ENTROPYA

The Entropya Difference

Entropya sees your struggle: budget pressure, overworked teams, and the risk of devastating breaches. Cybersecurity is broken, but together, we can shift the paradigm. Threats can't attack you if they can't find you. We remove the digital footprints that associate your start point and destinations and erase your fingerprints from what you touched along the way. Entropya's quantum-durable, untraceable solutions eliminate attack surfaces, simplify security, and restore confidence.

- **Global Trust:** Swiss company with subsidiaries in the USA and Romania.
- **Digital Sovereignty:** Gold standard privacy and data protections.
- **Our Team:** Senior military leadership with national-level track & hack cyber expertise.
- **Simplicity Without Compromise**
- **Amplify Your Competitive Edge**
- **Crush Your Risk:** Eliminate attack paths; block zero-days, and man-in-the-middle attacks.
- **Mission-Critical Reliability:** Engineered for high-security environments and resilient by design with uncompromising security.
- **Vetted Supply Chains**

Cybersecurity is Broken

Cybersecurity is struggling to keep up, and cybercrime is nearly the third-largest global economy. Your security teams are overwhelmed, using outdated tools that are not designed for this level of integration, complexity, or scale while attackers are faster, stealthier, and more resourceful than ever. Instead of breaking in, every exposed IP, every open port, every visible service is a clue leading attackers to your most critical systems and data.

Shift the Paradigm With Proactive Defense

Every cyberattack starts with reconnaissance. Your breadcrumbs include:

- Public IP addresses
- Visible Ports
- Exposed devices
- Hosting signatures
- App specific data
- Routing headers
- Traceable metadata
- VPN, Firewalls, Firmware

A New Way of Thinking:

- **HIDE**: Eliminate digital footprints
- **HARDEN**: Resilient & quantum-secure architectures
- **VERIFY**: Continuously authenticate & validate

It's a **critical** mindset shift.

We believe the future of cybersecurity starts with a simple idea:

"You can't attack what you can't find."

Entropya Sees Your Pain

Why Traditional Security Models Are Failing:

- Findable = Exploitable
- Complexity Creates Blind Spots
- Scan-Based Detection Is Reactive & Too Slow
- Static Defenses Can't Keep Up

You are not just a defense system. You are professionals protecting your critical resources for: unpredictable endpoints doing remote work from cloud and hybrid environments, using third-party tools, and facing legacy and critical systems. When something goes wrong, you get the blame, but you are not adequately equipped, and the **real problem** is foundational.

Let's Make a Difference

If you are tired of reacting to threats that never should have reached you, and are overwhelmed by tools that promise visibility but deliver exposure, then it's time to rethink your foundation. Let's talk about how to make your systems **unfindable**, **unreachable**, and **unbreakable**.

Contact: office@entropya.com

ENTROPYA

Digital Camouflage

Overview

Why are traditional defenses not working? Cybercrime is on track to become the third largest global economy. Entropya is shifting the security paradigm to proactive complexity and cost saving defense design, focused on durable future security and Digital Camouflage, making systems unfindable, untraceable, and unreachable. Our expert practitioner team designed Entropya's solutions, inspired by national-level cyber operations and military cover and concealment tactics. This approach eliminates the attack surface by hiding your critical digital infrastructure from spying and analytic tools. Entropya redefines proactive digital defense by prioritizing invisibility, unpredictability, and resilience.

Key Points

HIDE. HARDEN. VERIFY.

- HIDE: Blend into 95% of Internet traffic with an unlisted address; needle in a stack of needles.
- HARDEN: Use national security grade quantum-resistant cryptography and resilient design.
- VERIFY: Continuously authenticate and validate.

Digital Location is the #1 Vulnerability

- Planning an attack starts with target stalking. Attackers can't exploit what they can't find. Entropya's digital camo removes exposed IPs, DNS records, and metadata; no target mapping.
- No persistent IPs, no start/end point correlation, and no digital signatures to trace.

Untraceable Transport Engine

- Our solutions are unique, with no reliance on vulnerable proxy, VPN, or TOR tech. Instead, dynamic software-defined private networks with micro-segmented one-way traffic prevent attackers from finding start and end points.

Proactive vs. Reactive Security

- Digital Camouflage removes the attack surface entirely (99.999%), preventing threats before they begin.
- Uses quantum-ready cryptography and ephemeral (short-lived), one-way tunnels.

Benefits

- Reduce security overhead cost and complexity.
- Meet you where you are with what you have.
- Mitigate attackers from finding and spying on you.
- Imposes costly time and resources on attackers with no resulting payoff and mitigates tracing.
- Make zero-day vulnerabilities unexploitable.
- Resilient against AI-driven and quantum threats.
- Save time and cost of incident response.
- Standards compliant across industries.

Rethinking Defense

The MITRE ATT&CK® framework reveals how attackers exploit visibility and predictability. Entropya's model neutralizes these tactics by making the infrastructure unfindable. Instead of a 360-degree defense around your perimeter and every endpoint, Digital Camouflage takes you off the map, rendering targeting, entry, movement, and exploitation infeasible.

Applications

- Protect any service, any server, any infrastructure, any pathway, anywhere.
- **Critical Infrastructure:** Water, energy, transportation, and healthcare systems.
- **Financial Systems:** Banks, stock exchanges, and payment processors.
- **Defense & Government:** Secure communications, classified networks, and military systems.
- **Cloud & Telecom:** Distributed data sync, data centers, ISPs, mobile carriers, space.
- **Emerging Tech:** Blockchain, IoT, and AI platforms.

Contact: office@entropya.com

ENTROPYA

Managing Cyber Risk

The source and nature of your activities, logistics, financial transactions, and supply chains provide a telling story about your vulnerable cyber attack surface and their key dependencies. Entropya's solutions simplify the complexity of cybersecurity through unmatched privacy. Our solutions separate actors from targets, their starting points from destinations, as well as the digital landscape they traverse. By isolating the privacy value chain and the phases of an attack, Entropya segments each step to deliver untraceable solutions with highest-grade security.

