KASPERSKY FRAUD PREVENTION - CLIENTLESS ENGINE

Smarter security – better digital banking

While financial institutions are racing to provide customers with the most intuitive and satisfying online banking experience, professional cybercriminals are racing to develop ever more sophisticated malware to take full advantage of each new opportunity for online fraud.

Powerful new attack techniques you may well already have experienced in action include:

- **Web page infiltration** - extra fields 'injected' into your login page, capturing confidential customer data such as the CVS card number for use in 'card-not-present' attacks.
- **Fake (phishing) pop-ups** - adding the hacker's own 'pop-up' request for additional data, perhaps a mobile phone number so that 2-factor verifications can be intercepted.
- **Transaction tampering** - examples include instructing customers to 'repay' to the money falsely recorded as entering their account in error, or to make a 'test' transaction to assist the bank.

All these techniques begin by uploading malware, usually in the form of Banking Trojans, to your online banking system. And this malware is typically introduced through your system's most vulnerable point – your customers. The attackers begin by infecting your customer's own device, then use the customer's online connection to you as their point of entry.

How do you protect yourself from complex fraud attacks initiated from infected user devices, without compromising the relaxed, straightforward online banking experience that creates happy, loyal customers?

Kaspersky Fraud Prevention Clientless Engine prevents cybercriminals from launching successful attacks by:

Financial Malware Detection:
Proactively seeking out and identifying malware attempting to infect your web pages through your customers' devices.

Detecting any infected computer or mobile phone attempting to initiating malicious activity through its online connection to your site – with no impact on uninfected customers or their digital banking experience.

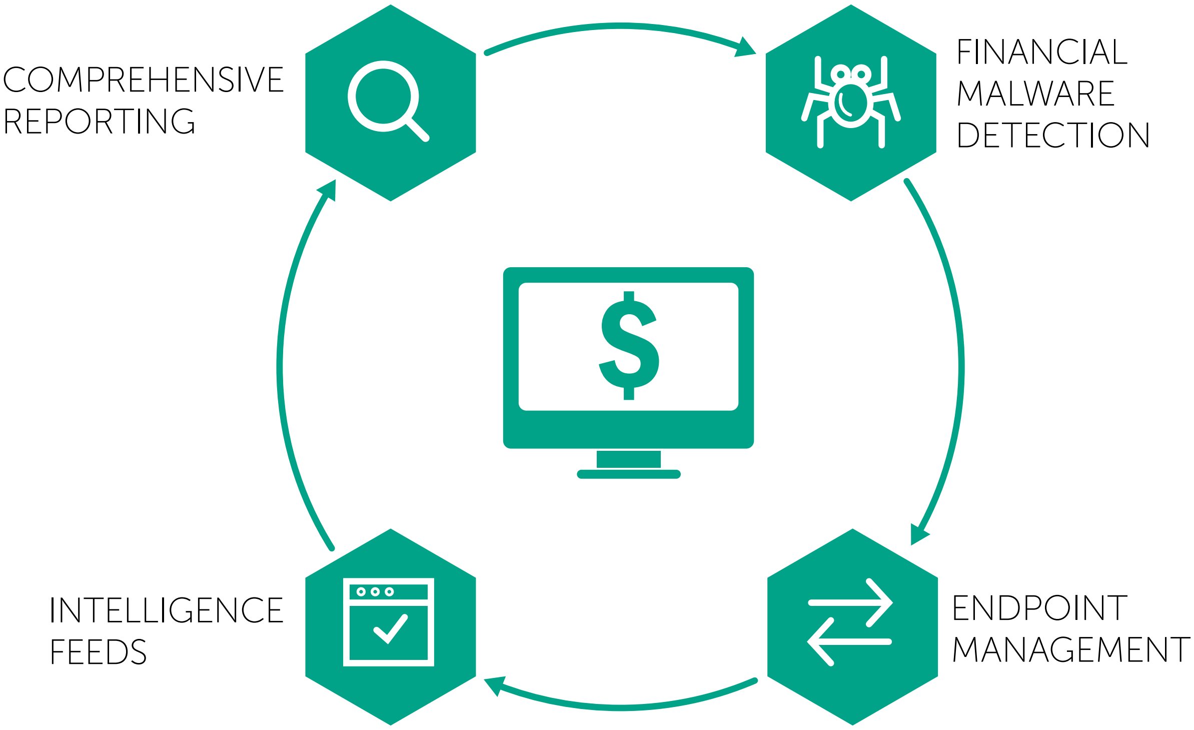
Comprehensive Reporting:
Alerting you so that your bank can take action, which could include:

- Blocking the transaction
- Terminating the user's session
- Managing the customer's case to ensure the incident is not repeated.

Endpoint Management:
Providing you with incident data through the Kaspersky Fraud Prevention console, and streaming this to internal or third party systems for further analysis and research if required.

Intelligence Feeds:
Giving your online banking management teams the information they need to make complex security decisions.

While you have visibility of every potential incident, the process is frictionless for users, unless their device has been compromised by banking malware. In which case, you'll be there to reassure them, and to advise them on how to stay safe in future.



The result is a safer online banking environment for everyone, freeing you to win and retain more customers by further developing the functionality of your digital banking portal, without increasing the risk of undetected fraud attempts.