SentryBay ARMORED CLIENT | IGEL | Ready

SOLUTION BRIEF

Armored Client for IGEL: Addressing a Critical Risk by Securing User Input Devices

The integration of IGEL and SentryBay Armored Client extends the security of IGEL Secure Endpoint OS Platform across the full endpoint I/O stack, delivering comprehensive protection.

The Challenge

Enterprises face an evolving class of threats that exploit endpoint weaknesses by targeting User Interface Devices (UIDs). Protecting endpoint input and output is now a critical but frequently overlooked element of risk management.

User Interface devices, including the keyboard, screen, camera, and microphone, must remain open and accessible to operating systems and applications to enable productivity. This architectural necessity makes them difficult to secure using traditional OS controls and legacy endpoint security tools.

At the same time, how users interact with applications continues to evolve. Dictation, collaboration platforms, SaaS applications, and AI-driven workflows all depend on expanded and continuous access to user interface devices. This growing reliance significantly increases the attack surface and creates new opportunities for exploitation.

Because User Interface Devices remain open during authenticated sessions, they are highly attractive targets for malware, insider threats, and rogue or AI-driven agents. The data exposed through the interface is inherently sensitive. Credentials, conversations, images, financial data, and intellectual property are all visible, audible, or entered through the UI, making the reward for attackers exceptionally high.

The MITRE ATT&CK framework formally recognizes these risks, classifying UID exploitation techniques such as screen capture (T1113), video capture (T1125), audio capture (T1123), and keylogging (T1056.001) as high-impact data collection methods. In addition, compromised I/O devices can be exploited to execute commands and manipulate live user sessions.

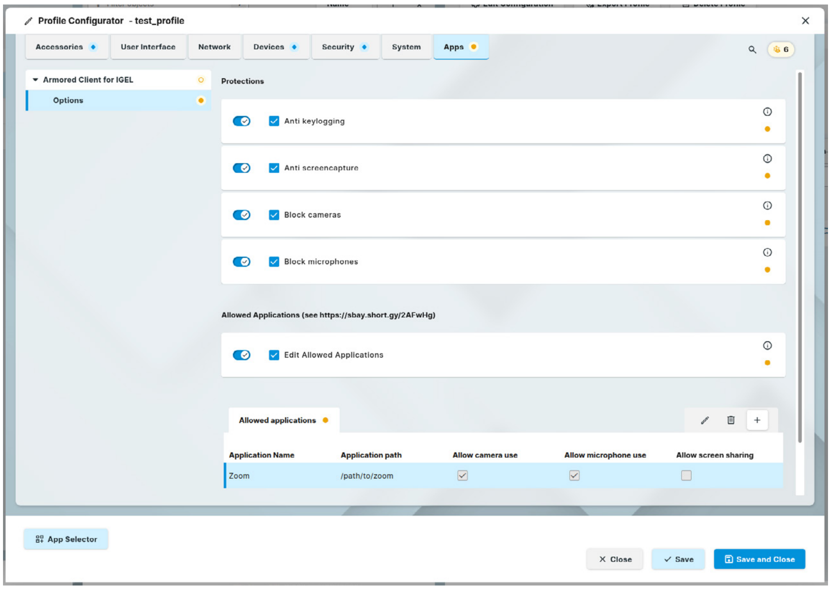
Most organizations have historically prioritized endpoint security investment around malware detection, device posture assessment, and network traffic controls. While effective at reducing initial compromise, these approaches do not adequately address UID-level exploitation once a session is authenticated and active. This gap is increasingly exploited by adversaries who leverage unprotected User Interface Devices to collect, exfiltrate, and abuse sensitive data.

Key Features

- **Frictionless Deployment.**
  Install and manage the IGEL-certified application directly through UMS with minimal operational overhead.
- **Anti-Keylogging Protection.**
  Substitutes real keystrokes with randomized input to neutralize keylogging attacks.
- **Anti-Screen Capture Controls.**
  Blocks unauthorized screen capture to protect sensitive on-screen data.
- **Camera and Microphone Protection.**
  Prevents unauthorized access to audio and video devices, reducing exposure to surveillance and impersonation threats.
- **Granular Application Controls.**
  Enables administrators to define precise access policies for keyboard, camera, microphone, and screen capture on a per-application basis.