"Be extremely subtle even to the point of formlessness." -Sun Tzu, The Art of War

Traditional Risk Mitigation

Cyber reconnaissance, attackers, and exploiters use the internet's self-reporting features and interconnectivity, tracing benign digital attributes to pinpoint vulnerable attack vectors. These trails are exploited through the complexity of cyber-dependencies, physical infrastructure, finances, and supply chain. Below are risk specific privacy levels to consider:

Basic Privacy: Simple measures like masking IP addresses may not suffice against advanced tracking tools, leaving identifiable traces.

Intermediate Privacy: Third-party services and pathways like VPNs, proxies, or TOR are each alone vulnerable and leave distinct signatures with attack vectors and association risks.

Advanced Privacy: Curating alternate digital identities and support channels is resource intensive and risks associations exposure if inconsistencies are found.

Effective privacy management must evolve to address these challenges and ensure digital activities remain secure and untraceable.

Entropya Risk Mitigation

Entropya's solutions mitigate these risks and provide unmatched protection by addressing the foundational framework of cyberspace:

- Remove finance, supply chain, and logistics trails
- Eliminate 99.999% signature (hard & software)
- Post-quantum cryptographic authentication for Zero Trust Transport, no man-in-the-middle
  - Transport has amnesia, retains nothing
  - Untraceable one-way random IP flows
  - Multilayered segmentation & encryption
- No third-parties & no proxies or TOR
- Default configuration:
  - No open defaults, no root access
  - Compliance configuration via jail-partition, network flows & packet capture, as desired
  - Intrusion detection & disaster recovery
- Labyrinthine segmentation available

Entropya's design secures all layers of the OSI model, from physical to application layers. This holistic protection ensures that vulnerabilities at every layer are addressed, providing a robust defense against cyber threats.

Entropya sets the bar for cyber risk management and privacy protection in the post-quantum era. Our holistic cyber protection strategy includes understanding attribution across your cyber value chain while securing your infrastructure and safeguarding against even the most advanced cyber threats. Entropya delivers a robust and resilient security framework, ensuring that your data stays private and durably protected. Let Entropya meet and protect you where you are, **SCHEDULE A DEMO**.

ENTROPYA

Zero Trust with Untraceability

Entropya's Zero Trust approach is built from a career of cyber intelligence, red teaming, and an expert practitioner's view of how to find and hack the hardest targets. Our solutions are built to withstand exquisite scrutiny for attribution, selector signatures, the complexities of cyber physical security layers to include logistics, supply chain, and financial transactions. This approach takes inspiration from Sun Tzu's wisdom about self-understanding, creativity, and deception.

Zero Trust acknowledges that all network boundaries are penetrable somewhere and all connected systems have vulnerabilities yet to be discovered. And yet, to exploit a connected system's vulnerabilities it must first be found. Entropya's Zero Trust foundation is fundamentally different in that our solutions make every connected system indistinguishable from the next.

Meet You Where You Are

Our architecture is engineered to extend your decision-making window and enhance resilience without requiring changes to your existing infrastructure. By securing all layers of the OSI model, we effectively eliminate your systems' attack surface and enable rapid deployment through **open, non-proprietary standard interfaces**. Our solutions transcend conventional digital boundaries, ensuring seamless operation across legacy infrastructure, modern multi-cloud environments, cellular and satellite networks, AI-driven ecosystems, and Industry 4.0 landscapes. This system-agnostic protection encompasses firewalls, VPN servers, web applications, proprietary protocols, and even end-of-life systems that are no longer upgradeable.

Protecting the most sensitive systems, we offer **transport and network labyrinths** generating internal mazes of indistinguishable infrastructure. This design is well-suited for ransomware-proof backups, financial platforms, critical infrastructure, and healthcare, transportation, and defense.

Your Future Today

Making your transport and network access **untraceable**, we **remove man-in-the-middle attack vectors** individually authenticating and optimizing every routing connection through our **global superhighways**. This design separates the source and destination of every session, discretely authenticates, randomly routes, and frequently generates new encryption keys. Addressing the remaining attack surface, we remove all signature attributes, eliminate Domain Name System (DNS) resolution to your infrastructure, and randomize transport pathways to neutralize **99.999% of attack vectors.** Further encapsulating your data with FIPS 203 post-quantum cryptography, Entropya delivers your future today without vulnerable proxies, VPNs, or TOR: the gold standard for Zero Trust.

> "Be extremely subtle even to the point of formlessness." Sun Tzu, The Art of War

Your future begins today with Entropya's Zero Trust solutions. We ensure that your transport remains untraceable, secure, and quantum safe while keeping you connected through the highest performance digital superhighways. Entropya's holistic cyber protection strategy empowers you to operate any infrastructure securely, safeguarding you against even the most advanced cyber threats. Let Entropya meet and protect you where you are, SCHEDULE A DEMO HERE.

ENTROPYA

ENTROPYA ENCRYPTED NETWORK

Overview

Entropya's Encrypted Network (EEN) redefines what's possible in hyper resilient and untraceable superhighways. Designed from technical expertise in national level cyber operations, this dual-use technology stack saves infrastructure upgrade costs, server protection, and cybersecurity overhead by removing 99.999% of your attack surface. The EEN makes you unfindable, fights Adtech and advanced analytics, and protects against the most sophisticated man-in-the-middle attacks. Implementing the highest grade of quantum-ready cryptography, the EEN applies Zero Trust architecture to data transport while delivering uncompromising performance, seamless integration, and quantum-readiness for highly sensitive needs.

Key Features

Untraceable Infrastructure

- Removes digital fingerprints and misdirects DNS resolution to prevent discovery.
- Randomizes IP pathways and obscures signatures; no trackable start or end points.
- Kernel level integration for the strongest security, performance, and session control.

Zero Trust Architecture

- Dynamically authenticates every connection, ensuring no unauthorized access.
- Eliminates open ports and protocols at public IPs, neutralizing 99.999% of attack vectors.

