F5 MobileSafe

DATASHEET

What's Inside

Protect Mobile Device Users from Online Fraud

Consumers prefer the convenience of engaging with institutions via smartphones or tablet devices. For this reason, mobile application services are essential for the future of online banking and financial services. With the increased sophistication in fraud threats and attacks, your institution's success depends on its ability to provide protections that bolster consumer confidence. Consumers who use mobile applications expect financial service institutions to take an active stance in preventing account fraud, and protecting against identity and cyber theft. The growth of your business depends on it.

F5® MobileSafe® helps your institution protect mobile device users from advanced cyber threats. MobileSafe delivers client-side safeguards that guard mobile application use in real-time—securing customer information and credentials, while helping to prevent identity theft and account takeovers.

Key benefits

Minimize fraud loss associated with mobile device usage

Identify fraud immediately and provide real-time protection for users of all mobile device types.

Improve mobile-app protections

Utilize MobileSafe's client-side financial fraud safeguards to provide another layer of protection that extends security services from the data center and across the transportation layer to the mobile device users.

Meet compliance standards

Effectively meet regulatory standards requiring reasonable security and confidentiality of customer information to protect against unauthorized account access.

Get 100% transparency and consumer coverage

Ensure methods are in place to help prevent threats for all mobile device users without relying upon consumer installations or changing the user experience, for 100 percent anti-fraud coverage and greater efficiency in deployment.

Drive immediate fraud response

Reduce the gap between fraud detection and action with 24/7 fraud security operations, monitoring services, and alert notifications.

F5 MobileSafe

F5 MobileSafe enables financial organizations to gain control over areas that were virtually indefensible until now—neutralizing local threats found on consumers' mobile devices, without altering the user experience in any way. MobileSafe is an SDK that integrates with any native mobile application to protect application users against attacks aimed at mobile devices. Commonly used for mobile e-commerce and banking applications, MobileSafe eliminates mobile-based identity theft and thwarts attacks by preventing mobile phishing, mTAN interception, and pharming attacks in real time. It detects mobile malware, identifies rooted devices, and ensures information intercepted by malicious programs will be rendered useless to an attacker. MobileSafe can run standalone or in combination with F5 WebSafe™ for more comprehensive protection for all online banking consumers.

Client-side mobile threat protection

With MobileSafe, your institution is equipped to protect against sophisticated client-side mobile threats that seek to gain trusted access to information and execute fraudulent transactions on behalf of mobile device users. MobileSafe provides a toolbox of capabilities that help prevent man-in-the-middle (MitM) exploits, DNS spoofing, and certificate forging. It detects and alerts fraud teams of a wide range of mobile device-based malware variants —including keyloggers, focus stealing, SMS grabbers, bank trojans, and bots—for all device types including the most prominent iOS or Android devices. MobileSafe helps to identify unauthorized mobile application modifications and includes expert malware research and analysis services that provide administrators with up-to-the-minute knowledge of threats to respond more effectively to cybercrime.

Rooted/Jailbroken device detection

MobileSafe protects against jailbroken or at-risk devices that allow attackers to easily download and run software from unverified sources executing malware. MobileSafe executes a variety of checks on each end-user device to expose rooted devices and sends an alert for each suspect device detected. MobileSafe also adjusts the safety score for transactions originating from at-risk mobile devices to thwart Zeus, Citadel, and other malware families that are easily integrated into cracked applications and used to obtain the victim's OTP, redirect SMS messages, and log information submitted by customers.

