WebSafe and MobileSafe

DATASHEET

Protect Your Business and Customers from Online Fraud

What's Inside

Online services allow your company to have a global presence and to easily reach users wherever they may be. Customers depend on you, however, to ensure the integrity of your e-commerce site or website and protect them against fraud and malicious activity.

F5® WebSafe™ and F5 MobileSafe™ safeguard banks, e-retailers, and other organizations, along with their online customers, from a broad range of web fraud across all devices—without impacting the user experience. WebSafe helps organizations identify and protect against web-based malware and online fraud targeting web applications. MobileSafe offers protection against advanced online threats targeting the mobile device user. Together, these services give your organization the ability to provide greater online fraud protection and make more informed security decisions.

Key benefits

Protect against targeted and generic malware

Recognize and safeguard against sophisticated threats, including web injection, credential grabbing, man-in-the-browser (MITB), man-in-the-middle (MITM), session hijacking, password stealers, and more.

Prevent phishing attacks

Identify phishing attacks before they are launched—at the point where attackers are creating and testing spoofed domains.

Cover all website users

Inspect all users, whether they are browsing from a desktop, mobile device, set-top box, or even a game console.

Easily deploy fraud detection and prevention

Secure your site without application modifications or changes to the user experience.

Maintain up-to-date global threat intelligence

Monitor the latest and most sophisticated attacks that may potentially impact your business.

WebSafe

WebSafe helps website owners identify and protect against targeted and generic malware, MITB, MITM, zero-day fraud, and phishing attacks, plus other fraudulent online activities. WebSafe applies a variety of identification techniques to recognize web fraud, attempted automated transfers, and other malware patterns.

WebSafe is easy to deploy and completely transparent to the user, requiring no changes to the application or user client installations. With WebSafe, your organization gains advanced real-time protection against the theft of identity, intellectual property, sensitive data, and money.

MobileSafe

MobileSafe is a product that integrates with native mobile applications to protect against fraud targeting mobile device users. Especially pertinent in online banking and e-retail, this unique service detects malware and jailbroken devices and protects against keyloggers and fraudulent applications, while ensuring information intercepted by malicious programs will be rendered useless to an attacker.

Web Fraud Protection

WebSafe and MobileSafe deliver transparent web fraud protection to businesses. Their combined features shield customer data, reduce fraud loss, and strengthen your security position while ensuring a seamless user experience.

Malware and fraud detecting

WebSafe applies advanced identification techniques that enable your organization to recognize infected users and sophisticated malware patterns, including MITB, injections of malicious script, or attempted automated transfers. MobileSafe allows you to verify SSL certificates, detect MITM malware, and identify mobile app modifications. These solutions help your organization understand the full scope of threats and ensure protection.

Advanced phishing detection

WebSafe provides advanced and preemptive phishing detection capabilities that help your organization to identify attacks before mass emails are communicated. WebSafe detects and alerts the organization when the phishing site has been loaded to a spoofed domain. WebSafe also identifies the attacker and referrer, as well as other critical details, and reports this back to the organization.

Application-level encryption

Advanced application-level encryption protects all sensitive information transferred from users to organizations and renders any data intercepted by an attacker worthless. The encryption protects account information that may become compromised prior to SSL encryption while data is in use within the browser or mobile application.

Transaction protection

WebSafe performs a series of transaction checks, including iFrame checks, behavioral analysis, signature and function verification, and more. WebSafe then assigns a risk score to each transaction based on its likelihood of being fraudulent.

Device and behavior analysis

WebSafe is able to identify and prevent automated payments and money transfers initiated by malware or bots by assessing a variety of device-specific and behavioral variables, which together are designed to distinguish human users from automated scripts or bots.

Jailbroken or rooted device detection

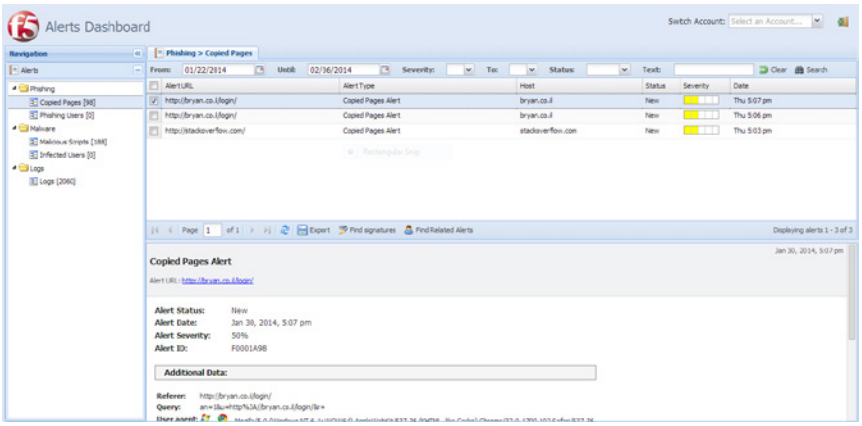
MobileSafe uses a variety of checks to identify security issues—such as outdated operating system versions or signs indicating that the application has been cracked—and then assigns a risk score to devices. Jailbroken or at-risk devices allow users to easily download software from unverified sources—and may contain malware. MobileSafe also detects transactions originating from at-risk mobile devices to thwart Zeus, Citadel, and other popular malware families that are easily integrated into cracked applications and used to obtain the victim's one-time password (OTP), redirect SMS messages, and log information submitted by the user.

User and application transparency

WebSafe and MobileSafe uniquely enable fraud detection and protection without modifications to applications or client-side installations. The fraud protection solution allows you to secure from online threats without changing the user experience or introducing complexities into application code, ensuring full transparency and greater efficiency in deployment.

A Security Operations Center

F5 has created a state-of-the-art Security Operations Center (SOC) that monitors global attack activities, notifies administrators of threats, and shuts down phishing proxies or drop zones to minimize impact to businesses. The SOC houses an experienced team of security researchers and analysts who investigate new attacks throughout the world, researching malware and drop zones and maintaining up-to-date information on the latest malware, zero-day, and phishing attacks. The center serves as an extension of your security team, keeping you aware of new attacks that might potentially become an immediate threat to your organization. The SOC has been responsible for discovering a variety of noted threats, such as Eurograbber and several key zero-day attacks, and it works closely with law enforcement in several countries.



The web anti-fraud dashboard allows users to monitor attacks targeting their organization in real time.

Accelerated protection starting tomorrow

With WebSafe and MobileSafe, you can begin protecting your entire user base from online threats in days instead of weeks. Seamlessly integrated with the F5 BIG-IP® platform, the world's leading Application Delivery Controller, WebSafe reduces time-to-production by eliminating any need for application development. WebSafe services can be easily configured and managed from the BIG-IP UI. This integration allows you to quickly define anti-fraud profiles, enable or disable fraud protection services, configure alert servers, and report on all protected URIs from a familiar interface. As a service on the BIG-IP platform, WebSafe enables management of all aspects of security and fraud from within the network security team. It can be configured and tuned by your network or security specialist in hours, with updates installed in minutes and without downtime. MobileSafe is a software development kit (SDK) that seamlessly integrates with native mobile applications.

F5 iRules® can also be used to reduce time-to-production for WebSafe. A flexible, events-driven scripting language on the BIG-IP platform, iRules gives you the ability to architect application delivery solutions that improve the security, resiliency, and scale of applications in the data center.

F5 Global Services

F5 Global 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 Global Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/services.

More Information

To learn more about WebSafe and MobileSafe, visit f5.com.

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.