Protegiendo a las Instituciones Financieras y sus Usuarios del Fraude Informático

Alejandro Dutto

Sr. Mgr, Field Systems Engineering – Latin America & Caribbean

alejandro@f5.com

Fraud and malware remains a challenge

Malware/Fraud Statistics

15% increase in malware,

- MC Afee threat report 2014

196 Million Unique malware samples in 2013,

- MC Afee threat report 2014

70% of malware targeting financial services companies

Mobile Malware (MM)

22,750 new modifications of malicious programs target mobile devices throughout the year

99% of newly discovered MM attacks target Android devices

Phishing attacks

37.3 million users around the world were subjected to phishing attacks 2013-2014

72,758 unique phishing attacks recorded in 1st half 2014 (WW)

Data sources include Symantec , Microsoft, Kaspersky, MacAfee, DarkReading, Gartner and Cybersource

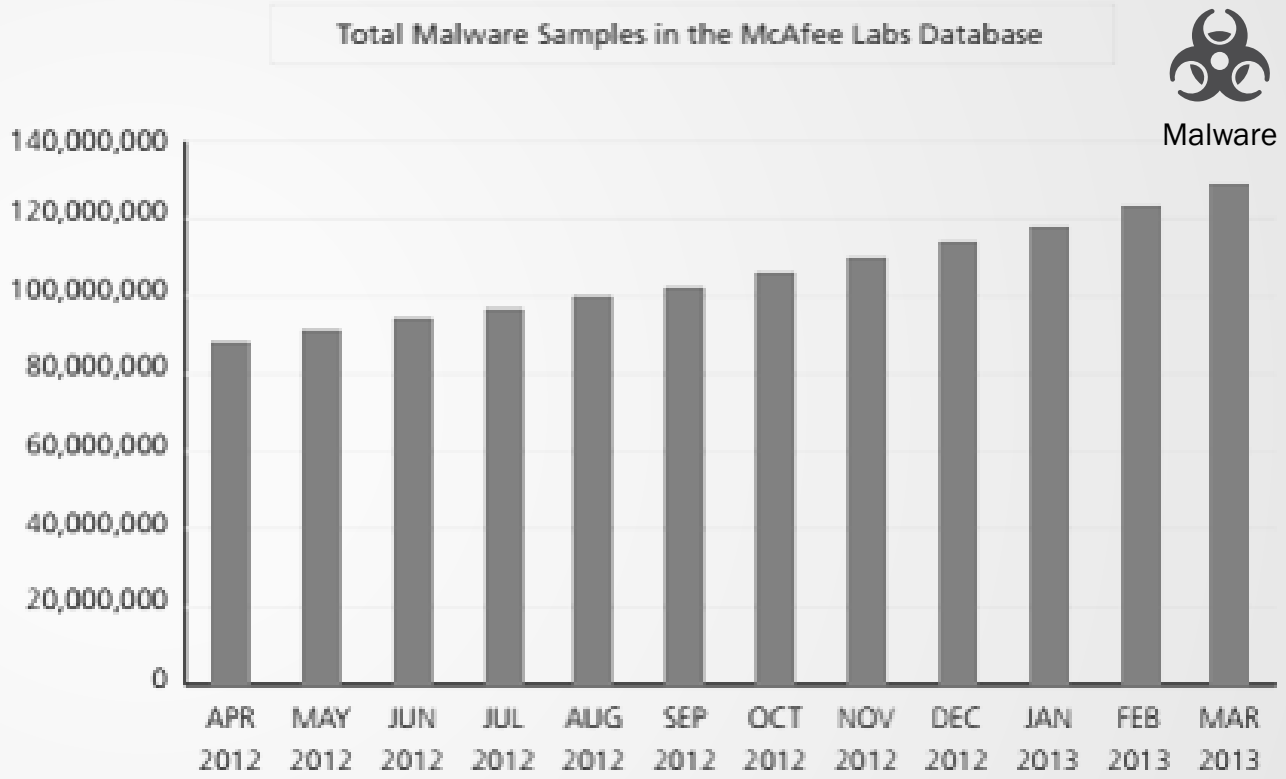
Malware Threat Landscape – Growth and Targets

25% Of real-world malware is caught by anti-virus

50% Of malware code is logic to bypass defenses

79% Existing malware strains are Trojans

82% Of Institutions learned about fraud incidents from their customers



Data sources: Dark Reading, PandaLabs, & ISMG

Securing against banking fraud can be complex

Ownership

Customers expect the banks to secure against all forms of fraud regardless of devices used or actions taken

Browser is the weakest link

Trojans, MITB attack the client browser or device where the bank has no security footprint

