Ironclad Encryption Corporation (OTCQB: IRNC) is an X-Generation cyber defense company that secures digital assets and communications across a wide range of industries and technologies. IronClad Encryption-powered solutions utilize our patented Dynamic Encryption and Perpetual Authentication technologies to make all known key-based encryption technologies virtually impossible to compromise. Dynamic Encryption Technology eliminates vulnerabilities caused by exposure of any single encryption key by continuously changing encryption keys and keeping the keys synchronized in a fault-tolerant manner. Perpetual Authentication Technology uses multiple virtual channels for encryption so that in the event one channel is compromised, the other channels maintain encryption integrity. Together, these technologies not only eliminate the single point of failure problem created by having keys exposed through brute force, side channel, or other types of attack, but do so with very low latency and system performance overhead. Developers, MSPs, MSSPs and IT organizations can now easily and effectively integrate ultra-secure authentication and encryption measures across essentially all mediums. This includes the latest processors and operating systems, legacy hardware and software, within or between networks and on compartmentalized data or entire databases. At rest or in-motion, IronClad Encryption ensures data remains safe, secure and uncompromised.

IRONCLAD ENCRYPTION (ICE) SOLUTIONS:

Ironclad's innovative approach to encryption key management overcomes the limitations of existing key management systems without adding latency or performance overhead. We enhance existing encryption methods including AES and 3DES so you can be confident that your data is always protected.

Continuous Key Generation

Ironclad's Dynamic Encryption technology eliminates the single point of failure problem inherent in single-key encryption techniques. Our key management system continuously generates synchronous keys between the sender and receiver. Each key is assigned to a small amount of data so if a hacker were to access one of hundreds of millions of keys, the amount of data he would obtain would be virtually useless.

Redundancy

Our key management system includes a redundant encryption channel. If one channel were compromised, the second channel would maintain encryption integrity.

Tolerance

We built in tolerance, so if a cell phone call or data packets drop due to a faulty network connection, for example, the keys remain synced between the sender and receiver.

Data Access Control

Ironclad Encryption provides fine-grain access control. Customers can put "rings" around a desktop computer, laptop, or server to control data access. For example, a team of people operating within a ring could be authorized to view documents but not allowed to download or transfer those documents. In addition, the rings support multifactor authentication and they can be used to enforce multiparty authorization by 2 to 64 parties.

Flexible Configurability

Ironclad's key management system is completely configurable so customers have the flexibility to decide how often the keys change, how much data keys are associated with, and which multi-factor authentication

mechanisms will be used. We also allow you to specify how many individuals are required for multiparty authorization and whether those authorizations must be simultaneous, sequential, geographic, etc.

Technology Agnostic

Ironclad Encryption is technology agnostic, so it can be embedded in any type of hardware, software, or network to protect data in motion and data at rest.

Low Overhead

Ironclad Encryption fortifies existing encryption methods and products without causing latency or performance degradation issues.

PRODUCTS:

To purchase or get further details on the products below, please contact sales@ironcladencryption.com.

Secure Phones

Ironclad Encryption has recently tested the ICE Phone, an ultra-secure mobile, ultra-rugged phone that will ensure absolute privacy. Testing conducted by PollenTech Oy demonstrates that IronClad's encryption algorithms are stable, reliable and add little performance overhead during encrypted VoIP calls. The testing was conducted by encrypting a call on a phone in PollenTech's Finland offices and transmitting the call to a DigitalOcean server in New York via intercontinental ocean fiber. The DigitalOcean server then rerouted the call back to a second phone in PollenTech's offices that decrypted the call. This exceptionally long distance was intentionally chosen to test the audio and call quality, with and without encryption, in a high latency environment. The duration of each call was approximately two hours. IronClad Encryption's ICE Phone will be built by Sonim Technologies, who produces the world's most rugged mobile phones used by civil emergency services as well as military personnel.

Secure Gateway

Our recently-announced ICE Box SCA 1 (Secure Communication Appliance) is a telecommunications gateway that will connect Ironclad's mobile handsets to PBX and call manager systems. Customers will also be able to install ICE BOX appliances at different locations to ensure the security of call traffic between the gateways. Use cases include secure connections between regional offices and between industrial physical assets and a designated office.

ICEMicro Context-Free, Natively-Secure Containers

Most software developers and IT professionals now realize that Docker containers have significant security vulnerabilities. Container orchestration platforms and transport layer security protocols don't solve the problem completely, so various vendors have responded with different types of solutions.

What if securing inter-container communications were as easy as packaging an application in a secure container? That was our question and that's why we created ICEMicro.

ICEMicro containers communicate with each other securely, out-of-the box. If you don't believe us, download one of our free images from Github and Docker Hub and try it. Within 5 minutes, you'll be creating and testing ICEMicro containers.

Our ICEMicro Community Edition enables developers to:

- Take ownership of application data security without the need for security expertise
- Build, deploy, and run secure applications without the costs associated with legacy security strategies
- Secure container communications between across disparate scheduling and orchestration platforms, IaaS services, transport-layer security protocols, and on-premises, cloud and hybrid environments
- Secure communications between software, devices, or software and devices

The possibilities are virtually endless, which is why we've open sourced our initial product.

Discover all the tools ICEMicro contains and how it can be used in both simple and complicated environments.

PARTNERSHIP OPPORTUNITIES:

IronClad Encryption works closely with consultants, manufacturers, developers, and service providers who want to differentiate their products or services or create entirely new products and services. Contact us today to discuss what IronClad Encryption can do for your company and its customers.

OEM, Software Developer, and Service Provider Licensing

OEMs, software developers. and service providers can drive new revenue streams and create competitive advantages using Ironclad technologies. For example, a network infrastructure vendor could charge a premium price for its switches and routers by enhancing their level of security. An Internet Service Provider (ISP) could offer its customers a premium security service.

Joint Development

Our technologists are currently working with development partners to bring new products to market. We can help you enhance the security capabilities of an existing hardware or software product or co-create a next-generation offering.

US Granted Patents:

US 10,154,021 - Securitization of Temporal Digital Communications with Authentication and Validation of User and Access Devices

US 10,171,444 - User-Wearable Secured Devices Provided Assuring Authentication and Validation of Data Storage and Transmission

US 10,154,031 - Devices that Utilize Random Tokens Which Direct Dynamic Random Access

US 10,171,435 - Selectable Key and Key Locator for A Hidden Dynamic Random Access Encryption System

US 10,154,016 - Devices for Transmitting and Communicating Randomized Encrypted Data Utilizing Sub-Channels

US 10,154,015 - Executable Coded Cipher Keys

US 10,158,613 - Combined Hidden Dynamic Random-Access Devices Utilizing Selectable Keys and Key Locators for Communicating Randomized Data together with Sub-Channels and Coded Encryption Keys

IRONCLOD ENCRYPTION CORPORATION
777 POST OK LANE, STE. 1700
HOUSTON, TX 77056
<u>**CONTACT US:**</u>

888.362.7972   Product sales: sales@ironcladencryption.com
888.ENCRYPT2   OEM licensing and partnerships: partnerships@ironcladencryption.com
Investor relations: ir@ironcladencyption.com   Public relations: pr@ironcladencyption.com