Web Fraud Protection

Luboš Klokner
Sr. Systems Engineer | F5 Networks

20/11/19 cz

Agenda

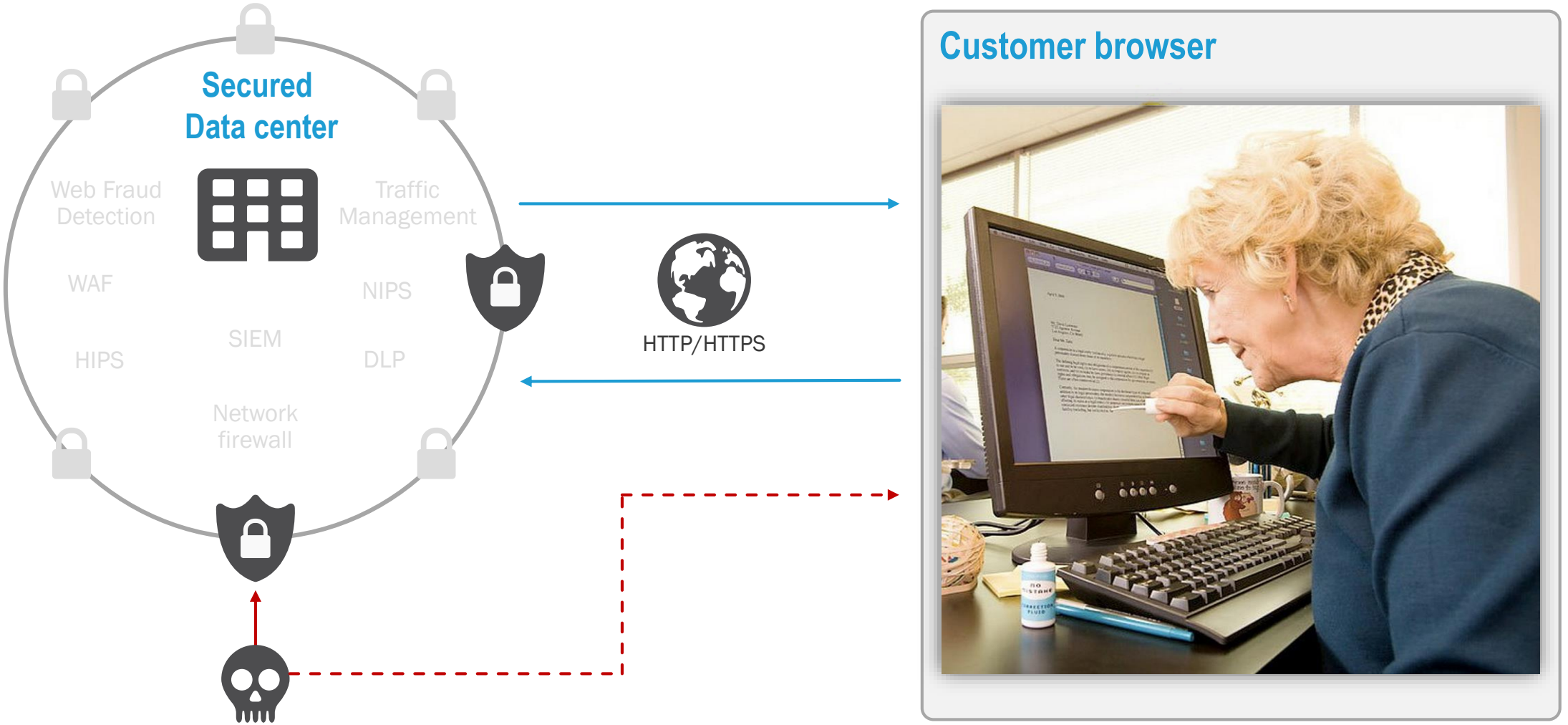
F5 Web Fraud Protection

- Trends
- Unique features
- General overview
- Features in detail

Questions

User is the Weakest Link

END POINT RISKS TO “DATA IN USE”