Changing threats

increasing in complexity requiring full threat reconnaissance

Attack visibility

Is often lacking details to truly track and identify attacks and their source

Compliance

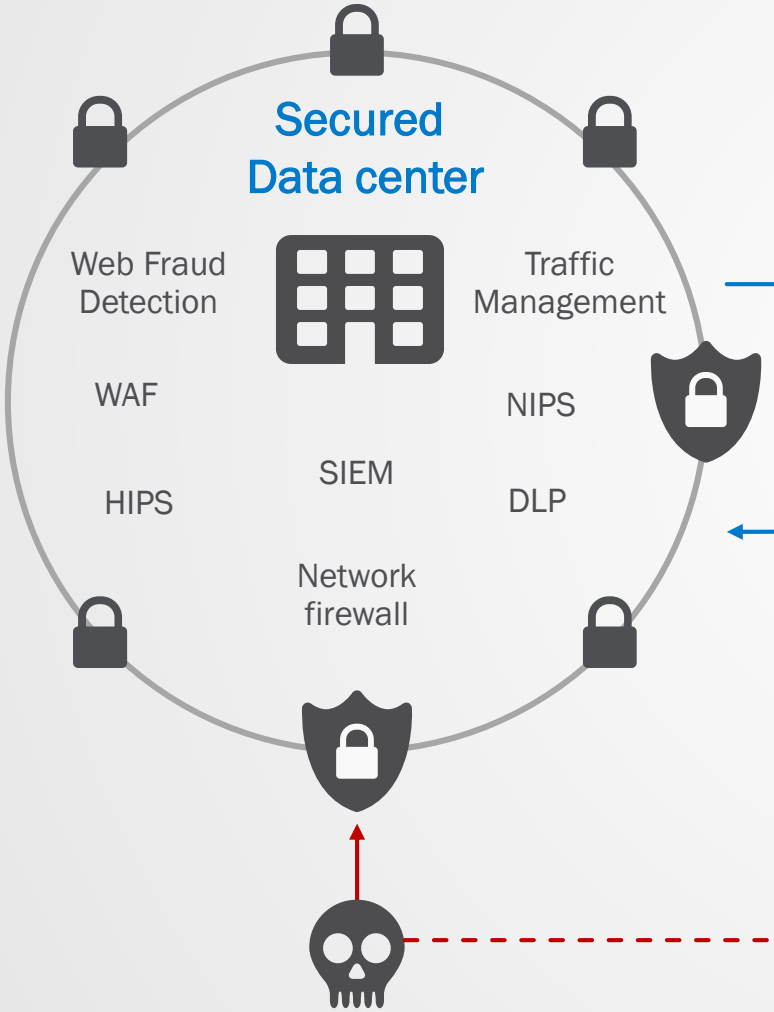
Ensuring compliance with regulations and FFEIC requirements

Endless customer Devices

desktop, laptop, tablet, phone, internet café, game consoles, smart TVs

Browser is the weakest Link

End point risks to “Data In Use”



HTTP/HTTPS

Customer browser

Leveraging Browser application behavior

- Caching content, disk cookies, history
- Add-ons, Plug-ins

Manipulating user actions:

- Social engineering
- Weak browser settings
- Malicious data theft
- Inadvertent data loss

Embedding malware:

- Keyloggers
- Framegrabbers
- Data miners
- MITB / MITM
- Phishers / Pharmers

Protecting against online fraud with F5

Anti-fraud, Anti phishing, Anti- malware services

Prevent Fraud

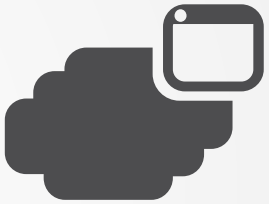
Targeted malware, MITB, zero-days, MITM, phishing automated transactions…

