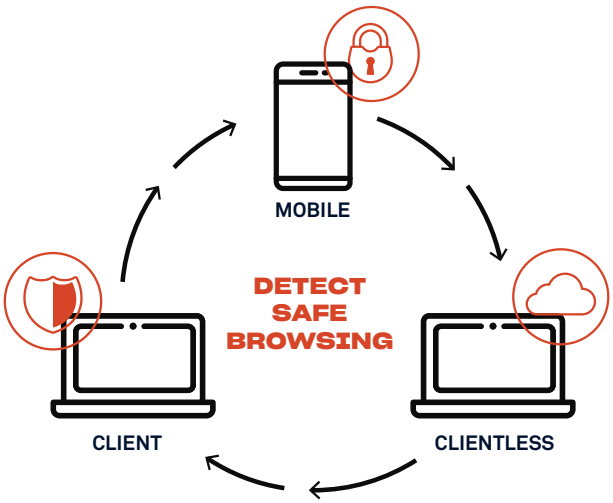
appgate

DATA SHEET

DETECT SAFE BROWSING

Secure Transactions On Any Device

MULTI-LAYERED FRAUD PREVENTION AND THREAT PROTECTION



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.

Detect Safe Browsing takes a different security approach. By disrupting the credential harvesting and external communication that malware uses to take over accounts and cash out attacks, it ensures that even compromised devices can continue to perform secure transactions.

DETECT SAFE BROWSING CLIENT

A downloadable application 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

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

Clientless 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 in pages
- Malware Snapshot for actionable evidence
- Compromised credentials detection

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. Uses advanced clientless identification technology to instantly recognize malicious code injections on your website's transactional pages.

UTILIZES REAL-TIME THREAT INTELLIGENCE

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

IMPROVES THE CUSTOMER EXPERIENCE BY SLASHING UNNECESSARY INTERRUPTIONS

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

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 the impact after a security breach has occurred.

REDUCES THE OPERATIONAL IMPACT OF FRAUD INVESTIGATIONS

Calibrate risk tolerance across channels while reducing alert volume and false positives, so that anti-fraud efforts can be targeted more efficiently to where they are needed the most. The innovative and unique mobile Risk Controller feature restricts access and functionality based on factors such as whether a phone is jailbroken, rooted, infected, connected to public Wi-Fi and much more.

PREVENTS THE ROOT CAUSE OF FRAUD BY FINDING ACTIVE THREATS

Stops threats as early as possible in the fraud lifecycle and accurately detects what can't be prevented. In this way, customers can take action against the most dangerous threats before being affected by them. The Clientless Malware Snapshot feature takes an instant screenshot of any malware-injected page to reduce the time spent on investigations and accelerate response.

DEFENSE AGAINST SMISHING ATTACKS ON ANDROID DEVICES

Protect your end users from falling victim to a phishing scam that targets them via SMS text messages, an attack known as Smishing. The DSB Mobile SDK scans SMS text messages on end user smartphones for any clickable links, looking for known phishing URLs, and URLs that could be new phishing attacks, while at the same time maintaining the end user's privacy. All detected URLs can be reviewed in the DSB Customer Portal, where the institution can confirm them as phishing, or categorize them as trustworthy.

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.

appgate