Protecting against online fraud

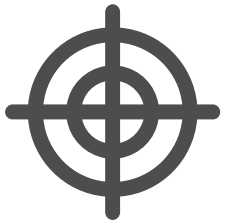
with 

Anti-fraud, Anti-phishing, Anti-malware services

KEY FEATURES

Prevent Fraud

Targeted malware, MITB, zero-days, MITM, phishing, automated transactions…

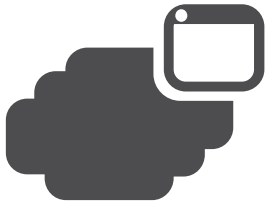


Protect Online User

Clientless solution, enabling 100% coverage. Desktop, tablets & mobile devices

Full Transparency

No software or user involvement required. No IB software modification



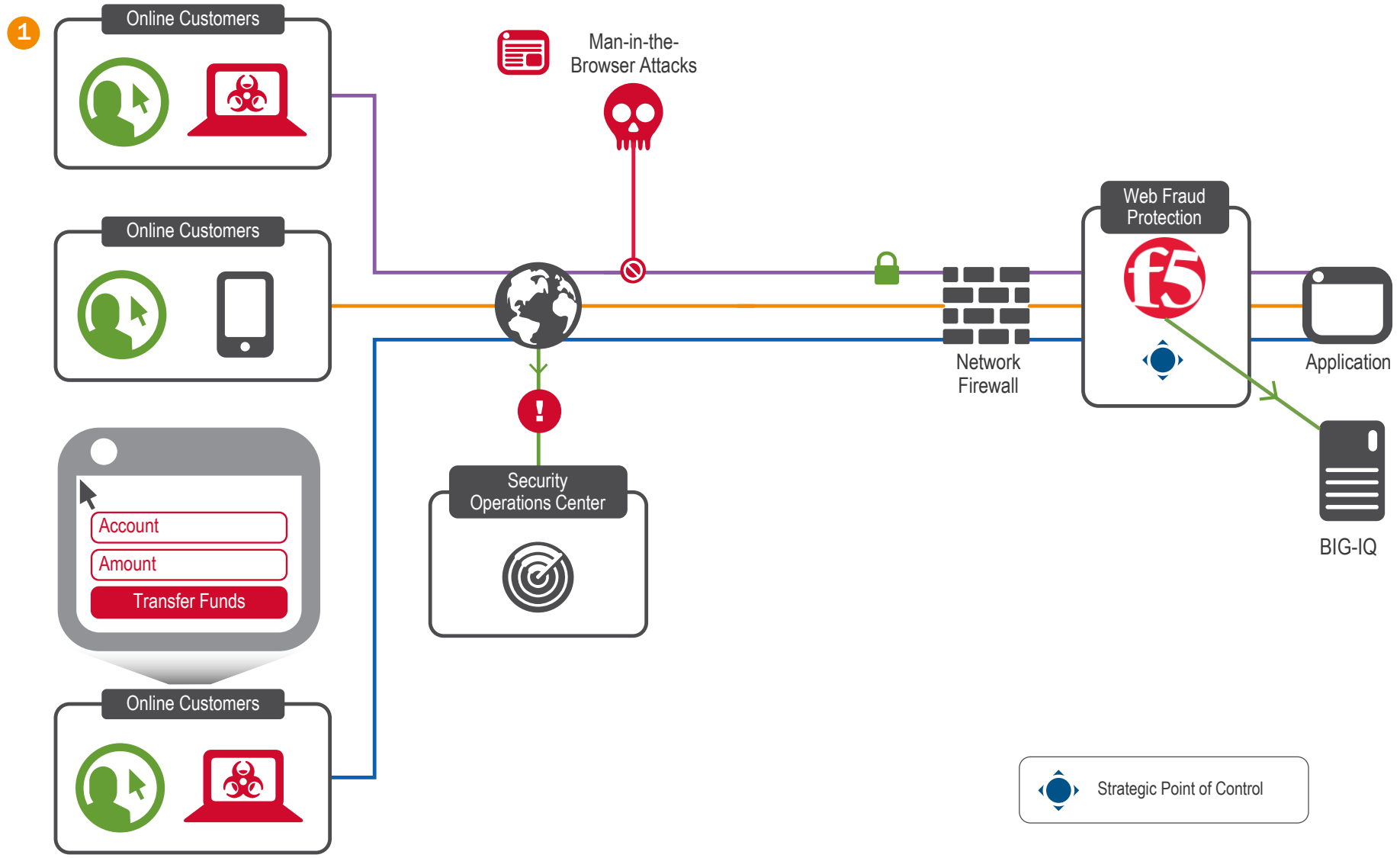
In Real Time

Alerts and customizable rules. Local and Cloud Dashboard

F5 Web Fraud Protection

KEY CUSTOMER SCENARIOS

1. Malware Detection and protection



Malware

CLIENTLESS GENERIC AND TARGETED MALWARE DETECTION

With real-time analysis and a variety of checks WebSafe identifies compromised sessions, malicious scripts, phishing attacks and malware including MitM/B, Bots, fraudulent transactions