Protect Online User

Clientless solution, enabling 100% coverage

On All Devices

Desktop, tablets & mobile devices



Full Transparency

No software or user involvement required

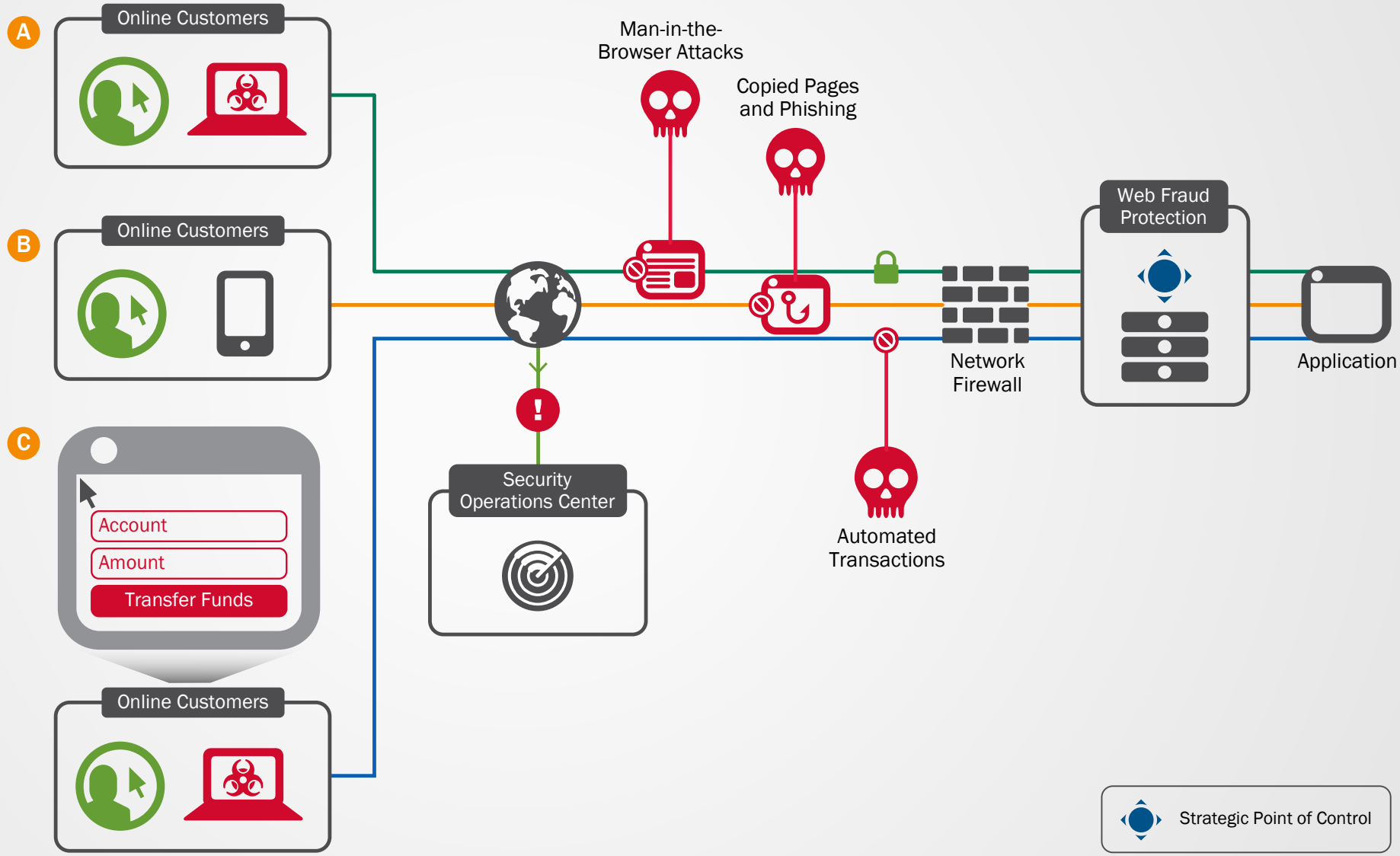
In Real Time

Alerts and customizable rules

Web Fraud Protection With F5

KEY CUSTOMER SCENARIOS

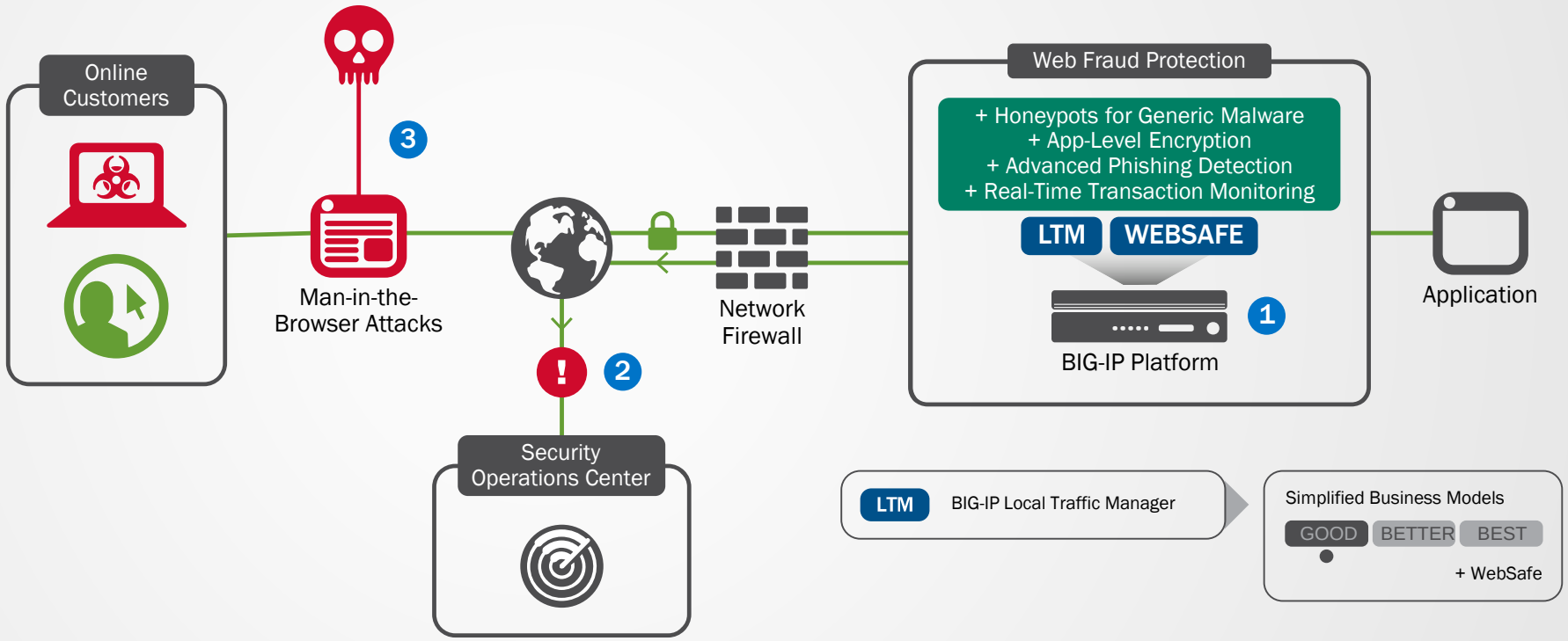
1. Malware Detection and protection
2. Anti-phishing
3. Stopping Automated transactions



