F5 WebSafe

DATASHEET

What's Inside

Protect Your Business and Customers from Online Fraud

Online services allow your company to have a global presence and to conveniently reach users wherever they may be. The future of your business is heavily weighted on your ability to ensure the integrity of your e-commerce site or website, and protect online customers against fraud and malicious activity.

F5® WebSafe™ delivers web fraud protection that safeguards banks, e-retailers, and other organizations exposed to online fraud. It protects online customers from a broad range of web fraud across all devices—without impacting the user experience. WebSafe helps organizations to achieve success in the fight against credential theft, web-based malware, and online fraud targeting web application users. Using unique and advanced capabilities that complement existing fraud prevention techniques and solutions, WebSafe gives your organization the ability to provide greater online fraud protection and make more informed overall security decisions that prevent account take overs, identity theft, and system breaches.

Key benefits

Guard against targeted and generic malware

Recognize and safeguard against sophisticated threats, including web injection, credential grabbing, man-in-the-browser (MITB), Remote Access Trojans (RATs), form loggers, password stealers, and more.

Preempt phishing attacks

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

Protect without client downloads

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

With WebSafe, companies can greatly reduce identity theft, account takeover, and fraudulent transactions. Advanced capabilities detect, alert, and protect against client-side targeted and generic malware, phishing attacks, and 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 client-side installations. With WebSafe, your organization gains advanced real-time protection against the theft of identity, intellectual property, sensitive data, and money.

Malware and fraud detecting

Using WebSafe, website owners identify and protect against financial malware, MITB, zero-day fraud, and other fraudulent online activities. WebSafe applies advanced identification techniques that enable your organization to recognize and be informed of sophisticated malware patterns. These patterns include injections of malicious script, attempted automated transfers, and RAT malware that gives attackers administrative control over a victim's computers. WebSafe draws out persistent variations of Zeus, Citadel, Carberp, and other sophisticated client-side malware types, and identifies infected users. Malware that steals credentials stored in browser memory or saved to clipboards can also be detected. WebSafe enables rapid response to zero-day events with custom user-defined alerts that filter client request data and alert on specific search findings—providing the most immediate coverage for identifying fraud attempts (or malware). These capabilities help your organization understand the full scope of threats and ensure protection.

Advanced phishing and pharming detection

Fraudsters today are dusting off and beefing up legacy tactics—such as phishing and pharming—to target online banking users' account information. WebSafe provides advanced and preemptive phishing and pharming detection capabilities that help your organization to identify attacks before mass emails are communicated. WebSafe detects and alerts the fraud team 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 and data protection

As credential theft rises, opening the door to substantial bank fraud and information theft, WebSafe helps to ensure those accessing your online services and applications are protected against identity theft. 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. It also employs form field obfuscation and other techniques to slow down attackers—preventing them from understanding the site and learning the type of information users are submitting (i.e., username, password, account number, etc.). In addition, WebSafe generates an alert when credentials stored in browser memory (or copied to a clipboard) are altered while the protected application is in use. Credential theft and data protection in WebSafe is 100 percent transparent, protecting information across all device types without changes to the app, client-side downloads, or end-user dependencies.

Advanced fraud protection

An effective fraud defense requires a multi-layered strategy that enables cross-correlation of fraud and security events, deep forensic analysis, and integration with the broader security infrastructure. The F5 BIG-IP® platform's security modules augment WebSafe capabilities with anti-DDoS and WAF protections. This enables the most accurate understanding of the full scope of threats institutions face—and helps thwart the broader aspect of sophisticated fraud exploits.

WebSafe easily integrates with third-party SIEMs, risk management, and logging systems for deeper analysis, compliance automation and assurance, and IT operational intelligence. Furthermore, WebSafe's advanced capabilities enable automated responses to all fraud threats. Fraud managers can configure policies triggered by specific fraud events and based upon score for effective event logging, temporary blocking of user access, or application traffic steering for in-depth analysis. WebSafe effectively frees up resources to focus on the most crucial fraud events, while ensuring every fraud alert is attended to.

