CRYPTO | CYBER SECURITY PORTFOLIO

KRYPTUS
shaping trusted bonds

ABOUT KRYPTUS.

Kryptus was founded in 2003 with a mission always to be ahead of threats, protect the status quo, and constantly innovate to generate and boost value and business opportunities. In its journey to shape trustworthy relationships among nations, companies, and individuals, Kryptus strives to ensure a secure environment so our customers can focus on their communications and data.

A BRAZILIAN-SWISS COMPANY WITH A GLOBAL PRESENCE.

Kryptus provides encryption and cybersecurity solutions worldwide for defense, intelligence, government, and private sector customers. Through projects integrating hardware, software, and services, Kryptus offers highly customizable, reliable, and secure solutions with cutting-edge technology, free from all surveillance laws.

INNOVATION AND TRUST ALWAYS AHEAD OF THREATS.

In 2020 Kryptus received a relevant contribution from the Aerospace Investment Fund (FIP), of which Embraer is the primary investor, to accelerate its innovative portfolio further and expand the operations territorially. Furthermore, in a strategic partnership with the Swiss company Kudelski Security, Kryptus complemented its portfolio with advanced research, development, and consulting services.

The Brazilian Ministry of Defense recognizes Kryptus as a "Strategic Defense Company" and the Gartner Institute as a "Cool Vendor," which are testimonies of the company's capabilities to operate in a rigorous military environment and also provide the same high-level security to business segments such as digital certification, banking and payments, and e-commerce.

KNET HSM

NEXT-GENERATION HARDWARE SECURITY MODULE

kNET is a high-security multipurpose device designed to offer a tamper-proof, scalable, and high-performance environment for cryptographic keys' storage, management, and operations. With FIPS 140 level 3 certification, kNET meets the most demanding security and auditing requirements to eliminate risks and vulnerabilities in data protection and the execution of critical applications.

VIRTUAL HSM.

Ready for environments with high availability, kNET features superior performance and the unique ability to create and execute virtual HSMs with true logical isolation in a multi-tenant environment, segregating sets of keys, users, and applications.

CLOUD HSM.

Kryptus offers HSM as a Service through competitive models to allow access to an ultra-secure and scalable infrastructure, regardless of the size or necessity of the operation. Its native KMIP (OASIS Key Management Interoperability Protocol) API facilitates integrations within the most diverse business scenarios, resulting in an agile deployment.

PAYMENT.

kNET HSM is designed to meet all auditing requirements for PCI-DSS compliance and features pre-integrated payment and banking applications to streamline the setup of new card-based operations.

The solution features a TR-31 key cluster, an added layer of security for quick identification of forged keys.

PUBLIC KEYS INFRASTRUCTURE.

kNET HSM offers high operational performance and secure storage for up to 2.5 million objects, making it perfect for Trusted Service Providers.

Kryptus can also support national authorities in creating and operating the official public key infrastructure and the internal certificate authorities of private, public, or defense institutions with a complete solutions portfolio.

TIMESTAMP SOLUTIONS.

Kryptus TAS: Time Source Master Clock Synchronism and Auditing System, used by the Root Time Authority for time source management, timestamps networks, and audit trails storage. The kNET HSM Cryptographic Security Module completes the solution by protecting Kryptus TAS cryptographic keys.

Timestamp Server that complies with RFC 3161 and has all the functionality required by a timestamping authority for managing and generating timestamps. It also relies on the kNET HSM to protect Kryptus TSS cryptographic keys by registering synchronization data and timestamp signatures.

Kryptus systems offer a web interface and custom-development APIs to make it easier to manage them all.
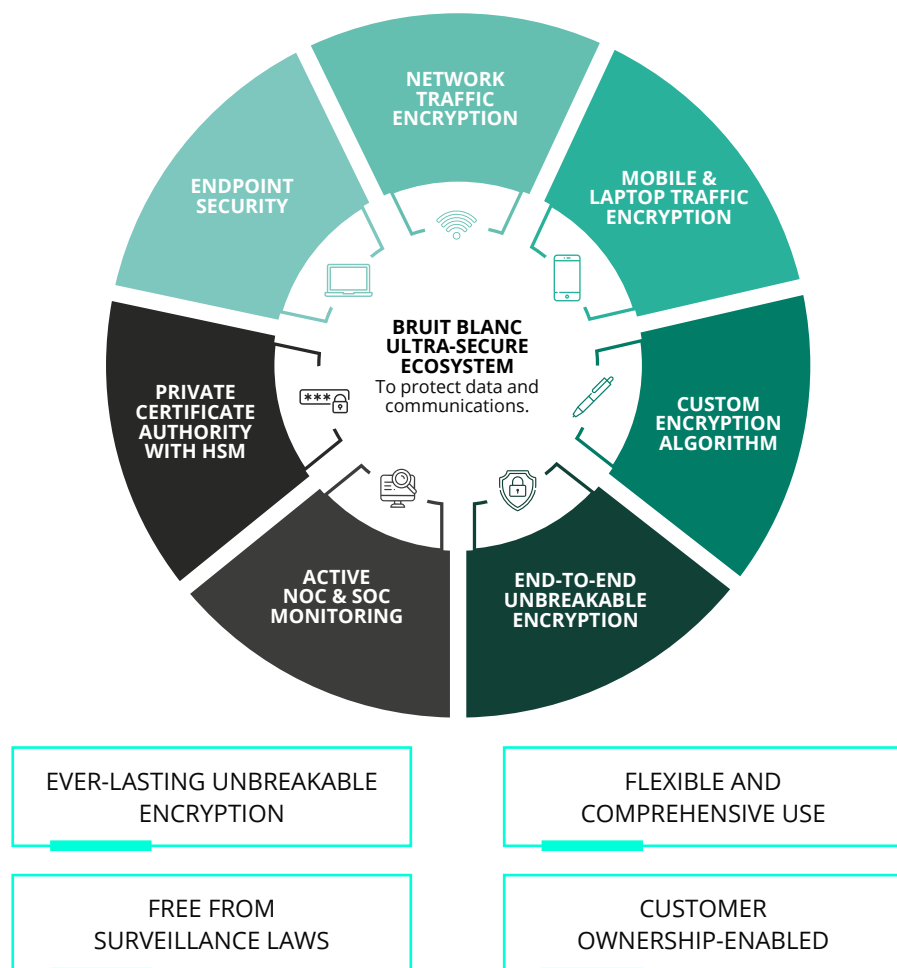
KRYPTUS KMS