Malware Detection and Protection

HOW IT WORKS

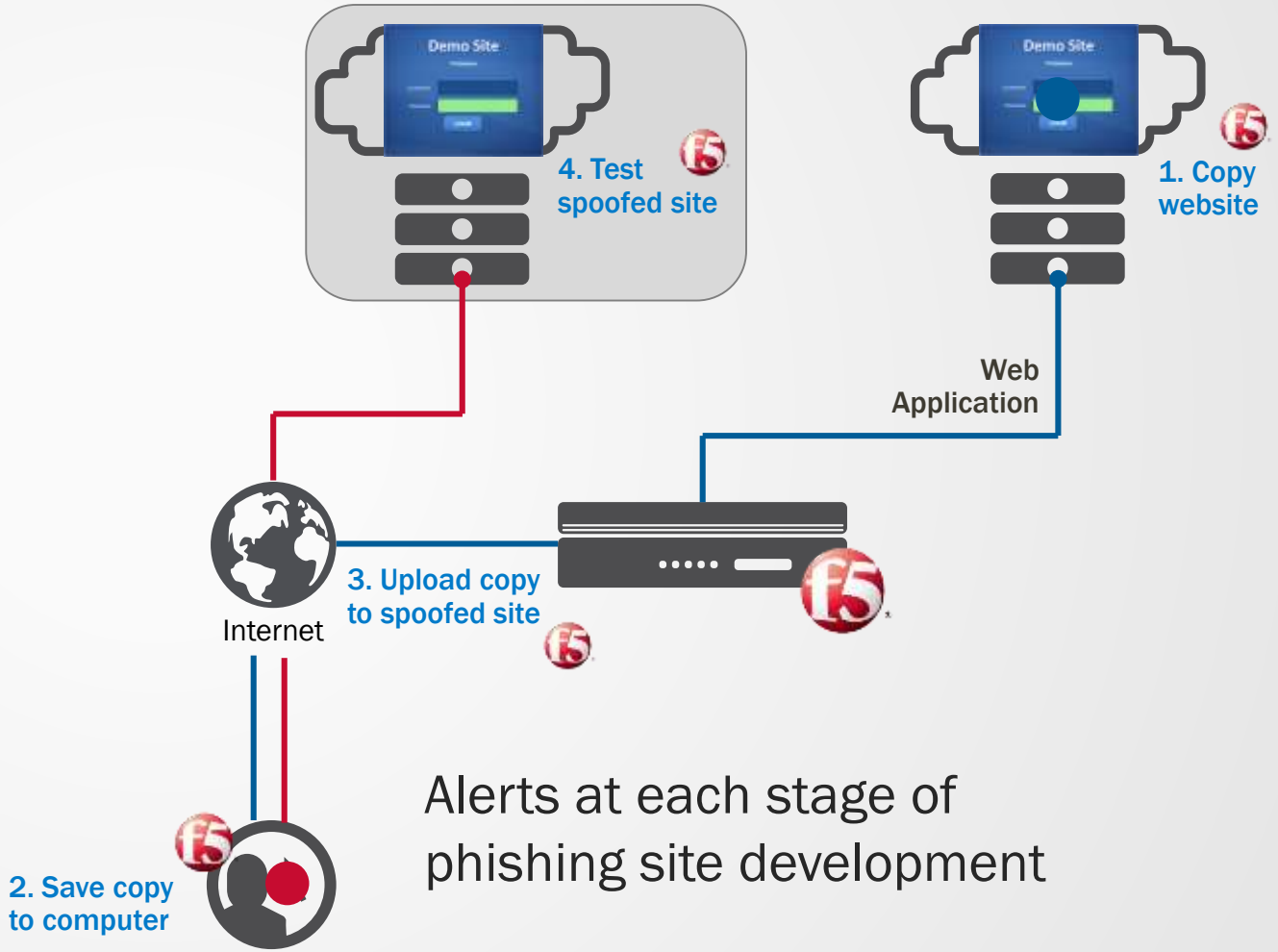
1. Malware detection component assesses user device ID, checks SSL
2. Validity, and ensures HTTPS connection is secure
3. Any anomalies trigger an alert. Encryption component renders any stolen data worthless to an attacker