Benefits

- Shields against surveillance, DDoS, and zero-day exploits by becoming unfindable.
- Reduces the complexity and costs of traditional layered security approaches.
- Buys you time: Future-proofs infrastructure; creates an undetectable quantum-ready boundary protecting critical data, backups, and vulnerable Public Key Infrastructure (PKI) for trustable authentication.
- Replace susceptible firewalls, VPNs, and comms.
- Any server, infrastructure, and system is quantum-resistant with exceptional performance.

User Experience

- Entropya's EEN combines simplicity with elite-grade security. Designed for rapid deployment and seamless integration, it requires low-to-no configuration while delivering high-speed, low-latency performance. Users gain hidden, resilient protection without compromising usability or performance.

Infrastructure-Agnostic Design

- Operates seamlessly across fiber, cloud, cellular, space, and terrestrial networks.
- Rapidly employs with legacy systems and enjoys near zero-config deployments.

Performance Without Compromise

- Delivers ultra-low latency and high throughput across all pathways.
- Enables multi-cloud resilience without the overhead. Become hyper secure with distributed infrastructure across any global fiber, data center, CDN, cellular carrier, or space transport.

Applications

- Secure hidden transport for foreign affairs, national security data, and defense systems.
- Stealth armor for critical infrastructure, industrial control systems, and IoT.
- Safeguarding data-sensitive sectors like financial services and healthcare.
- Distributed data sovereignty, synchronization, and backup.
- Secure operations for cloud, edge, and remote workforce environments.

Contact: office@entropya.com

ENTROPYA

USE CASES: ENTROPYA'S POST-QUANTUM ENCRYPTED NETWORK

HIDE. HARDEN. VERIFY.

Entropya's encrypted private networking technology suite offers unmatched security and anonymity for a wide range of applications. It provides versatile and robust digital superhighways with leading grade security for zero-trust communication and data needs.

1. **Anonymous & Encrypted Network**
   Organizations require secure, anonymous communication channels to prevent intrusion and ensure privacy. Entropya's Encrypted Network (EEN) provides one-way and obfuscated pathways that separate source and destination IP addresses, masking you in the noise of the Internet's HTTPS traffic. This approach is ideal for confidential information, assuring against both penetration attacks and internal lateral movement.

2. **Data in Transit and at Rest**
   Businesses need to secure sensitive data during transmission and storage to prevent data breaches. Our EEN supports secure data-in-motion and storage using quantum-ready cryptography, encryption, and synchronization protocols to protect your most critical data from sophisticated threats.

3. **Decentralized Systems**
   Decentralized systems like cloud databases, distributed ledgers, blockchain nodes, and synchronized storage require secure access. Our solutions provide untraceable secure connections, ensuring data integrity, privacy, and access across distributed infrastructure.

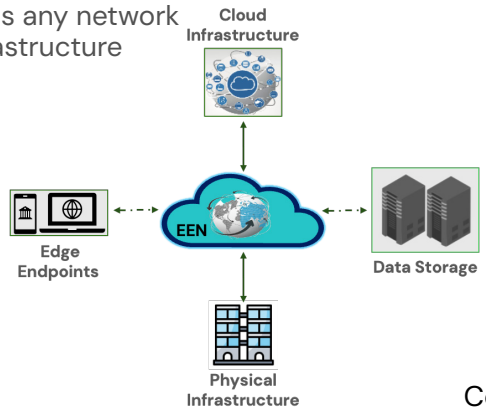
4. **Network Obfuscation**
   Networked platforms require advanced security measures to counter persistent cyber threats. Entropya's EEN hides and hardens any network and platform making critical infrastructure unfindable.

5. **Financial Transactions**
   Financial institutions rely on secure transactions. The EEN provides quantum resistant end-to-end cryptography to prevent fraud and breaches.

6. **Digital Last Mile**
   Delivering digital services to end-users requires a highly resilient and secure last-mile connection. The EEN connects space, cellular, fiber, and data center infrastructures into a seamless and resilient private super-highway, delivering quantum-ready digital services for the most remote needs.

7. **IoT and Metaverse Applications**
   Emerging technologies need robust security. Entropya provides quantum resistant pathways and data protection for digital transactions, IoT devices, the metaverse, and 5G/4G LTE private Access Point Name (APN) internet access.

8. **Healthcare**
   Healthcare providers need to protect Personal Health Information (PHI) and Personally Identifiable Information (PII). Our solutions level up the protection of sensitive patient information using post-quantum hardening to exceed compliance and safeguarding needs.



Contact: office@entropya.com

ENTROPYA

POST-QUANTUM AGENTS

Overview

Entropya's Post-Quantum Agents connect users and devices into the Entropya Encrypted Network (EEN). The EEN is designed to provide digital super-highways for unparalleled protection and anonymity for data in transit, data at rest, and digital communications using multiple encryption protocols through a one-way proprietary randomization algorithm. The EEN is designed to obscure both the source and destination IP addresses while protecting from analytics and pattern of life (POL) signature development. It is a fully decentralized, end-to-end encrypted, software, and hardware agnostic platform. It can reside and connect all infrastructure to meet the most demanding needs.

EEN uses a suite of Post-Quantum Cryptography (PQC) standardized in Federal Information Processing Standards (FIPS) Publication 203 as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). The EEN takes the FIPS 203 standard and implements the highest level, ML-KEM 1024, in a customized software defined private network (SDPN) delivering untraceable and hidden networking pathways. This robust and resilient transport is flexible as end-to-end PQC or fused between any standard encryption protocols found in commercially available hardware. We meet where you are.

Key Features

A Hyper Resilient Network

- Interconnects the world's highest performance infrastructures to create ultra-resilient SDPNs.

Entropya Encrypted Network (EEN)

- Our untraceable and hidden transport ecosystem removes 99.999% of your vulnerable cyber fingerprints and zero days.

Vetted Providers

- Resiliently connect through our global high speed digital highways and with your preferred providers.