Analyzes browser for traces of common malware

Malware

CLIENTLESS GENERIC AND TARGETED MALWARE DETECTION

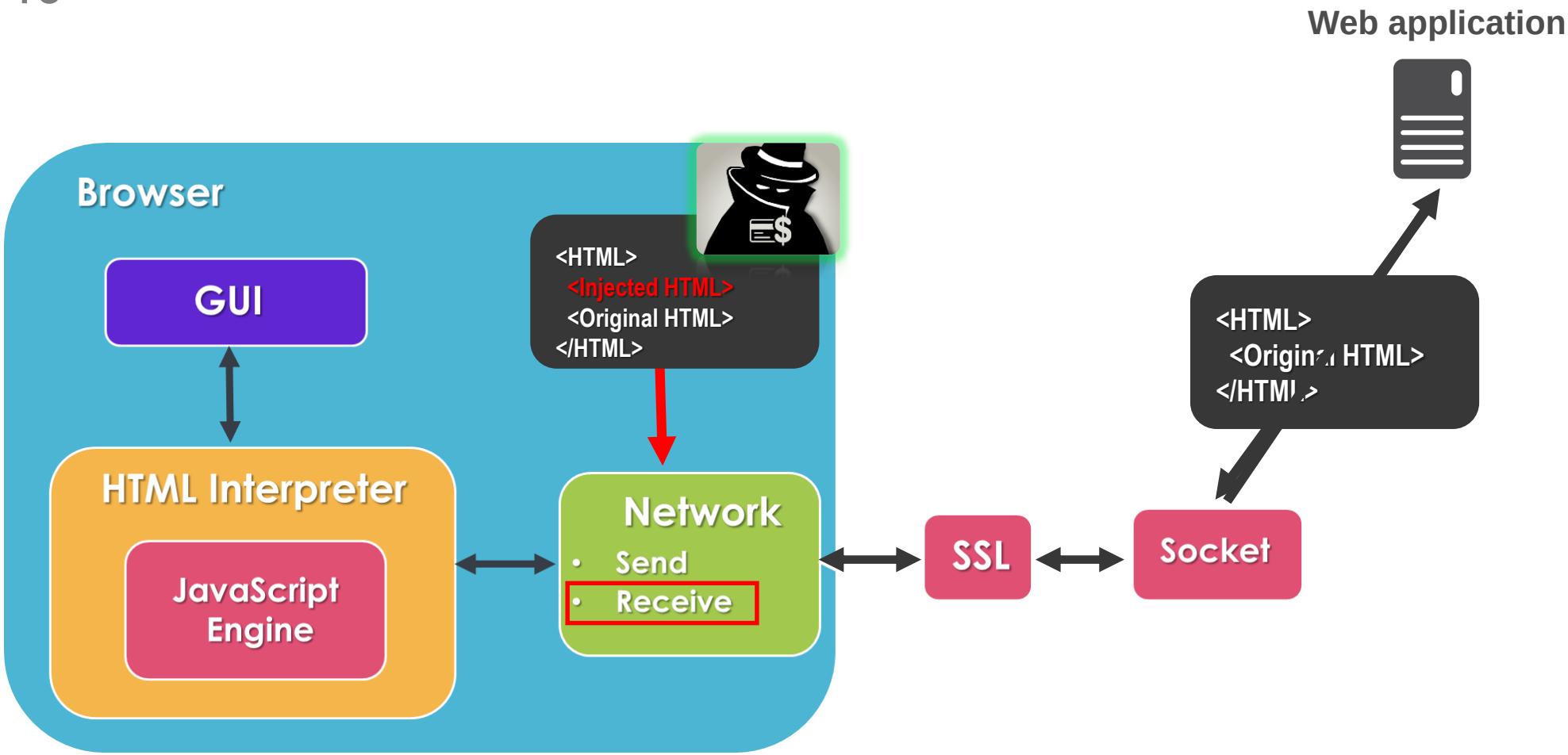
Identifies the presence of Remote Access Trojans (RATs)