The Solution

SentryBay Armored Client for IGEL enables organizations to extend the security of IGEL Secure Endpoint OS Platform across the full endpoint I/O stack, delivering comprehensive protection for the entire User Interface Device set.



Protections

☑ Anti keylogging

☑ Anti screencapture

☑ Block cameras

☑ Block microphones

Allowed Applications (see https://sbay.short.gy/2AFwHg)

☑ Edit Allowed Applications

Allowed applications

Application Name	Application path	Allow camera use	Allow microphone use	Allow screen sharing
Zoom	/path/to/zoom	☑	☑	□

Armored Client FOR IGEL adds a preventative OS-level security layer that proactively blocks keylogging and puts screen capture, camera, and microphone access for each endpoint under full administrative policy control.

Deployed through the IGEL App Store and centrally managed via the IGEL Universal Management Suite (UMS), Armored Client for IGEL is designed to support diverse enterprise use cases without adding operational friction. Advanced data obfuscation techniques, combined with intelligent enforcement of screen capture, camera, and microphone access, neutralize UID-level exploitation techniques favored by modern attackers.

Rather than relying on detection and response, Armored Client introduces a preventative security layer that proactively blocks keyloggers, screen capture tools, unauthorized camera and microphone access, and insider abuse at the OS level.

This approach safeguards highly sensitive data, including credentials, personally identifiable information, financial records, voice and image data, and intellectual property. By blocking UI exploitation at its source, Armored Client stops zero-day and unknown threats before data exposure occurs.

The solution delivers consistent, device-wide protection across every IGEL OS endpoint, whether supporting VDI, DaaS, or SaaS sessions. From remote workers and contractors to privileged access environments, Armored Client for IGEL transforms endpoint security from reactive to resilient.

Key Benefits

- Proactive extension of IGEL security against exfiltration malware, reconnaissance activity, deepfakes, and impersonation attacks.
- Prevention of the exfiltration of sensitive data, including credentials, PII, financial data, and intellectual property.
- Universal protection across VDI, DaaS, and SaaS sessions.
- Support for regulatory and jurisdictional compliance requirements.
- Full administrative control over how individual applications use I/O devices.
- Proven device protection leadership with over ten years of market experience.

Enterprise Use Cases

- Call Centers. Policy-driven UID protection aligned with operational workflows. Camera access can be restricted to approved roles, while microphone access remains available for agents. Keyboard input and screen capture are protected by default, preventing credential harvesting and unauthorized data exposure during customer interactions.
- Healthcare. Protects camera and microphone I/O paths against covert recording and eavesdropping. Ensures confidentiality of patient interactions, supports compliance requirements, and reduces the risk of privacy breaches during virtual care sessions.
- Executive Users. Enforces comprehensive protection across keyboard, screen, camera, and microphone channels. Prevents impersonation, deepfake-enabled fraud, and unauthorized capture of sensitive discussions, enabling executives to participate securely in high-risk meetings.

About IGEL Ready

IGEL Ready is an exclusive technology partner program designed to enable hardware, software and IT peripheral companies to develop verified, integrated solutions with IGEL products. IGEL Ready focuses primarily on identifying recommended partner products and solutions that are trusted and verified to work with IGEL OS. All products featured in IGEL Ready have completed rigorous verification testing, thereby providing our joint customers confidence in our combined solution compatibility and effectiveness.

About Armored Client

Armored Client is a next-generation security solution tailored specifically for the IGEL platform. Our technology harnesses advanced anti-keylogging and anti-screen capture measures—combined with intelligent application-specific whitelisting—to deliver unparalleled endpoint protection. Trusted by organizations seeking robust, zero-day threat defenses, Armored Client secures IGEL digital workspaces against the evolving tactics of modern cyber adversaries. Embrace a proactive security strategy and protect your IGEL assets with Armored Client.

This comprehensively positions Armored Client for IGEL as a proactive, robust, and strategic security solution—ideal for organizations looking to fortify their digital workspaces against emerging threats. Additional imagery, customer testimonials, and technical specifications can be added as needed to further tailor the presentation to your audience.

IGEL The Secure Endpoint
OS Platform for Now & Next