Advanced phishing attack detection and prevention

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

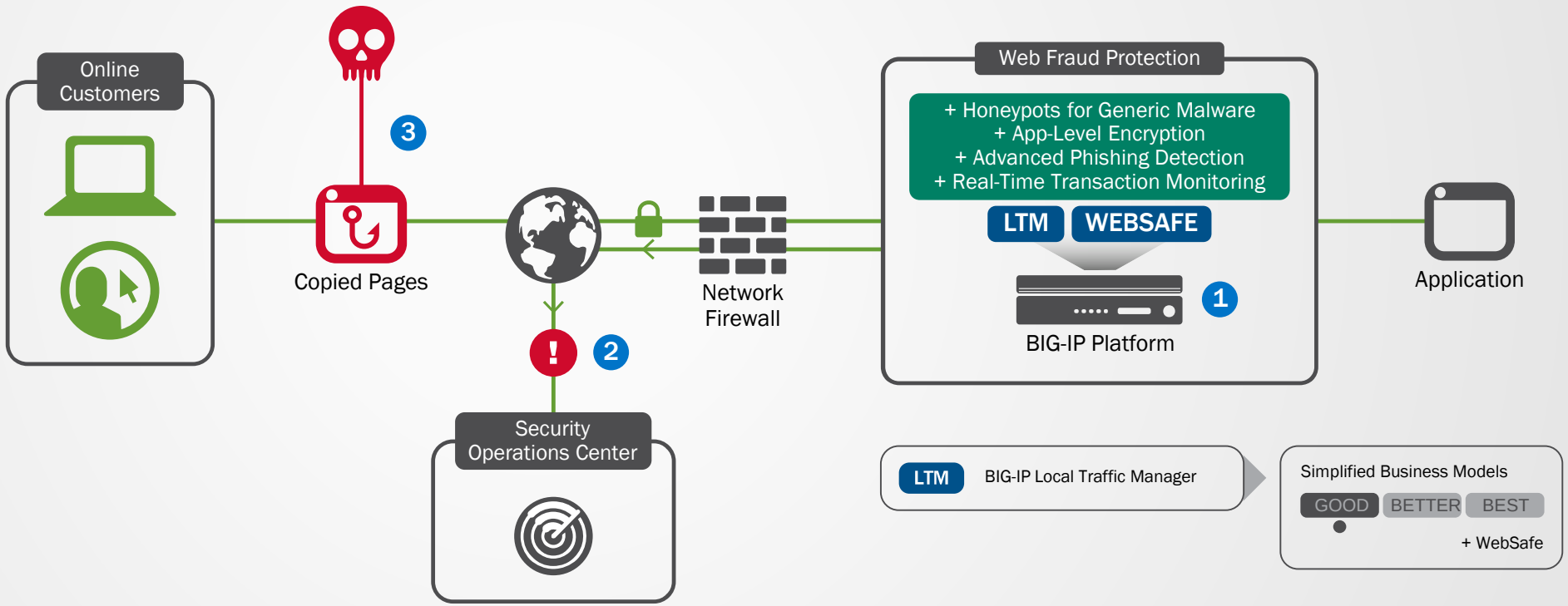


Alerts at each stage of phishing site development

Protection from Spear Phishing

HOW IT WORKS

1. Phishing detection component detects copying and uploading of web pages
2. An alert is issued
3. Attacker's IP address, drop zones, and any compromised credentials are identified