Detects browser redressing

Performs checks on domain and other components

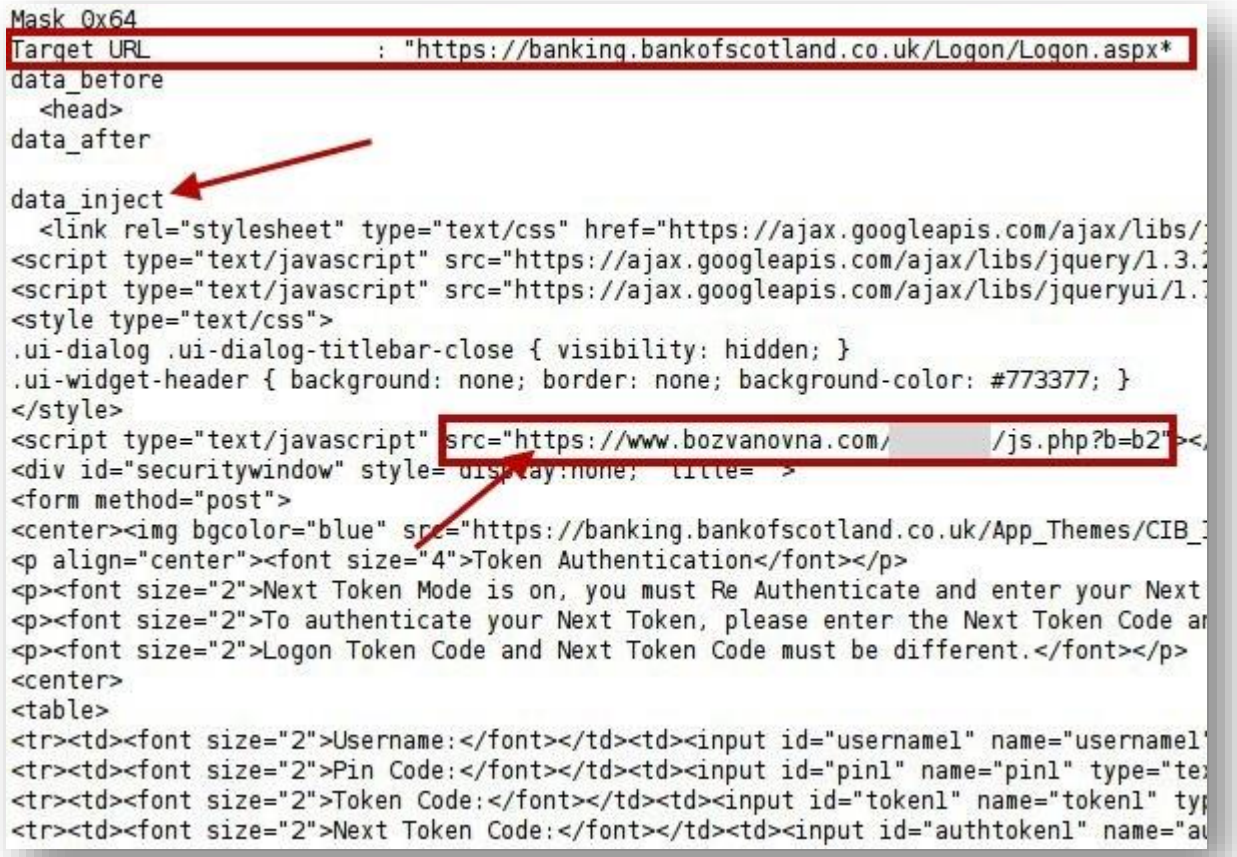
Webinjection

HOW TO



Webinjection

CONFIGURATION EXAMPLE



Malware

REMOTE ACCESS TROJANS

Identifies malware initiated RAT connection

Detects simultaneous connections on same device

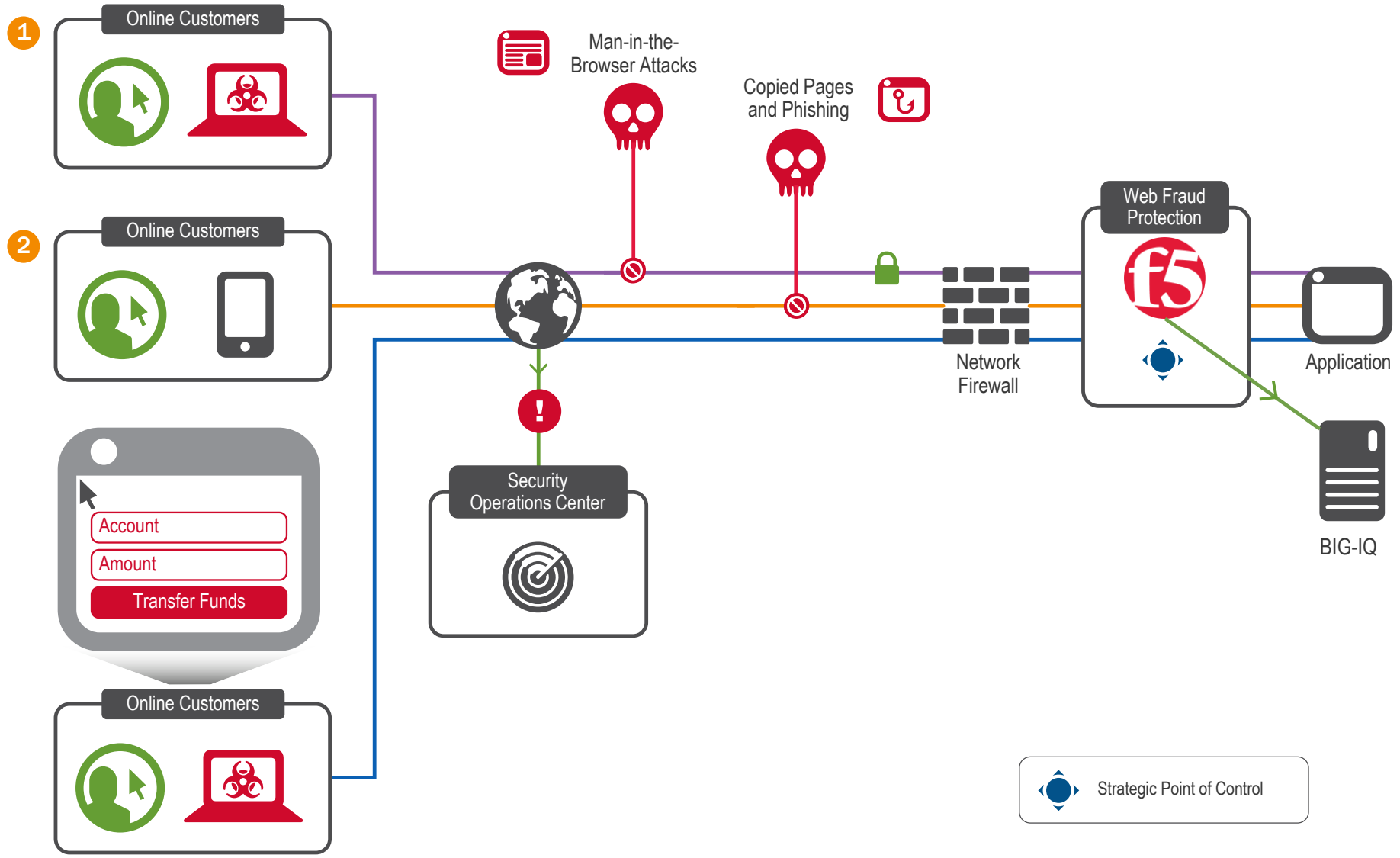
Differentiates between legitimate and fraudulent transactions on the same device