Post-Quantum Attack Resistance

- Employs leading grade security that hides and hardens as the first line of defense. U.S. defense fielded.

Randomization

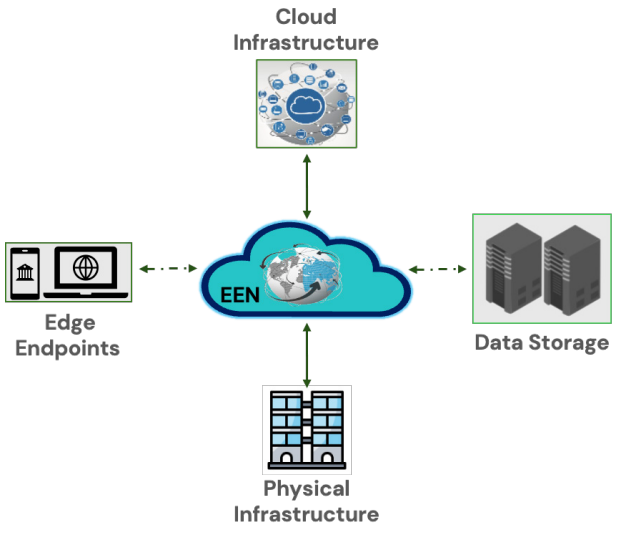
- Introduces custom randomized one-way pathways, removing reliance on legacy technologies like proxies or TOR.

Research and Development

- Entropya develops innovative security and privacy technologies from the world's brightest minds. The EEN technology suite is patented as a dual-use technology.

Benefits

- Low probability of detection and interception (LPD/I) because of the anonymous encrypted network that separates sources from destinations for untraceability.
- Hides sensitive data-in-transit & at-rest while removing their unique signatures.
- Anonymously and securely connects decentralized server databases, distributed ledgers and blockchains.
- Protect and obfuscate network platforms.
- Supports the digital last mile.
- Secure IoT, Web 3.0, metaverse, and Industry 4.0.
- Deploy with 5G and 4GLTE through Private Access Point Name (APN) Network.
- Protection and anonymity of PHI and PII information.
- Dark web research.
- Mature platform at Technology Readiness Level 9.



Contact: office@entropya.com

ENTROPYA

MOBILE 5G TRAVEL ROUTER

Overview

The ENTROPYA Mobile 5G Travel Router is a versatile Wi-Fi 6E solution offering non-attributable data service. This Mobile Hotspot Router provides and operates on 5G mm-wave and Sub-6 bands for lightning-fast internet speeds and connectivity. Our 5G mobile router offers standard Access Point Name (APN) routing or a private APN with post-quantum cryptography (PQC) through an Entropya Encrypted Network (EEN), ensuring untraceably secure and encrypted data-in-transit.

Key Features

Carrier Agnostic

- Hop between carriers with priority fast service using our Mobile 5G Travel Router. Wherever you are, reap the benefits of the best connections, hassle-free and seamless across carriers while staying untraceable.

Carrier Hidden SIMs

- Global connectivity is easy with our carrier-hidden SIMs. No matter the area and available carriers, you can connect without trouble.

Unthrottled Priority Network Access

- Never worry about data speed while moving between carriers because of our unthrottled network access; your speed will not experience downgrades, keeping your connection lightning-fast.

Multi SIM Shared Data Plans

- For ultimate flexibility, these SIMs are not tied to individual devices. This new freedom allows for easy SIM swapping. Our shared plans allow for multiple SIMs and eSIMs managed under a single account.

Benefits

- **SIMplified SIM & eSIM Procurement**: Eliminate the hassle with your SIM card procurement process.
- **Lightning-Fast 5G Connectivity**: Enjoy global wireless broadband access at the fastest rates and lowest latency.
- **Multi-Gig Wi-Fi Speeds**: A multi-gig Ethernet port and Wi-Fi 6E connect up to 32 devices simultaneously.
- **Secure and Encrypted Connections**: Upgrade with a Private Access Point Name (APN) through Entropya's Encrypted Network (EEN's) for Quantum Resistant digital super highways, end-to-end encrypted with complete randomization. This design is the most resilient, private, and secure on the market.
- **Market and Maintenance**: Entropya provides flexible procurement pathways with privacy-first supply chain options, including monthly service and management.

User Experience

- The Entropya Mobile 5G Travel Router functions seamlessly, creating a wireless hotspot with easy setup, no cables, and global access. The device features a built-in color LCD screen for convenient setup, Wi-Fi settings adjustment, and data usage monitoring.

Contact: office@entropya.com

ENTROPYA

CIPHER PHONE

Overview

The Cipher Phone guarantees secure communication and data exchange, specifically designed for sensitive users at all levels. Its robust infrastructure supports various communication needs while ensuring user protection and communication anonymity. The Cipher Phone service employs Entropya's non-attributable Primary-Alternate-Contingency-Emergency-Stranded (PACE-S) resilience with the PiEpsilon Communication Platform, as well as Voice Over IP (VOIP) technology. This is further enhanced by the use of hardened Software-Defined Private Network (SDPN) smartphones.

Key Features

Communication Security

- Cipher Phone provides a complete security solution, accommodating numerous communication protocols.

Global Cyber VOIP Service

- Entropya's Cipher Phone includes a VOIP service with global coverage, allowing users to choose a phone number from over 30 countries. This service functions without the need for authentication or connection to local networks, ensuring location privacy.

Double Encryption

- Your VOIP number is ported to a secure third-party application to provide double encryption and anonymity for enhanced security.

Device Compatibility

- Untraceable emails and anonymous accounts linked to the device are encrypted using custom-generated private and public keys, ensuring secure communication.