Application-level encryption

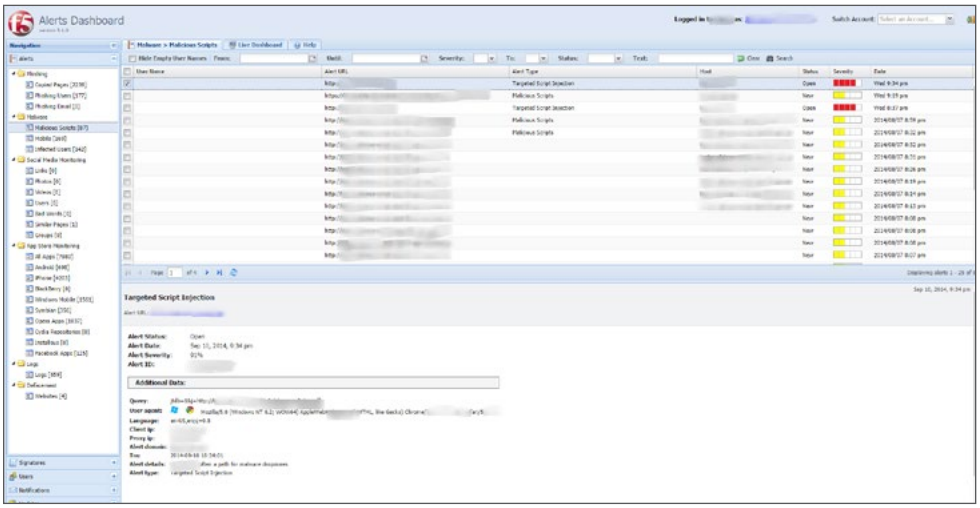
Advanced application-level encryption secures all sensitive information at the point of capture and renders any data intercepted by an attacker worthless. The unique encryption method protects exposed information within the browser that may become compromised prior to SSL encryption. MobileSafe layer 7 encryption seals exposed data to prevent the success of keylogging/formlogging and ensures protection even where the SSL tunnel may be fraudulently terminated on the device to expose the data within. With application-level encryption, MobileSafe renders mobile device traffic-sniffing malware useless and protects data in a more fine-grained way than is possible with traditional forms of encryption alone.

Real-time alerts and threat visibility

MobileSafe provides complete visibility into threats targeting mobile application users. Real-time alerts are generated on suspicion of threat and detection of malware, or malicious activities enabling more immediate action to be taken. Alerts can be communicated by phone, text message, email, the SIEM console, and the F5 Web Fraud Dashboard. The

dashboard provides a consolidated view into the threat landscape for each mobile app URL. It also lists all threats and attacks identified over a period of time and provides details including the threat type, level of risk, and source. Unique client device identifiers including phone number, locations information, and other details about end-user devices accessing protected mobile apps can also be included with each alert generated and captured in the dashboard.* This strengthens alert reporting and enables more effective risk engine support and behavioral analysis. Hosted by the F5 Security Operations Center, the dashboard is easily accessed from any browser, enabling real-time monitoring of all threats targeting your organization—from identification to intelligence and remediation. You'll also receive real-time alerts through email and SMS.

*Device identification data points considered protected by law can be strickened (made anonymous) within alerts to comply with local or national laws.



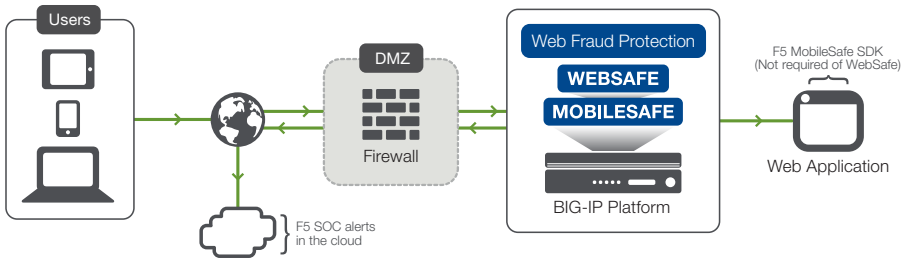
The Web Fraud Dashboard allows users to monitor attacks targeting their organization in real time.

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. Working closely with law enforcement and third-party agencies and organizations throughout the world, the SOC has been responsible for discovering a variety of noted threats, such as Eurograbber and several key zero-day attacks. 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 SOC serves as an extension of your security team, keeping you aware of new attacks that might potentially become an immediate threat to your organization.

F5 Web Fraud Protection

MobileSafe is a component of the F5 Web Fraud Protection solution, which is designed to safeguard banks, e-retailers, and other organizations (along with their online customers). MobileSafe protects organizations from a broad array of online and mobile fraud across all devices—without impacting the user experience. Fully integrated as a core component of the BIG-IP platform, F5 Web Fraud Protection and application protection solutions combine to provide the coverage financial services institutions and others need to effectively defend against online theft and fraud loss.



F5 Web Fraud Protection solutions offered as component of the BIG-IP platform with 24x7 F5 SOC support.

Supported operating systems

MobileSafe provides protections for devices that run either of the following operating systems:

- iOS
- Android

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.

DevCentral

The F5 DevCentral™ user community of more than 200,000 members is your source for the best technical documentation, discussion forums, blogs, media, and more related to Application Delivery Networking.

More Information

To learn more about F5 MobileSafe, visit f5.com.

Solutions for
an application world.