Delivers highly accurate detection with zero false positives

F5 Web Fraud Protection

KEY CUSTOMER SCENARIOS

1. Malware Detection and protection
2. Anti-phishing



Advanced Phishing attacks

ALERTS AT EACH STAGE OF PHISHING SITE DEVELOPMENT

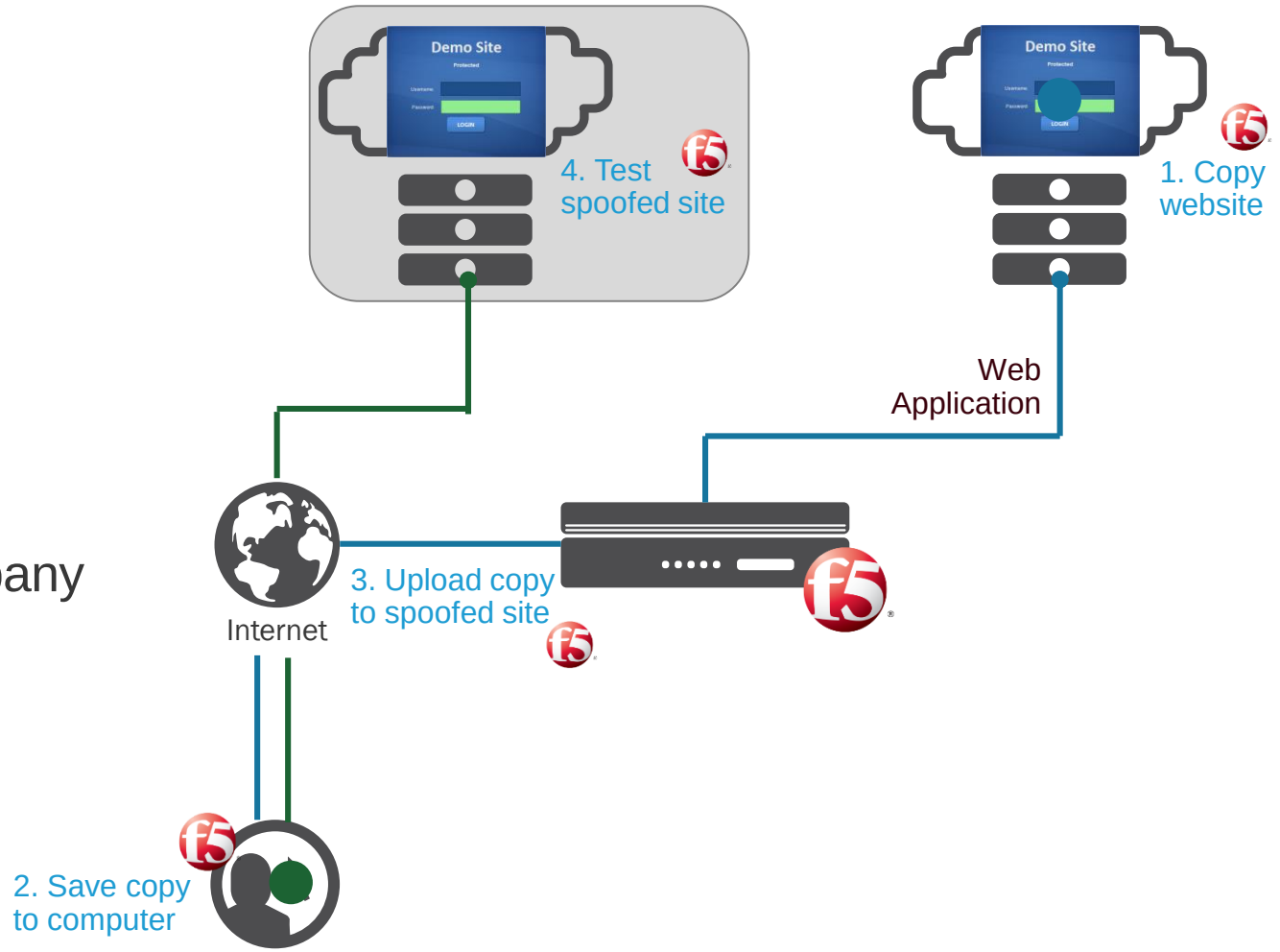
Identifies phishing threats early-on and stops attacks before emails are sent

Alerts of extensive site copying or scanning

Alerts on uploads to a hosting server or company

Alerts upon login and testing of phishing site

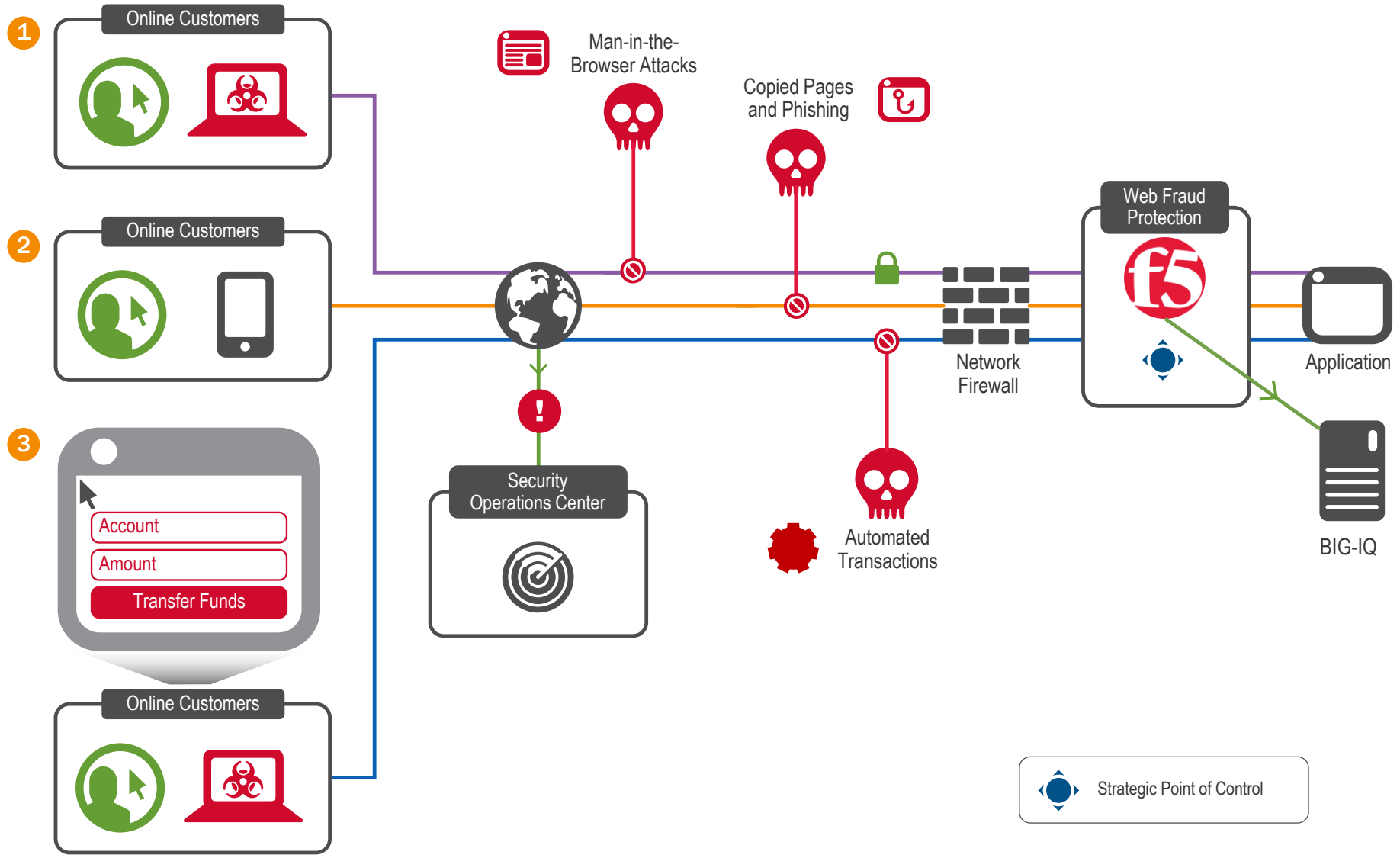
Shuts down identified phishing server sites during testing