Advanced application-layer encryption

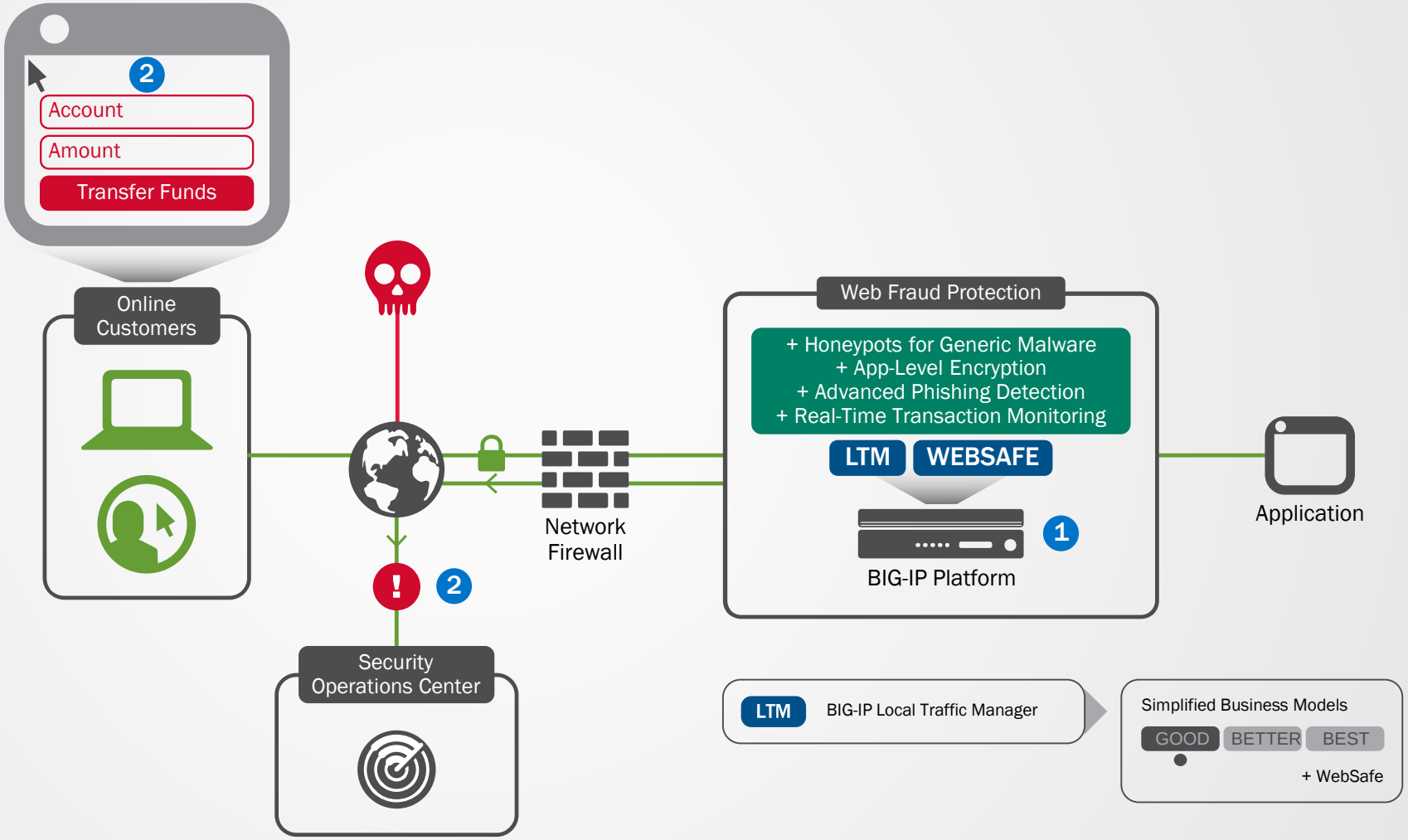
F5 secures credentials and other valuable data submitted on webforms.

- Any sensitive information can be encrypted at the message level
- User credentials & information is encrypted then submitted
- Data is decrypted using WebSafe on BIG-IP hardware
- Intercepted information rendered useless to MiTM attacker

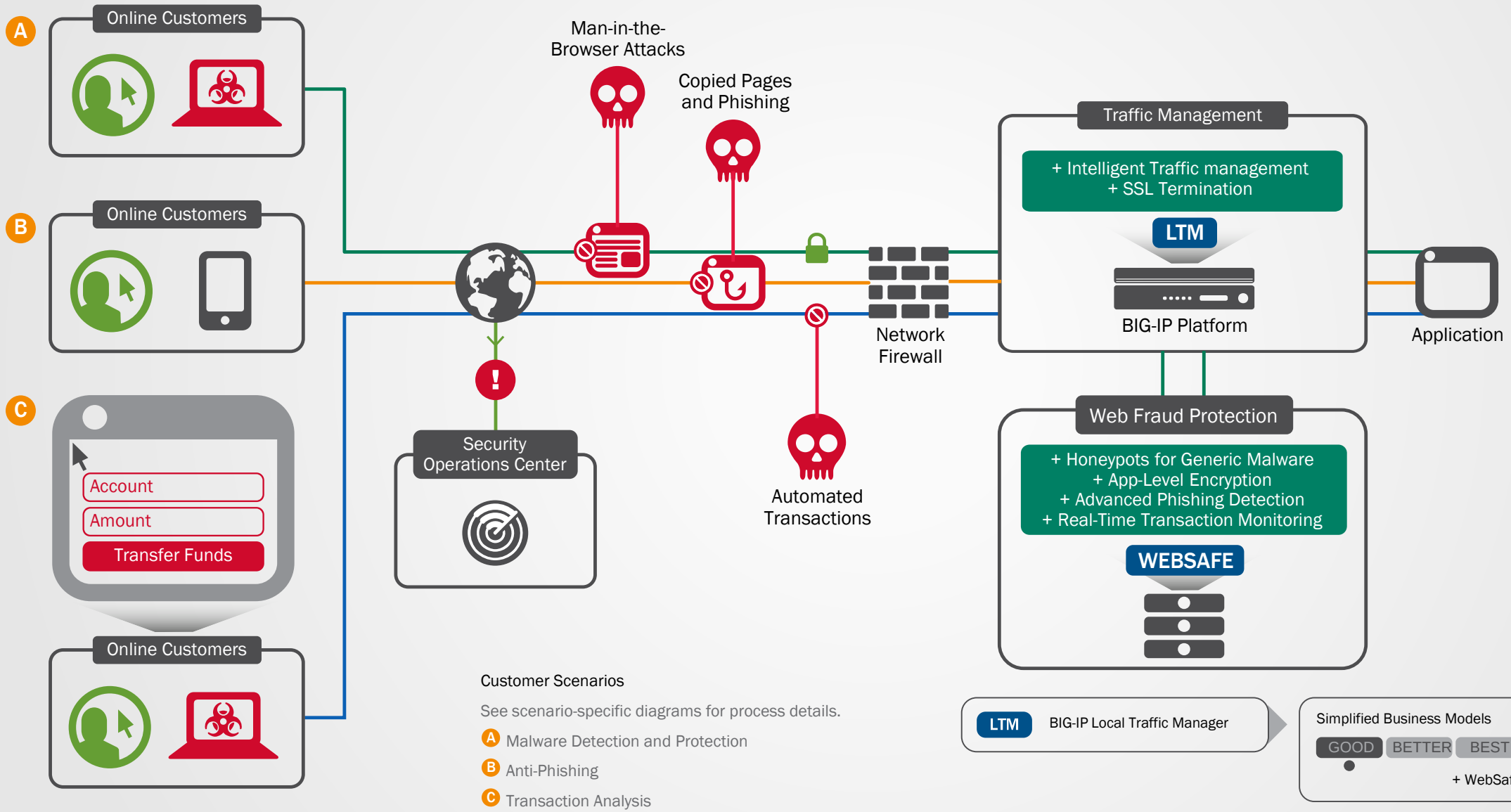
Preventing Automated Fraudulent Transactions