Transaction protection

With each transaction executed and upon site login, WebSafe performs a series of transaction checks—including iFrame checks, behavioral analysis, signature and function verification, and more. The rich set of capabilities enables it to accurately distinguish legitimate transactions from those initiated by fraudsters in real time, and even malicious connections initiated from the same device. WebSafe assigns a risk score to each transaction based on its likelihood of being fraudulent. Alerts are generated against high-risk transactions, driving rapid response actions. WebSafe raises the bar on transaction protection, giving fraud teams real-time notice of malicious transaction attempts—including session hijacking, transaction cookie tampering, and transaction exploits that replace account numbers maintained in browser memory or saved to clipboards.

Device and behavior analysis

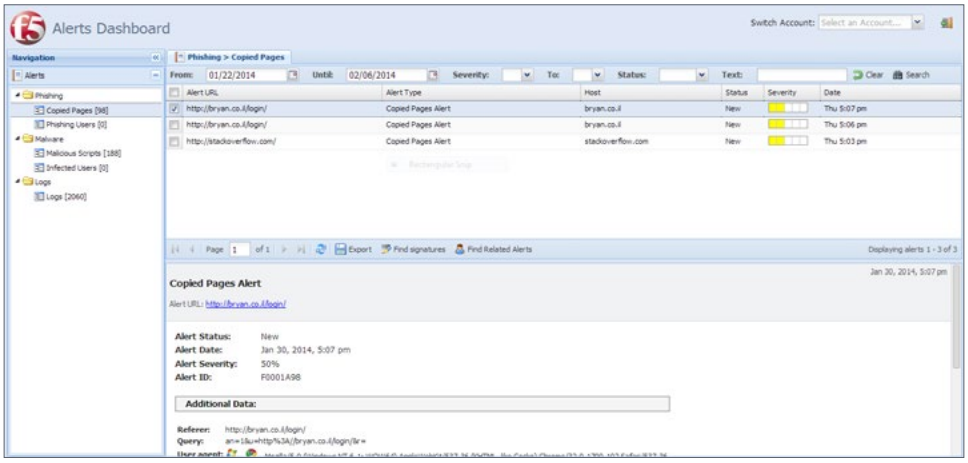
WebSafe is able to identify and prevent automated payments and money transfers initiated by malware or bots by assessing a variety of device-specific and behavioral variables, which together are designed to distinguish human users from automated scripts or bots.

User and application transparency

WebSafe uniquely enables fraud detection and protection without modifications to applications or client-side installations. The fraud protection solution allows you web fraud protection services and credential theft protections 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 Fraud Dashboard allows users to monitor attacks targeting their organization in real time.

FFIEC compliance

F5 Web Fraud Protection solutions help banks and other financial institutions maintain awareness of cybersecurity risks they are facing and respond rapidly to the increasing volume and sophistication of cyber threats. WebSafe and F5 MobileSafe® complement existing forensic, access management, and security solutions to provide a more in-depth, multilayered defense that helps minimize online credential theft and bank fraud. These solutions go beyond traditional fraud solutions to provide real-time visibility into the entire fraud landscape—with detailed intelligence that allows financial institutions to make informed risk management decisions and implement effective risk management practices. WebSafe integrates with the BIG-IP platform and F5 application protection solutions. This helps you ensure effective threat controls that protect not only credentials and account information, but your most critical banking applications and the application infrastructure. The combined solution identifies and helps prevent access by compromised devices, and automatically asserts control over networks and authentication, authorization, fraud detection, and response management processes.

Accelerated protection starting tomorrow

With WebSafe, you can begin protecting your entire user base from online threats in days instead of weeks. Seamlessly integrated with the industry-leading F5 BIG-IP® 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.

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/support.

More Information

To learn more about WebSafe, visit f5.com/websafe.

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.