F5 Web Fraud Protection

KEY CUSTOMER SCENARIOS

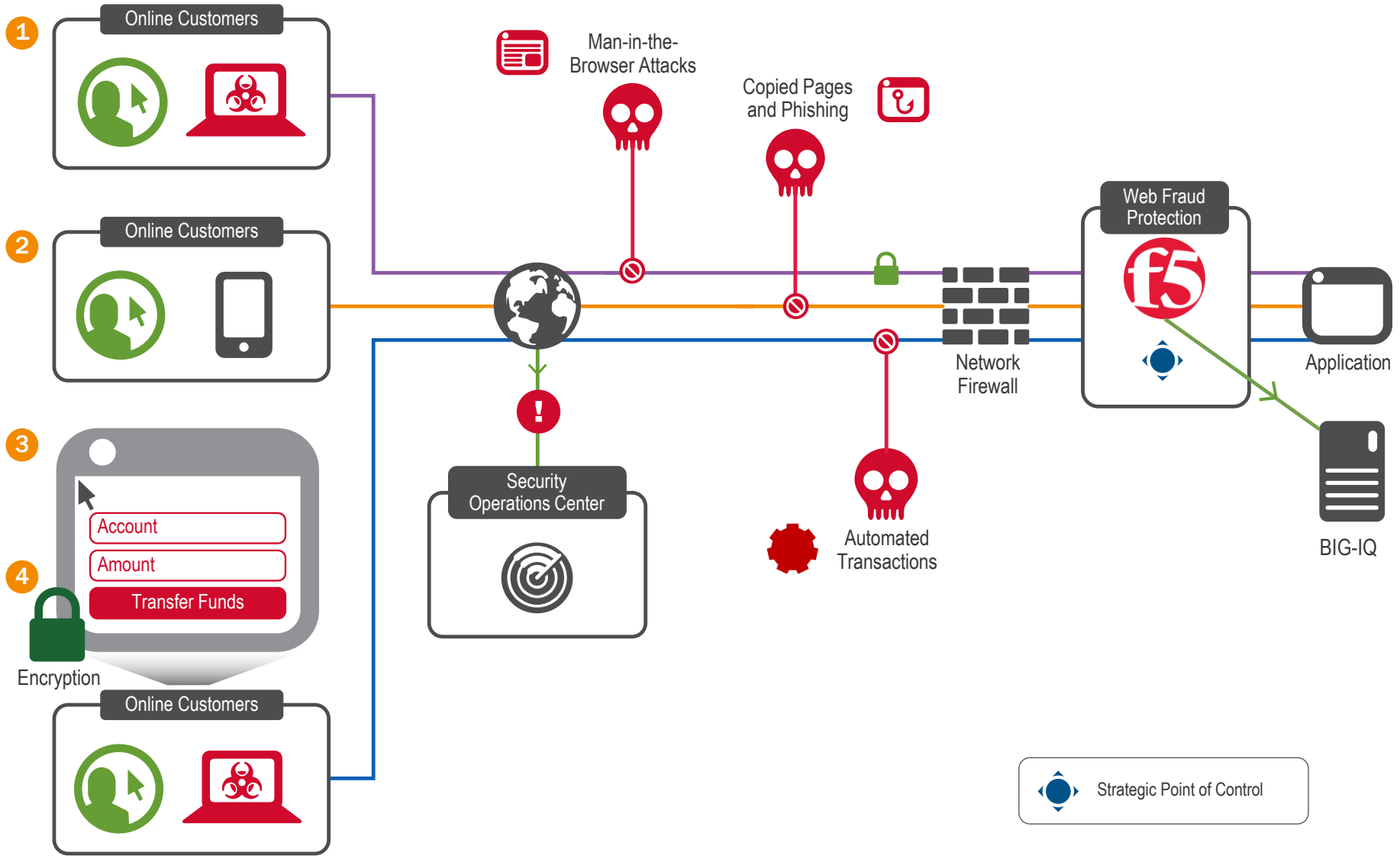
1. Malware Detection and protection
2. Anti-phishing
3. Stopping Automated transactions



