

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

Spam sources: Known IP address for sending or creating spam.

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

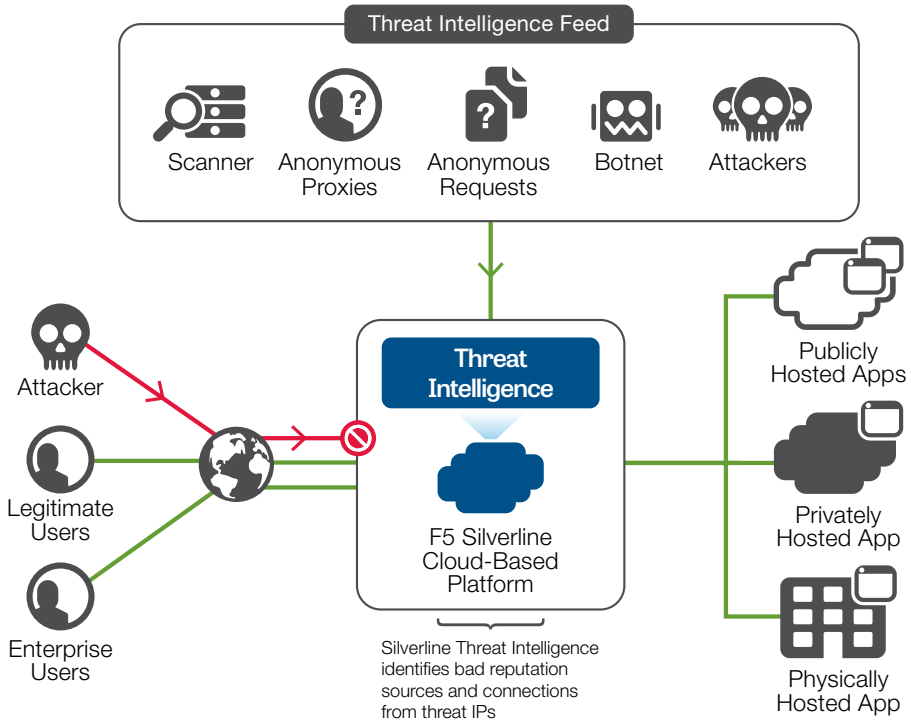
Windows exploits: Active IP addresses offering or distributing malware, shell code, rootkits, worms, and viruses.

Granular Threat Reporting and Automated Blocking

Armed with the latest intelligence and predictive risk analyses, F5 SOC experts incorporate Silverline Threat Intelligence to reveal inbound communication with malicious IP addresses, and enable granular threat reporting and automated blocking. This increased visibility exposes IP-based threats such as phishing attacks, attackers using anonymous proxies, and the TOR network for online attacker anonymity. Once identified, these threats are mitigated by automatically blocking traffic through SOC-selected IP categories.

Sophisticated Threat Detection and Analysis

Silverline Threat Intelligence inspects network traffic and behavioral data from all IP addresses. This information is collected, analyzed, and assigned to threat categories—providing visibility into IP address-based threats as they evolve.

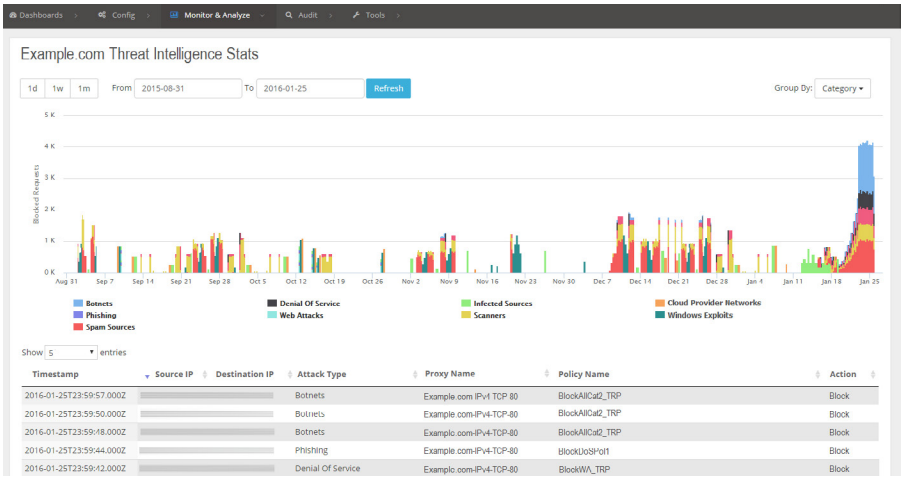


Silverline Threat Intelligence identifies IP addresses, compares them to the global IP reputation database, and allows or blocks connections based on current known threats.

