SentryBay®
DEFENCE BEYOND DETECTION

DATA SHEET

BankSAFE

Advanced AI-Powered Endpoint Data Protection

KEY FEATURES

- Kernel mode anti-keylogging
- Anti-screen capture
- Anti-Ransomware
- Anti-Phishing

Anti-Keylogging

BankSAFE's keylogging protection harnesses SentryBay's patent protected methodology and provides the most robust, low-level keylogging protection. From the kernel level, the keylogging protection is seamless and transparent to the user.

After being battle tested by some of the largest banks and technology partners in the world the solution has proven itself to be industry leading.

The way it works is by scrambling each keystroke entered with a keyboard which means any untrusted application or bad actor will be fed a stream of redundant data, except for the automatically targeted web browser processes.

- Provides credential theft protection across all websites
- All applications other than the web browser will receive redundant data
- The protection functions from the kernel level

Anti-Screen capture

The screen capture protection gives a critical layer of security which ensures that an attacker would not be able to retrieve any sensitive information that may be visible when the user is browsing the internet or online banking. This protection functions by applying a persistent rule that while enabled, any screen capture is returned as a black screen, the user also has the option to enable/reenable this protection so they can take screen captures when needed.

- Any screen shot or screen recording will produce a black screen – *Can be disabled (for purposes such as video calling)*
- Protects sensitive information that may be visible on the web browser

Anti-Ransomware

BankSAFE proactively monitors all encryption processes, intercepting and halting malicious processes before they encrypt files. This contrasts with many traditional methods that react after the fact or depend on recognising the threat before it acts. When an encryption activity is detected, BankSAFE employs a risk assessment system to determine its legitimacy. After evaluating the risk, a decision, such as 'Allowed' or 'Blocked', is made, and subsequently communicated to the user. The evaluation system considers multiple factors to render its judgment and operates with precision.

- Every encryption process is monitored proactively.
- Risk scoring system – *9 major factors used to determine if the process is malicious*

Anti-Phishing

Leveraging a diverse range of reliable phishing intelligence, BankSAFE delivers a robust safeguard against both new and emerging phishing threats. This serves as an additional layer of anti-phishing security, stepping in to protect users when the built-in protections of the browser fall short.

- Uses multiple sources of phishing intelligence
- Customisable phishing threat warning

Browsers Protected

Mozilla Firefox, Google Chrome, Microsoft Edge, Safari, Internet Explorer

Supported Operating Systems

DPS for Mac:

- macOS 10.13 (Mojave) and higher

DPS for Windows:

- Windows 8.1 and Windows 10

Minimum Hardware Requirements

- At least 512MB of RAM
- Processer with at least 233Mhz clock speed

Is Your Financial Institution FFIEC Compliant?

SentryBay
DEFENCE BEYOND DETECTION

UK
20 Little Britain
London
EC1A 7DH
+44 203 478 1300

USA
16900 Ashton Oaks
Charlotte, North Carolina
28278
+1 949 394 4902

SentryBay is a privately held firm headquartered in London and the USA with clients and partners globally.