SentryBay
DEFENCE BEYOND DETECTION

DATA SHEET

Armored Client

Delivering a Zero Trust Approach at the Endpoint

KEY FEATURES

- Kernel mode anti-keylogging
- Advanced anti screen capture
- Screen capture whitelisting
- Malicious injection protection
- Enforced security without UEM enrolment
- Virtual machine blocking

Anti-Keylogging

Armored Client targets individual application processes on Windows, macOS and Stratodesk with its industry leading protection to secure applications with active defence against keylogging, screen capture and malicious injection attempts by feeding randomised characters to endpoint agents.

- Provides credential theft protection at the point of sign in
- Provides in-session keystroke protection

Advanced Screen Capture Protection + Screen Capture Whitelisting

The advanced screen capture protection blocks the ability for applications to capture via screen shot or record and incorporates a unique capability to 'whitelist' individual applications from screen capture allowing applications to be permitted to capture the screen whilst at the same time blocking against malware or unsanctioned applications capture the screen.

- Blocks screen capture from malware and accidental use capture
- Allows applications such as Optimised Microsoft Teams to share the screen when used in VDI

Malicious Injection Protection

Applications protected by Armored Client are immunised from injection attempts, this could be from a piece of malware attempting to hijack the application to customise native protections or for privilege escalation, data theft from memory or even blocking keyloggers from burying themselves into targeted applications.

- Blocks malicious files from injection, such as ability to turn off screen capture protection in Azure Virtual Desktop

Enforced Security Without UEM Enrolment

Armored Client provides a proactive enforcement mechanism that ensures only protected devices are authorised to sign into Azure Virtual Desktop or Windows 365, this ensures critical security is in place from unmanaged endpoints such as 'bring your own computer' or third-party vendors and that unprotected devices are unable to log into Azure Virtual Desktop or Windows 365.

- Block unprotected devices from accessing Azure Virtual Desktop

Virtual Machine Blocking

Armored Client can detect if is installed on a virtual machine and shut down. The effect of this is the protected application become inaccessible due to enforcement. This type of protection is vital as virtual machine can be used to circumvent keylogging and screen capture attempts.

- Block Virtual Machines from being used to circumvent screen capture and keylogging attempts

Supported Operating Systems

- Microsoft Windows 10 21H1 or newer
- Microsoft Windows 11
- Apple macOS Monterey or newer

Armored Client Protects Data at the Endpoint

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.