Threat Expertise from an Evolving IP Reputation Database

Managed by the F5 SOC, Silverline Threat Intelligence uses insight about the Internet's most threatening IP addresses to block connections from those requests. This evolving database of addresses is refreshed from the cloud frequently to keep threat data current, minimize the threat window, and protect the organization and its reputation.

By detecting and blocking malicious traffic, Silverline Threat Intelligence reduces a significant percentage of network resources. Emerging threats are continuously captured and published, while IP addresses that are no longer a threat are removed from the threat data. Silverline Threat Intelligence also enhances Silverline DDoS Protection or Silverline Web Application Firewall (WAF) services without compromising access to legitimate IP addresses.



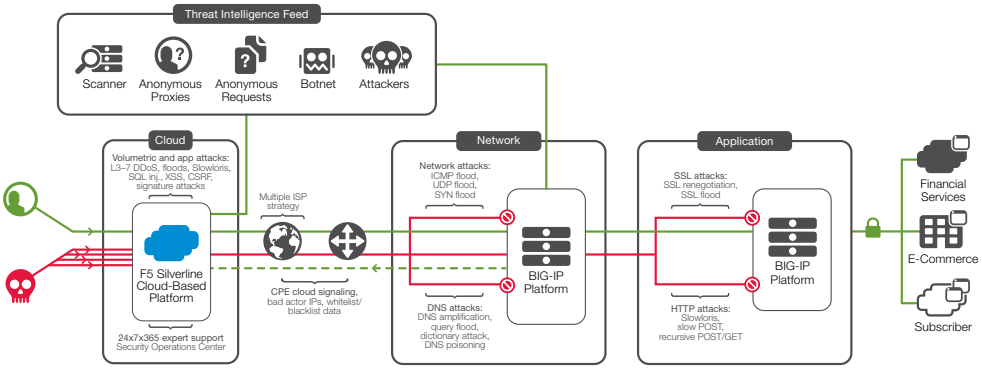
The Silverline Threat Intelligence customer portal allows you to learn what current and past violations have been mitigated, and the detail stats for each violation.

Real-Time Updates for Continuous Protection

Authenticated access to global threat data in the cloud enables Silverline Threat Intelligence to update frequently. This service is configured to receive real-time updates, delivering additional security and protection while providing additional context during IP requests.

Incorporate Threat Intelligence with Hybrid Security Solutions

F5 offers comprehensive hybrid security on premises, in virtual environments, and across hybrid cloud. Silverline DDoS Protection and Silverline Web Application Firewall are cloud-based managed services that are easily consolidated with security solutions available on the F5 BIG-IP® platform—for hybrid DDoS and hybrid WAF deployments. Silverline Threat Intelligence is available only as an add-on to either Silverline DDoS Protection or Silverline Web Application Firewall for enhancing IP threat protections. Silverline Threat Intelligence builds on the PCI-DSS compliant Silverline DDoS Protection and Silverline Web Application Firewall managed services with additional threat protection.



Silverline Threat Intelligence adds IP reputation and threat protection services to Silverline DDoS Protection or Silverline Web Application Firewall.

The Silverline Cloud-Based Platform

F5 Silverline is a cloud-based application services platform. Its services can be deployed on-demand to achieve seamless scalability, security, and performance for applications in traditional and cloud environments. By combining on-premises application services with F5 Silverline services, organizations can achieve faster response times, unparalleled visibility and reporting, and cost efficiencies.

Flexible Licensing

Silverline Threat Intelligence is available in 1-year and 3-year subscriptions based on clean bandwidth required.

F5 Security Operations Center

The F5 Security Operations Center offers world-class support and guidance to help you get the most from your F5 Silverline investment. Whether it's providing fast answers to questions, guidance on your security questions, or assisting with modifications to your implementation, the F5 SOC can help ensure your applications are always secure, fast, and reliable. For more information about the SOC, visit f5.com/soc.

More Information

To learn more about Silverline cloud-based application services, please contact your F5 representative or channel reseller.

You can also visit f5.com to find these and other resources:

Web Pages

F5 Silverline Cloud-Based Application Services
F5 Silverline DDoS Protection
F5 Silverline Web Application Firewall
F5 Silverline Threat Intelligence
F5 Security Operations Center

If you're under attack, F5 offers 24-hour support:

+1 866-329-4253

+1-206-272-7969

f5.com/attack

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

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle East/Africa emeainfo@f5.com
Japan f5j-info@f5.com

Solutions for an application world.

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. DC0315 DS-SILVERLINE IPI-62642768