Benefits

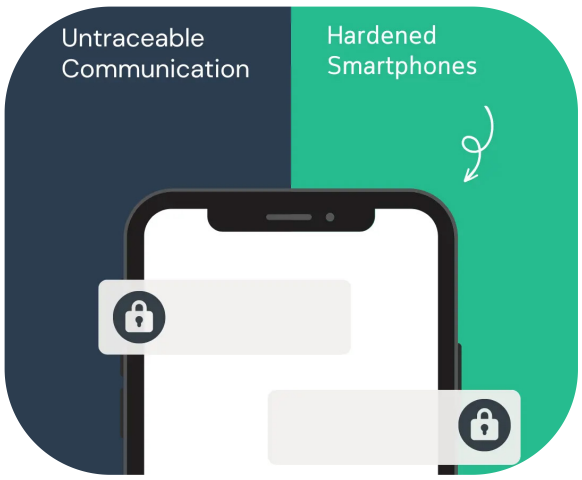
- **Untraceable and Authenticated:** Ensures untraceable and encrypted communication on GSM/CDMA local networks without carrier or device association, removing your signature from third-party servers.
- **Base Band Protocol-Free:** The phone operates without using the Base Band protocol, enhancing security.
- **Wi-Fi Encryption:** Wi-Fi connections are automatically encrypted through a proprietary non-attributable SDPN.
- **Encrypted Mail Configuration:** Available on any make and smartphone model (some phone models may increase quoted price).

Applications

- **Secure Communication Across Industries:** The Cipher Phone is designed for high-profile and privacy sensitive clients requiring intrusion and tracking resistant digital and voice communications globally.

User Experience

- The Cipher Phone offers a smooth user experience with secure communication, ensuring peace of mind in all environments.



Contact: office@entropya.com

ENTROPYA

IRON EDGE GATEWAY (IEG) ROUTER

Overview

Entropya's Iron Edge Gateway (IEG) is a quantum-ready router that isolates and hides everything connected behind it. The IEG provides untraceable digital super-highways through Entropya's global software-defined private network (SDPN). Unique to the IEG's design, it isolates and obscures digital signatures, masking them in the noise of the Internet's HTTPS (port 443) traffic. The IEG's trusted supply chain and firmware are cyber-hardened with fortified default configurations. The IEG uses post-quantum cryptography (PQC) protected tunnels that conceal the public IP, making your online presence disappear. Optionally managed through a robust attribution mechanism, the Iron Edge Gateway boasts leading-grade security, independently tested and verified. Entropya meets you where you are, simplifying complexity and delivering the highest security and performance possible.

Key Features

Seamless Connectivity

- The Iron Edge Gateway (IEG) seamlessly connects protected broadband Internet to local networks, acting as a DHCP server for internal devices. We meet you where you're at with what you have.
- Our IEG is also configured with the trusted pfSense firewall for seamless integration and enhanced security.

Entropya's Encrypted Network (EEN)

- The IEG Router authenticates to the Entropya Encrypted Network (EEN), an interconnected labyrinth of software-defined private pathways designed to protect your online activity. The EEN scales infinitely and works seamlessly with public, private, and commercial infrastructure to include data centers, cellular, space, and private Content Delivery Networks (CDNs).

Post-Quantum Cryptography (PQC)

- Entropya implements the highest grade protocols at the National Institute of Standards and Technology (NIST) PQC Security Level 5. The IEG and Entropya Encrypted Network (EEN) use the FIPS 203 Post-Quantum Cryptography protocol suite Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) 1024.

Dynamic Traffic Handling

- The IEG creates post-quantum encrypted tunnels for your internet traffic, making it the leading grade untraceable Internet access for all your connectivity needs. With customizable connection points and one-way routing, EEN ensures that your location and digital destination remain separate, enhancing privacy. In randomization mode, it obscures the public IP exit to the Internet by routing traffic through a hidden and distributed EEN, effectively eliminating both traceability and your attackable digital signature on both sides.

Benefits

- **Versatile Network Integration:** Seamless integration into any existing network infrastructure for flexible ease of use.
- **Cutting-Edge Security:** Enjoy digital freedom with a hidden IP address that makes you disappear from the Internet.
- **Scalability:** Whether securing a large enterprise or a small office, the IEG Router scales effortlessly to meet your needs—supporting up to 10 users with a Professional license and 100 users under an Enterprise license. Configurations continue to scale up to meet your needs.

Contact: office@entropya.com

ENTROPYA

PI EPSILON ARMORED COMMUNICATION PLATFORM

Overview

Pi Epsilon offers a cutting-edge decentralized, anonymous, end-to-end encrypted communication platform to include voice, text, video, chat, and group video conference through a proprietary configuration without third-party providers or their listening infrastructure. This includes apps and platforms like Wickr, Signal, Wire, and VOIP providers. The Pi Epsilon platform can be installed anywhere to include your location.

Key Features

Advanced Security

- The Virtual Dissimulated Encrypted Server (VDES) provides enhanced security, creating a decoy obfuscation environment that shields the real server IP address from potential threats. The platform seamlessly integrates with VoIP, enhancing communication capabilities.

Complete Control

- Maintains autonomy with no reliance on third-party providers or cloud backbone infrastructure, ensuring complete control over your communication platform.

Flexible Deployment

- Offers versatile deployment options such as a dedicated obfuscated Virtual Private Server (VPS), bare metal, Hypervisor, or any virtualized environment tailored to specific needs.

Seamless Connectivity

- Enables smooth communication between multiple Pi Epsilon servers, supporting a federated infrastructure for connectivity across networks.