F5 Web Fraud Protection

KEY CUSTOMER SCENARIOS

1. Malware Detection and protection
2. Anti-phishing
3. Stopping Automated transactions
4. Sensitive data encryption



Advanced application-layer protection

ENCRYPTION AS YOU TYPE

Sensitive information can be encrypted at the message level

Encrypted credentials and information is encrypted with public key

Data is decrypted by WebSafe on BIG-IP hardware using a private key

Intercepted information rendered useless to attackers

HTML Field Obfuscation (HFO)

Uses advanced HFO techniques to go beyond encrypting field values on the client.

Protects against malicious scripts that seek out form elements before HFO runs.

Adds fake form fields to further confuse attackers.

Dynamically changes field names on a frequent interval.

MobileSafe

ANTI-FRAUD PROTECTION FOR MOBILE DEVICE USERS

Mobile site Phishing detection

Advanced M-malware detection capabilities

Validates DNS and SSL certificate

Preforms app signature checks to identify application tampering

Flags obsolete or vulnerable device OS and sends score

Discovers rooted/jailbroken devices using several techniques

F5 Alerts Dashboard

BIG-IQ CENTRALIZED MANAGEMENT

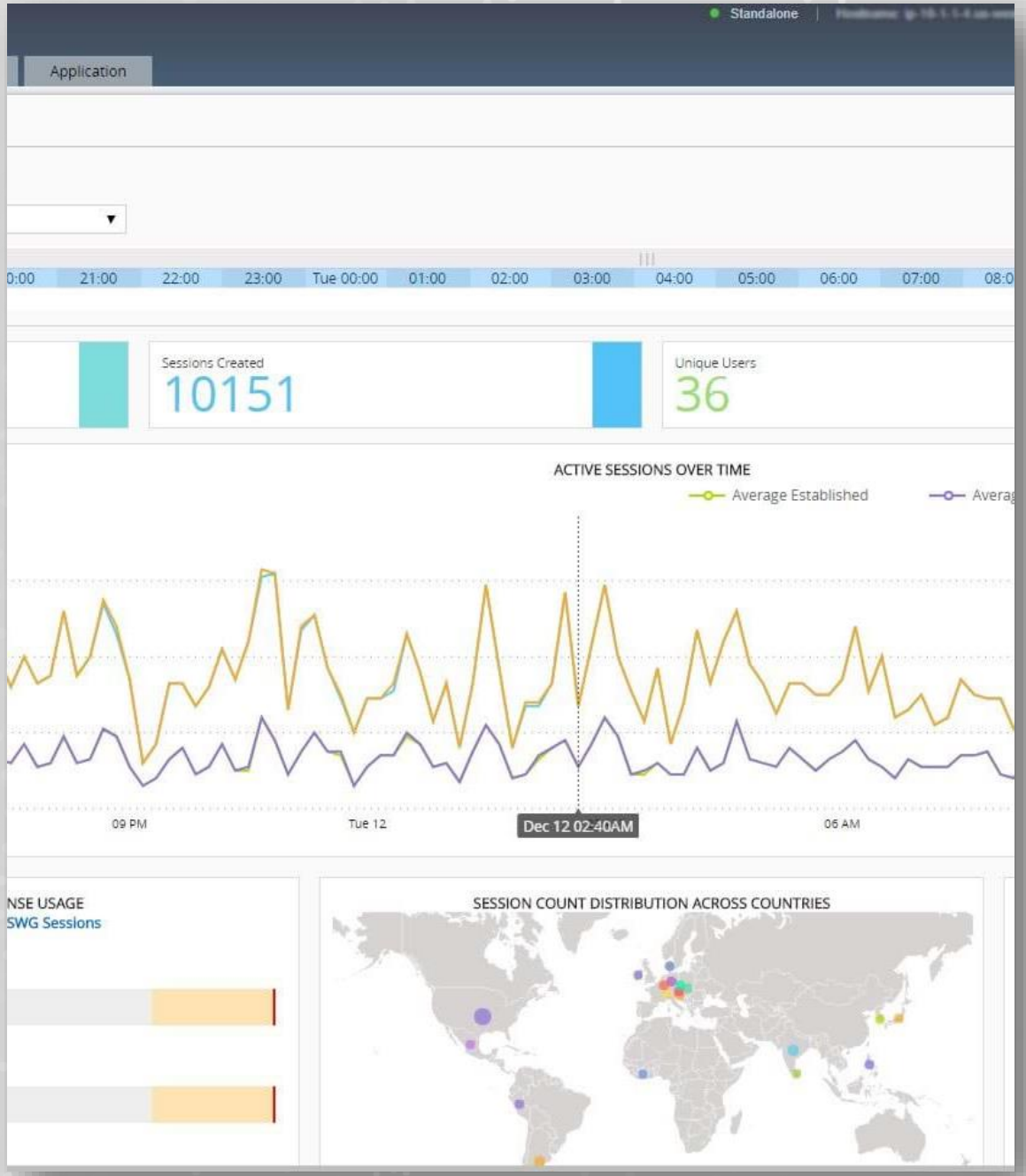
Easy view and track all fraud alerts including infected devices, malware, phishing and more

