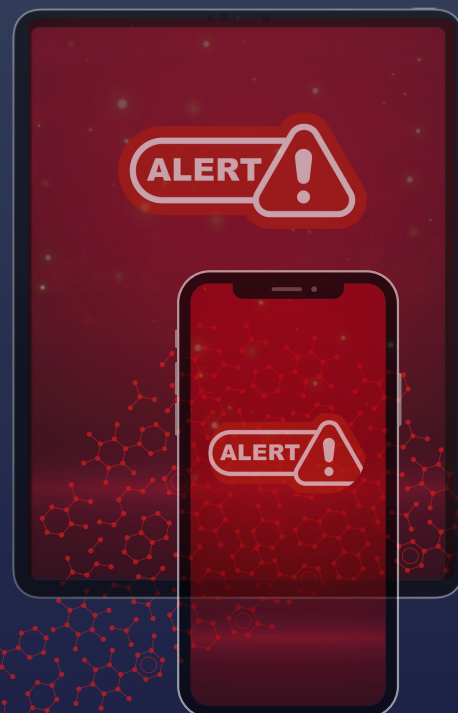# ENVOID

MAKE PHONES SAFE AGAIN

⚙ MOBILE SECURITY CHALLENGES

In the modern era of constant connectivity, mobile devices are indispensable information exchange tools, making them prime targets for increasingly sophisticated mobile spyware attacks.

These evolving threats go beyond typical cybercrime, repeatedly targeting high-profile individuals such as politicians, business leaders, lawyers, accountants, and other influential figures.

As mobile spyware becomes more advanced, it exploits vulnerabilities with precision and stealth, frequently without the victim's awareness.

This makes robust defense and proactive prevention more crucial than ever.

✧ ENVOID: WHO ARE WE

ENVOID is a specialized mobile cybersecurity firm that delivers unmatched protection against the most sophisticated and advanced mobile spyware threats.

Our approach transcends conventional solutions by offering comprehensive security designed to safeguard your personal data, providing peace of mind.

With cutting-edge technology, we detect and neutralize zero-click attacks, spyware, and malicious intrusions in real-time, ensuring swift, seamless, and intuitive protection.

We empower you to confidently navigate the digital landscape, knowing your connections and data remain fully secure and uncompromised.

MISSION AND VISION

Mission:

Empowering individuals with full control over their personal devices, ensuring absolute privacy and security in the mobile digital world.

Vision:

Restoring trust in technology by making personal mobile devices truly safe again.

OUR TECHNOLOGY

Live Prevention: ENVOID is the only company that provides 24/7 real-time detection and prevention of mobile infections, offering unparalleled protection.

Unique Technology: ENVOID's software is the only solution specifically designed to defend against the most advanced mobile cyber threats, ensuring cutting-edge protection.

Seamless Deployment: Enroll multiple devices across various locations within your organization in under an hour, with zero disruption to your daily operations.

Persistent Attack Defense: Our platform defends against the most sophisticated attacks, including 0-click attacks, watering hole, 1-click attacks and more.

Expert Technical Support: Our experienced team of vulnerability and threat researchers provides continuous support, ensuring your security stays ahead of emerging threats.

Encryption: Our solution incorporates End-to-End Encryption (E2EE) and Full Disk Encryption (FDE) to secure data both in transit and at rest, safeguarding sensitive information from unauthorized access.

Proven Success: Our technology has a demonstrated track record of defeating real-world spyware attacks and delivering reliable protection in critical scenarios.

Data Privacy: ENVOID does not collect any data. All information processed remains 100% self-hosted on the client's premises, ensuring complete data privacy.

Periodical Historical Infection Analysis: Each device undergoes a comprehensive historical infection analysis upon initial connection, periodically or when manually triggered, ensuring thorough protection from past threats.

✺ THREATS ENVOID PREVENT

- **Zero-Click Attacks**

A zero-click attack is a stealthy cyberattack that infiltrates a device without user interaction.

- **One-Click Attacks**

A one-click attack is a cyberattack triggered by a single, seemingly harmless user action, like clicking a link or opening a file.

- **Nation-backed spyware**

Nation-backed mobile spyware is sophisticated surveillance software developed or supported by governments to monitor, infiltrate, and extract data from targeted mobile devices for intelligence or security purposes.

- **Phishing**

Phishing is a deceptive cyberattack where attackers impersonate trusted sources to trick users into revealing sensitive information or clicking malicious links.

- **Juice Jacking**

Juice jacking is a cyberattack where malicious actors exploit public USB charging ports to steal data or install malware on connected devices.

- **Malicious domains**

Malicious domains are websites specifically designed to distribute malware, steal sensitive information, or perform fraudulent activities by deceiving or exploiting users.

- **Advanced Persistent Threats (APTs)**

APTs are stealthy, long-term cyberattacks that target high-value entities, using sophisticated methods to infiltrate, persist, and exfiltrate sensitive data without detection.

- **Remote Access Trojans (RATs)**

RATs are malicious software tools that grant attackers unauthorized remote access to a device, enabling data theft, surveillance, and control over system functions.

- **Data-unlockers (Cellebrite etc.)**

- **Hacking Multitools (Flipper Zero etc.)**

⚙ DEPLOYMENT METHODS

On Premise/Selfhosted

On Premise Method allowing the server to be self-hosted either on the customer's own servers or directly on the device itself.

Whether hosted on dedicated infrastructure or locally on the device, our solution provides seamless integration, optimized performance, and the highest level of data protection to meet specific operational and security requirements.

Mobile device needs to be connected to any WiFi Network.

⚙ DEPLOYMENT METHODS

Cloud Service

Cloud Method ensures secure and seamless delivery by utilizing both VPN and cloud-based services. Simultaneously, our cloud service enables efficient, scalable, and flexible deployment, ensuring minimal downtime and optimal performance.

Mobile device needs to be connected to dedicated VPN and to any WiFi Network.

ᚸ DEPLOYMENT METHODS

ENVOID Portable

Our solution features a Portable Method with an integrated Wi-Fi module, enabling continuous 24/7 protection and secure connectivity in any location, ensuring uncompromised security even in remote or mobile environments.

Mobile device needs to be connected to the portable device WiFi Network.

✺ DEPLOYMENT METHODS

ENVOID Servers

External Servers Method provides protection and efficient processing of information.
By managing and securing external servers, we enable seamless data processing while maintaining high levels of confidentiality, integrity, and availability.

Mobile device needs to be connected to any WiFi Network.

ENVOID

POWER OF PROTECTION

Let's Talk