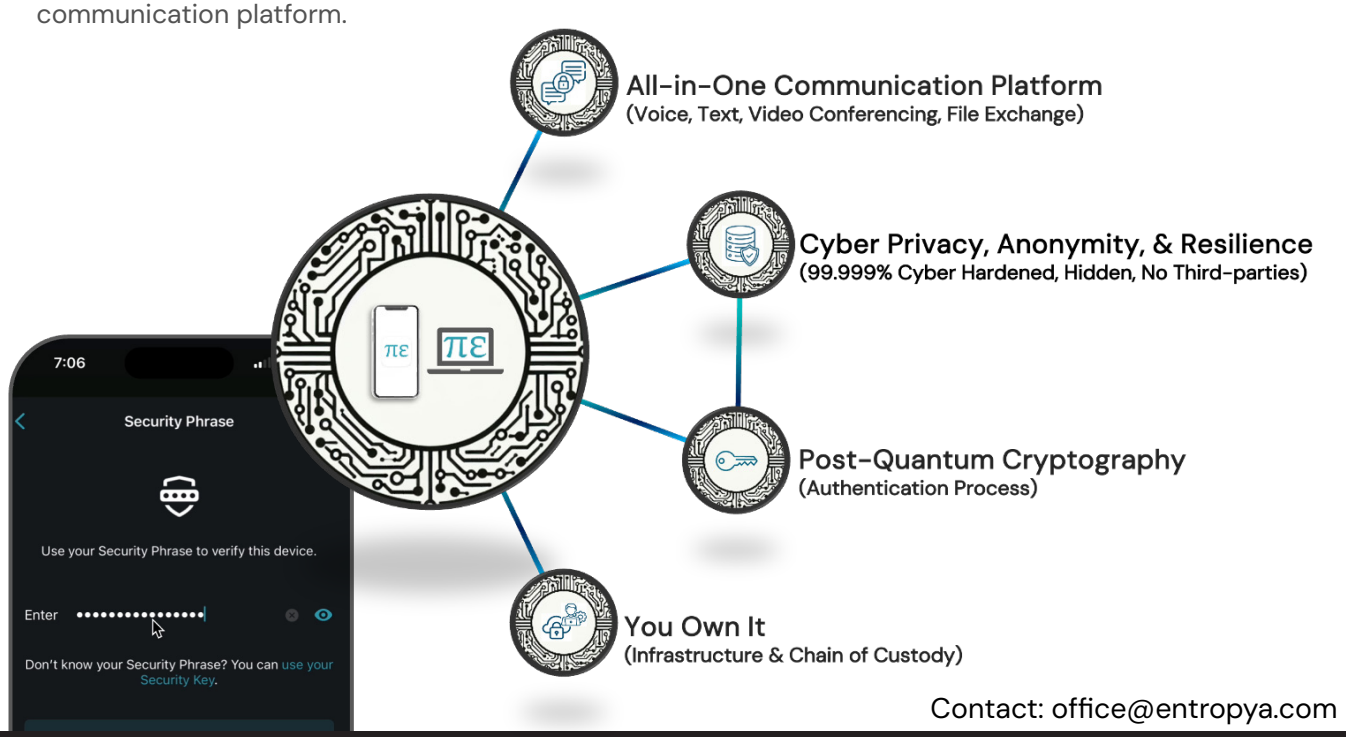
Benefits

- **Enhanced Privacy & Security**: Achieves a new level of privacy through obfuscated and decentralized communication with robust encryption.
- **Customized Deployments**: We tailor your deployment to your specific needs.
- **Complete Independence**: Not reliant on third-party providers, ensuring control over the communication platform.

Applications

Pi Epsilon addresses applications cross-cutting industries:

- Government & Defense.
- Finance, Legal, & Digital Transactions
- Telecom, IT, & Media Infrastructure
- Critical Infrastructure & Public Sector
- Manufacturing & Supply Chain



Contact: office@entropya.com

ENTROPYA

PI EPSILON USE CASES

1. Government and Defense Communications

- **Scenario**: Aircraft carrier port-call requiring commercial services and logistics from local vendors.
- **Use Case:** Real-time sensitive logistics coordination through commercial communications infrastructure. Pi Epsilon privately connects post-quantum secure voice, text, video, and file exchanges obfuscated through any digital infrastructure and end-to-end encrypted—optional bridges to platforms like WhatsApp and Signal.

2. Financial Sector

- **Scenario**: National and regional banks coordinating sensitive transactions and supporting documentation.
- **Use Case**: Financial organizations can use PiEpsilon to secure communications between branches and other corporate entities. Its decentralized nature ensures that sensitive data is not exposed to third parties.

3. Healthcare Industry

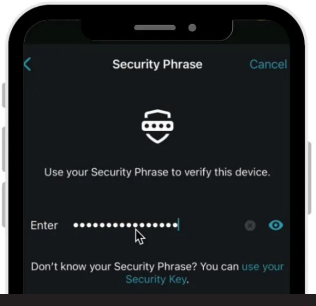
- **Scenario**: The healthcare industry needs to protect patient data and ensure compliance with regulations like HIPAA.
- **Use Case**: PiEpsilon enables secure communication of patient information, consultation sessions, and transfer of medical records. Its end-to-end encryption ensures that sensitive health data is kept confidential from threats.

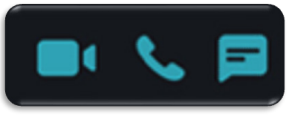
4. Legal Sector

- **Scenario**: Law firms and legal departments handle confidential client information and need to provide privacy and security.
- **Use Case**: Legal professionals can use PiEpsilon to communicate securely with clients, share legal documents, and conduct video conferences. The platform's ability to bypass third-party providers reduces the risk of data breaches.

5. Corporate Communications

- **Scenario**: Corporations require secure internal and external communication channels to protect intellectual property and strategic plans.
- **Use Case**: Companies can deploy PiEpsilon to facilitate secure communication among employees, partners, and clients. The platform's versatility allows it to be integrated into various IT environments, ensuring seamless and secure communication across the organization.





6. Critical Infrastructure

- **Scenario**: Operators of critical infrastructure need to safeguard communication channels to prevent cyber-attacks.
- **Use Case**: PiEpsilon provides a secure communication platform for operators of utilities, transportation, and other critical services. Its low probability of detection (LPD) and low probability of intercept (LPI) features enhance the security of critical infrastructure operations.

7. Remote Work

- **Scenario**: The rise of remote work requires secure communication tools to protect company data and employee interactions.
- **Use Case**: Remote teams can use PiEpsilon for secure video conferences, chats, and file sharing. The platform's end-to-end encryption ensures that remote communication remains private and secure, regardless of the employees' locations.