Forwards alerts to Syslog, Web Services and SMS Service Providers

Feeds additional fraud detection and risk systems automatically

Filters and finds events by time, username, severity or status

Can live in the cloud or on-premises



Live Signatures and Engine updates

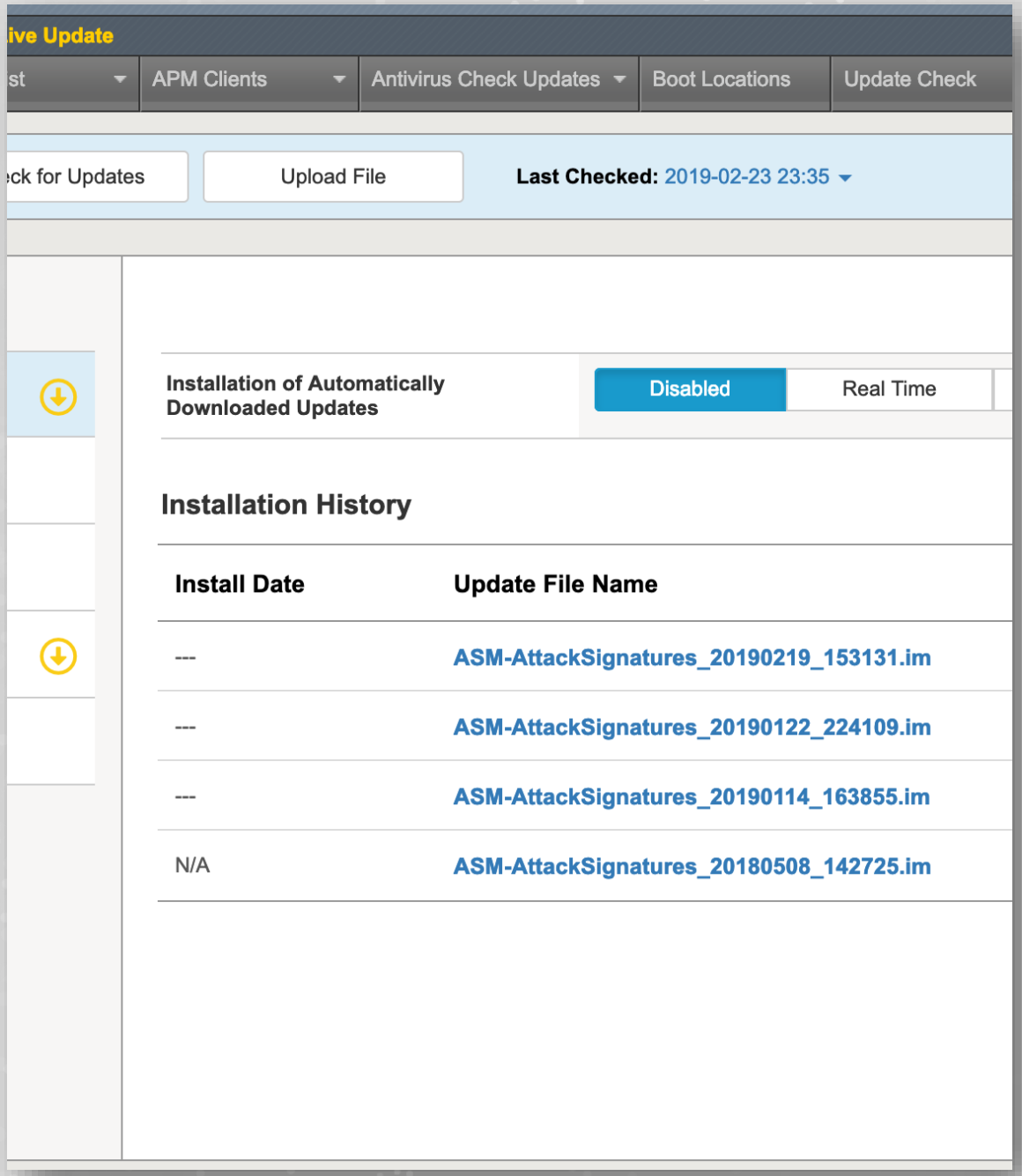
Receive alerts of available updates

Enable automatic updates, set specific times or update manually

Check version and the date of last update server connection

Signature updates are effective immediately and w/o service interruption

Updates are always backward compatible



F5 Security Operations Center

F5 Security Operations Center (SOC)

24x7x365 fraud analysis team that extends your security team

Researches and investigates new global fraud technology & schemes

Detailed incident reports

Continuous product component checks

Real-time alerts activated by phone, sms and email

Optional site take-down: Phishing sites

Phishing or brand-abuse sites

F5 SOC: Phishing site take-down service

Complete attack assessment & post-partum attack report

Leverage relationships with ISPs, anti-phishing groups and key international agencies

Malicious site take-down in minimal time

Recommendations for counter security measures

F5 SOC: Cyber intelligence

Sources information from a variety of resources

Analyzes malware files and researches dope zones

Provides quarterly dedicated reports

Delivers the right information: identify attacker's, C&C, drop zones, mule accounts, compromised users, and more...

Identifies social network scheming, sophisticated online fraud and brand abuse