



INTACT

INTACT's advanced technology ensures your data is protected, even if an attacker gets past other cyber-defenses and gains access to both your locked data and its decryption keys.

INTACT can be integrated with applications within minutes, further when combined with our product HIVE, you can stop the malware right at the source and hide your stored data even against internal threats.

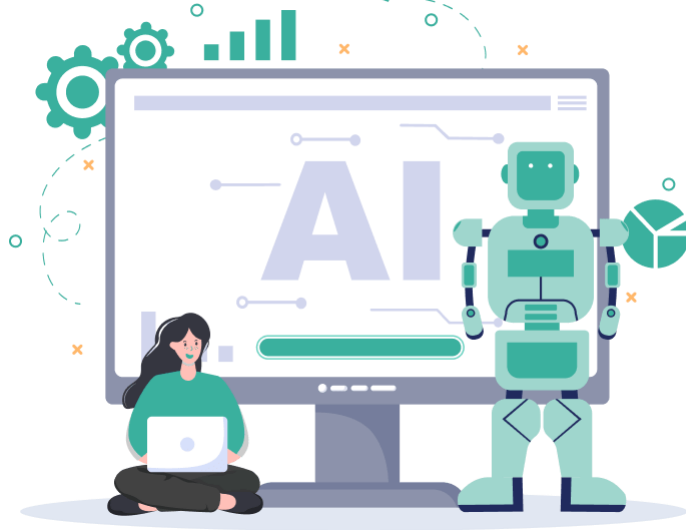


Protect your data in transit and at rest. Intact is not just an encryption tool, it is meticulously engineered to provide off the shelf protection against a wide range of cyber-attacks such as but not limited to Bluetooth Low-energy Spoofing Attacks, Relay Attacks, Replay Attacks, Side Channel Attacks, MITM Attacks, Brute Force Attacks, Denial of Service Attacks, Cross Site Scripting ANacks, Internal Threats and more.

Unique Qualities of INTACT

- Patented rapid deployment End- To-End Encryption system.
- Capable of protecting against a range of cyber-attacks.
- Patented tamper-proof cryptographic keys that protect data, applications and devices even if both the locked data and its corresponding cryptographic keys are obtained by an attacker.
- Patented encryption that can bond data, devices, persons, groups and applications with each other for the ultimate security.
- Patented automated data pattern randomizer.
- Fast encryption capable of handling large volume of data including live streaming.
- Light weight application that can be deployed even in small processors in IoT devices.
- Automated key management system with XIMP Standards.

Some of the used cases examples INTACT may include:



- Protect data stored in a vault in a cloud, mobile, IoT devices, machines, etc, even if an attacker gets into the vault and gets hold of decryption keys and the locked data.
- Protecting IoT devices, machine, mobile etc from being taken over by an attacker.
- Protecting data transmitted using wifi, network, Bluetooth, etc.
- Enabling secure connection between IoT devices, mobile, vehicles, laptops, etc.
- Protecting firmware integrity to avoid attacks during software updates or when the copy of source code is stored.
- Preventing Bluetooth low energy spoofing attacks.
- Protecting communications between controller and controlled machines, so an attacker cannot spy on the data transmitted or take control of the machine.
- Protecting drones, remotely operated vehicles, TV's, cameras, etc.
- Key logger immune keypads.
- Protecting against corporate espionage.
- Within minutes software developers can protect any data stored or transmitted from the mobile or desktop application against a wide range of attacks.