8. Research and Development

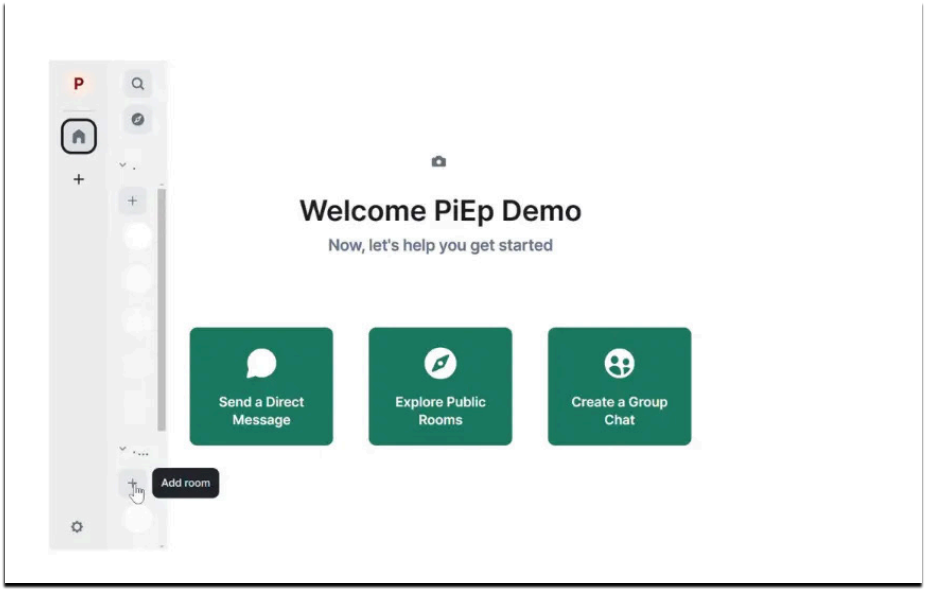
- **Scenario**: R&D departments need to protect proprietary information and research data from cyber espionage.
- **Use Case**: Researchers can use PiEpsilon to communicate securely about ongoing projects, share research findings, and collaborate on sensitive developments. The platform's post-quantum cryptography ensures that future quantum computing threats are mitigated.

9. International Organizations

- **Scenario**: International organizations require secure communication channels to coordinate activities and share information across borders.
- **Use Case**: PiEpsilon offers a secure communication platform that can be hosted in various locations, making it ideal for international use. Organizations can conduct secure video conferences, share documents, and communicate without the risk of interception.

10. Personal Use for High-Profile Individuals

- **Scenario**: High-profile individuals and celebrities need to protect their personal communications from privacy invasions.
- **Use Case**: Individuals can use PiEpsilon to ensure the security of their personal calls, messages, and media sharing. The platform's ability to bypass third-party providers prevents unauthorized access to their private communications.



Contact: office@entropya.com

ENTROPYA

DATA VAULT

Overview

The DATA VAULT Private Encrypted Data Storage Server is a robust solution designed to counter the imminent threats to traditional encryption methods posed by man-in-the-middle attacks and quantum computing. Available in multiple storage sizes (16 TB, 24 TB, 32 TB, 64 TB, 100 TB, 1 PB), it employs NIST standardized Post Quantum Cryptography (PQC) for superior data protection. With complete user control over data access, location, and management, DATA VAULT ensures the highest level of security for sensitive data at rest. Optional integration with the Virtual Dissimulated Encrypted Server (VDES) gateway and the Entropya Encrypted Network (EEN) further enhances protection by obfuscating endpoint addresses and redirecting traffic over randomized IPs.

Key Features

Quantum Ready Cryptography

- Protect your data with the NIST gold standard for Post Quantum resistant Cryptography. This advanced algorithm ensures data security against man-in-the-middle, supercomputers, and future quantum computing threats, surviving where other methods like RSA and AES fall short.

Flexible Remote Access

- DATA VAULT enables users to access, edit, and share their stored data remotely from any location. Customers maintain complete control over their data, providing flexible management while ensuring uncompromising security.

Hidden Storage

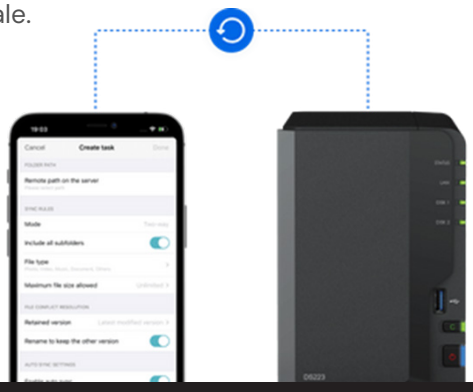
- Our Data Vault features a Virtual Dissimulated Encrypted Server (VDES) Gateway that sits between the ISP modem and the storage server. This setup protects your system from AI, machine learning predictions, and pattern-of-life analysis. It obfuscates real IP addresses and randomizes traffic across multiple pathways, enhancing your privacy.

User-Controlled Storage Anywhere

- The storage server can be installed at your preferred locations, ensuring that the data remains under your control, both digitally and physically.

Benefits

- **Quantum-Proof Security:** Ensures durable protection against quantum computing threats.
- **Privacy:** The VDES Gateway hides the DATA VAULT, protecting its real location, and shields against tracking and analytics.
- **Full Data Control:** Have complete confidence in quantum-ready secure private remote access from anywhere.
- **Scalable Storage:** 16 terabytes to petabyte scale.



Applications

Critical Data Backups:

- **Enterprises & Corporations:** Securely manage sensitive business data.
- **Healthcare Providers:** Protect patient data and ensure compliance.
- **Government & Defense:** Safeguard critical information with secure remote access.
- **Legal & Financial Institutions:** Quantum-safe storage for legal and financial records.

User Experience

- DATA VAULT features an intuitive interface, providing seamless remote access and data control. Advanced security features such as the VDES Gateway operate discreetly in the background, ensuring untraceability without added complexity. Securely manage your data with confidence.

