EASYSOLUTIONS®
A CYXTERA BUSINESS

> Solution Overview

The Detect Safe Browsing Framework

Secure Transactions On Any Device

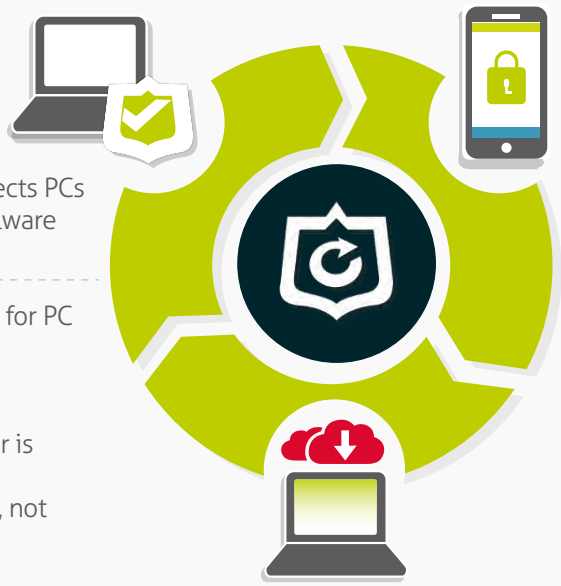
Identifying and eliminating malicious files is not enough to stop financial malware; the vast majority of devices are already infected, and new strains exploiting zero-day vulnerabilities arrive daily. The Detect Safe Browsing Framework takes a different security approach. By disrupting the credential harvesting and external communication channels that malware uses to take over accounts and cash out attacks, it ensures that even infected devices can continue to perform secure transactions.

Multi-Layered Fraud Prevention and Threat Protection

Detect Safe Browsing Client

A downloadable client that protects PCs and Macs from phishing and malware attacks.

- Lightweight desktop software for PC
- Cloud back-end
- Open API architecture
- Browser-agnostic
- Protection even when browser is updated
- Focuses on malware behavior, not signatures



Detect Safe Browsing Mobile SDK

Protects both the banking app and mobile browsing by detecting malware and other mobile risks.

- Full visibility
- Simple deployment
- Targeted MitM, overlay, pharming and repackaged app attack protection
- Device risk assessment and risk-based authentication

Detect Safe Browsing Clientless

Transparent, software-free detection that identifies malware attempting to tamper with online portals and sessions.

- Targeted malware, MitB, zero-day, MitM, and phishing attack detection
- Identifies HTML code injection to pages
- Malware Snapshot® records attack evidence
- Compromised credential detection

EASYSOLUTIONS®
A CYXTERA BUSINESS

> Solution Overview

The Detect Safe Browsing Framework – Features and Benefits

Detects and Stops Malware Infections

Alerts security teams about malware infections by analyzing all processes running on devices, and helps to protect against malware attacks by blocking connections to command and control servers.

Safeguards Sensitive End-User Data

Identifies the DNS poisoning that signals a pharming attack is taking place and blocks redirection to fraudulent websites. Encrypts keystrokes from keyboard to browser so they can't be intercepted.

Discovers and Halts Phishing Attacks

Our unique threat monitoring solution penetrates the remote cybercrime zone known as the Dark Web looking for compromised credit/debit card data to proactively mitigate impact after breaches and other security incidents occur.

Prevents the Root Cause of Fraud by Finding Active Threats in Real Time

Stops threats as early as possible in the fraud lifecycle and accurately detects a wide range of potential risk factors on end-user devices. In this way, organizations can take action against the most dangerous threats before being impacted by them.

Improves the Customer Experience by Slashing Unnecessary Friction

Reduces redundant authentication challenges, transaction verification and other disruptions that negatively impact the customer experience, delivering a proactive remediation solution for risky devices and sessions.

Reduces the Operational Impact of Fraud Investigations

The Detect Safe Browsing Framework allows organizations to calibrate their risk tolerance, helping to reduce alert volume and false positives so that anti-fraud efforts can be targeted more efficiently to where they are needed the most.

Utilizes Real-Time Threat Intelligence

Our team of 24-7 Security Operations Center agents analyze the intelligence that the Detect Safe Browsing Framework collects from over 270 million endpoints and hundreds of global organizations to adapt protection to each invididual customer interaction.