HOW IT WORKS

1. F5 adds hidden JavaScript code to web page served to online customer
2. F5 actively monitors user behavior interacting with the web page
3. If anomalous behavior is detected, an alert is triggered



Additional Methods for Implementing Websafe



F5 Security Operations Center (SOC)

Always on the watch

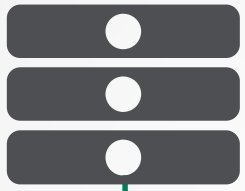
- 24x7x365 fraud analysis team that extends your security team
- Researches and investigates new global fraud technology & schemes
- Detailed incident reports
- Continuous product component checks
- Real-time alerts activated by phone, sms and email
- Optional site take-down: Phishing sites
  - Phishing or brand-abuse sites

Benefits

Only 100% transparent anti-fraud solution

Combined fraud detection & protection

Simple product rollout



Ensures compliance

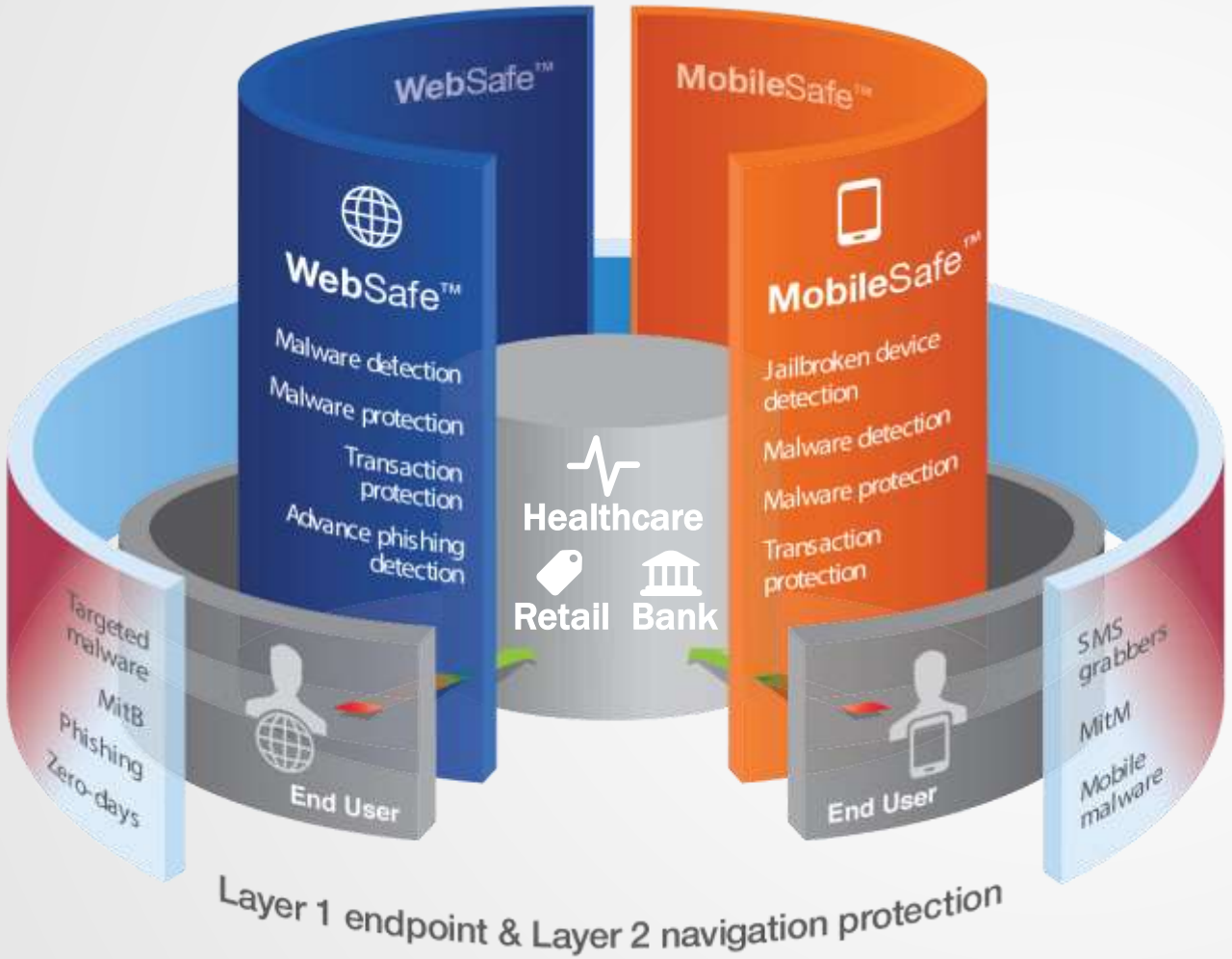
Protects users data in use

Prevents phishing attack

protect all customers on all devices

BACKED BY WORLD-CLASS SUPPORT AND PROFESSIONAL SERVICES

F5 fraud protection services

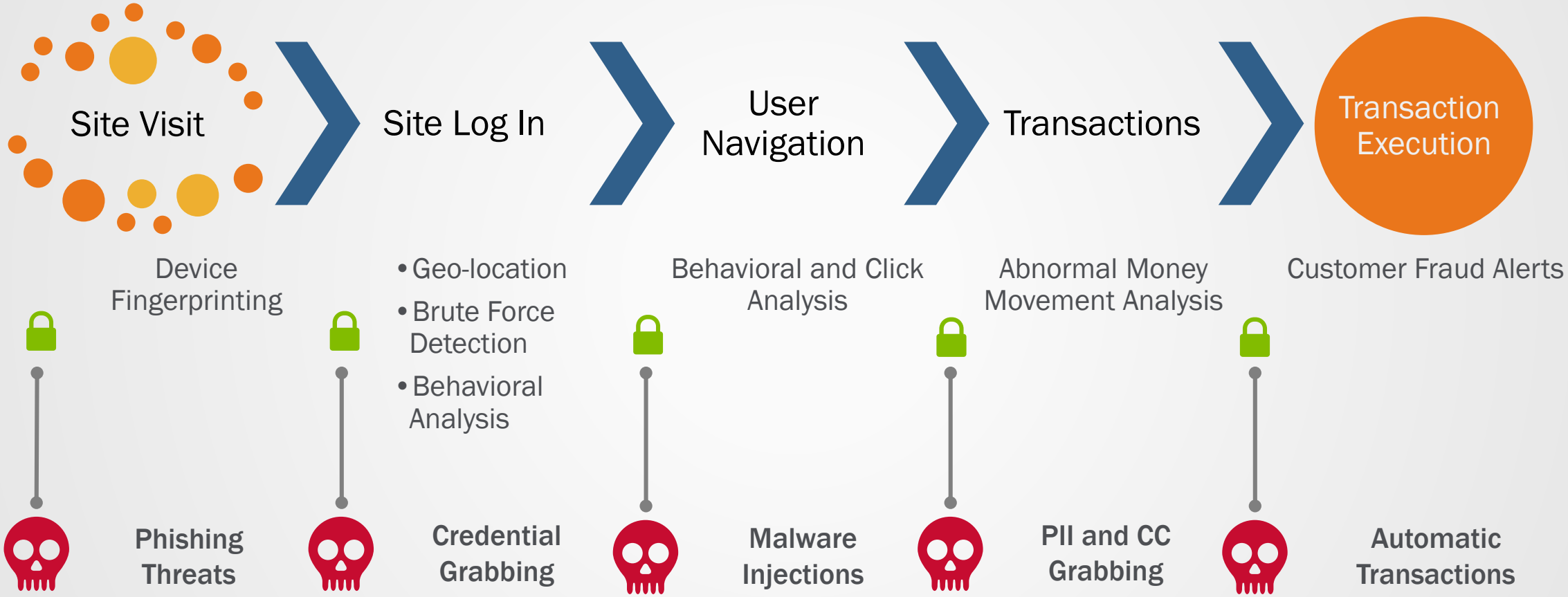


"The knowledge that our online users are protected from fraudsters, wherever they are and at any time, enables our team to focus on developing new products and services."

Executive Vice President, Leumi Bank

Our unique solution

Offers protection to cover the gaps with most security solutions



Solutions for an application world.