Contact: office@entropya.com

ENTROPYA

DIGITAL DEAD DROP (D3)

Overview

The Digital Dead Drop (D3) Data Server offers a state-of-the-art solution for post-quantum cryptography (PQC) secured data management, synchronization, and backup across distributed networks worldwide. Built with a distributed architecture and protected by PQC, this platform ensures total confidentiality, integrity, and access, with seamless and HTTPS hidden synchronization of sensitive data across servers. The innovative architecture leverages a Software Defined Private Network (SDPN) to provide robust, untraceable data-at-rest and data-in-transit protection, setting new standards in cybersecurity.

Key Features

Distributed Server Architecture

- D3 operates on a fully distributed server platform ensuring resilience. It uses a global network of transit nodes for data synchronization, supported by the latest standard for PQC, combating man-in-the-middle attacks, supercomputers, & quantum computing.

Hidden Server

- Our D3 server integrates either an Iron Edge Gateway (IEG) or a Virtual Dissimulated Encrypted Server (VDES) Gateway between the Internet and the data server, ensuring data encryption at the gateway level, removing digital signatures and hard selectors. This eliminates dependencies on third-party service providers and further enhances security. Both VDES and IEG ensure zero detection or interception during the backup synchronization process.

Robust Backup Feature

- D3 offers a highly secure backup system through a secondary destination server using separate encrypted SPDN routes. Data is routed through various locations (e.g., Frankfurt, New York) and segregated via the VDES gateway.

Global Data Synchronization

- The synchronization process spans multiple global transit servers (e.g., London, Singapore, Amsterdam) using randomized IP addresses and quantum-ready cryptography, securely synchronizing data. This ensures requests are handled across separate software-defined and randomized private superhighways, making data breaches nearly impossible.

Benefits

- **Uncompromising Performance:** Enjoy high performance and protection simultaneously.
- **Leading Grade Security:** Harden to 99.999% security and become durably quantum ready.
- **Seamless Global Synchronization:** Resiliently synchronize data globally and hide as HTTPS traffic.
- **Unparalleled Data Integrity:** Our decentralized and PQC SDPN prohibits tampering and interception.
- **Scalability:** 16 terabytes to petabyte scale.

Applications

- **Finance:** Secure sync and backup.
- **Healthcare:** Protect, update, and archive sensitive patient records and medical data.
- **IoT Networks:** Safeguard and sync data from IoT devices across distributed networks.
- **Government & Defense:** Ensure critical data security for national defense infrastructure.
- **Critical Backups:** Prevent loss and secure data with write-only immutable backups.

User Experience

- The D3 platform offers seamless integration with minimal user interaction. Data invisibly synchronizes and backs up, blending in with HTTPS traffic.

Contact: office@entropya.com

ENTROPYA

VIRTUAL DISSIMULATED ENCRYPTED SERVER (VDES)

Overview

The Virtual Dissimulated Encrypted Server (VDES) is a platform designed for maximum concealment. It hides the real endpoint IP address and infrastructure. The VDES acts as a traffic redirector by accepting connections from end-user devices. It generates an encrypted tunnel, employing the Post-Quantum Cryptography (PQC) gold standard, FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) over a private IP, and redirects the traffic through an internal encrypted tunnel to a non-routable IP server. This infrastructure is built and configured according to the highest security standards, incorporating multiple layers of protection, including an Intrusion Detection System (IDS) and Disaster Recovery. Unlike other providers, the VDES can be optionally configured to provide highly secure direct access to historical and live logs and records through a unique SSH key, ensuring complete oversight and compliance for the most sensitive Zero Trust needs.

Key Features

Traffic Obfuscation

- VDES serves as a traffic redirector, concealing the real endpoint IP address of landing servers.
- Operates web servers on masked ports, blending seamlessly with cyberspace noise.
- Reveals only two open ports during external cyber scans for enhanced external security.

Decoy Obfuscation Tool (DOT)

- Creates a symbolic link for the PQC certificate connection, rendering destination servers non-routable.
- Conceals the IP address of destination servers from the outside cyber world.

Post-Quantum VPN Technology

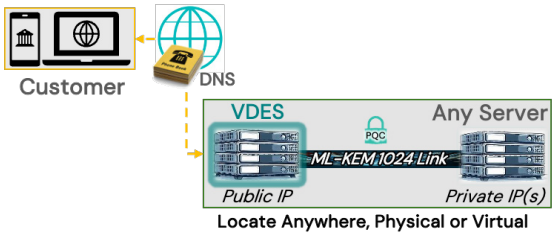
- Features a proprietary VPN server with ML-KEM, National Institutes of Standards and Technology (NIST) Security Level 5 technology, as ML-KEM 1024.
- Generates a single PQC certificate with no DNS resolution for added obfuscation.
- Exported certificate is hard-coded onto destination servers, ensuring a singular coupling.

Multi-Layered Security Configuration

- The PQC-KEM VDES is armored with multiple security layers, enhancing overall protection.
- Conveys no unique digital signatures, further contributing to its cyber stealth.

Benefits

- **Maximum Security**: The PQC-KEM protected VDES offers robust security layers, Post-Quantum Cryptography, and decoy obfuscation, ensuring your digital assets remain safeguarded from persistent and advanced cyber threats.
- **Stealth Operation**: The solution operates discreetly, concealing proprietary digital signatures and 99.999% reduction to the vulnerable attack surface.
- **User-Friendly Integration**: With a user-centric approach, the VDES seamlessly integrates into your existing infrastructure, providing a secure and transparent experience for end-users.



Locate Anywhere, Physical or Virtual

Applications

- Ideal for securing unique servers and services such as blockchain, web, VOIP, Citrix, and database access.
- Suitable for environments where IP obfuscation and protection against advanced cyber threats are paramount.

User Experience

- Device requests an HTTPS session that directs it through automatic DNS routing to the VDES.
- The VDES relays through an ML-KEM tunnel to the protected server to complete the request and authentication.

Contact: office@entropya.com