KEY MANAGEMENT SOLUTION FOR DATA PROTECTION

Kryptus KMS solution combines cryptographic key lifecycle orchestration and automatic encryption application with the high performance hardware-based security of kNET HSM for secure key handling and processing.

By managing and distributing cryptographic keys, the Kryptus KMS solution controls the use of keys for applications, databases and communications. Besides the modules for tokenization, masking, and encryption to protect structured or unstructured data wherever it resides, the solution includes databases connectors, data discovery, and classification features.

BruitBlanc

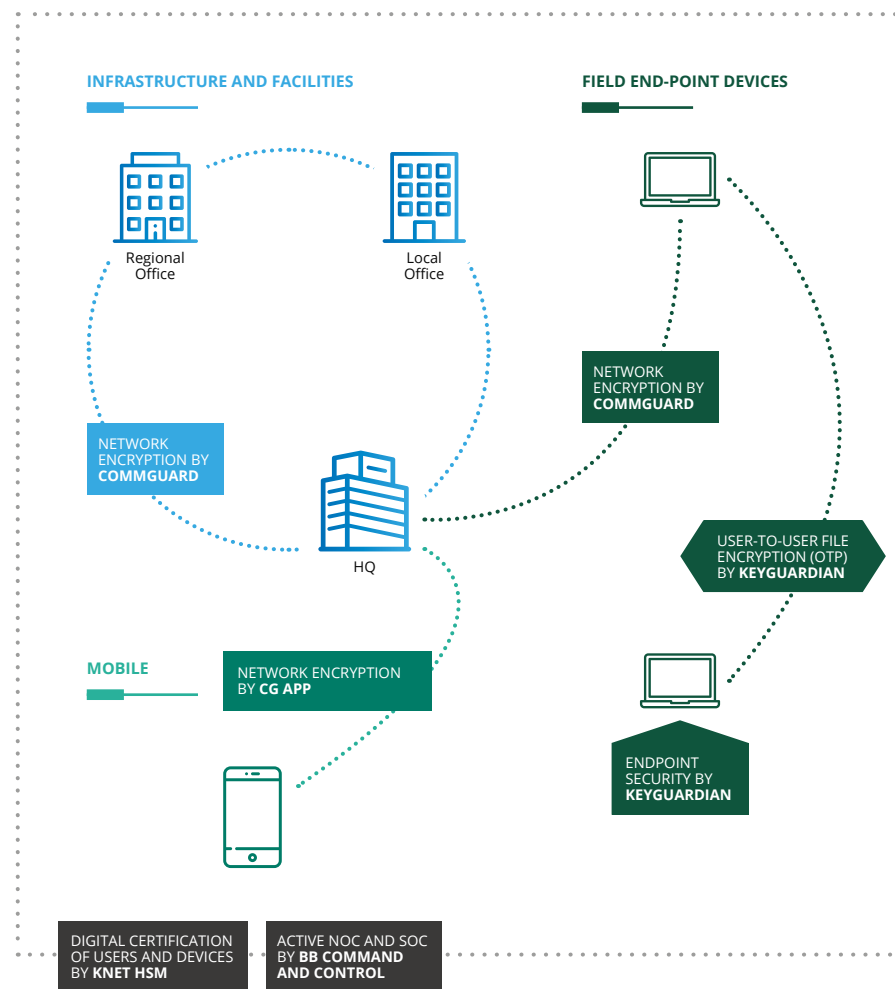ULTRA SECURE ECOSYSTEM TO PROTECT
DATA AND COMMUNICATION

BruitBlanc is a complete ecosystem for high-level security and performance to protect critical data, information, and communication in any kind of infrastructure.

**BRUIT BLANC
ULTRA-SECURE
ECOSYSTEM**
To protect data and
communications.

- NETWORK TRAFFIC ENCRYPTION
- MOBILE & LAPTOP TRAFFIC ENCRYPTION
- CUSTOM ENCRYPTION ALGORITHM
- END-TO-END UNBREAKABLE ENCRYPTION
- ACTIVE NOC & SOC MONITORING
- PRIVATE CERTIFICATE AUTHORITY WITH HSM
- ENDPOINT SECURITY

EVER-LASTING UNBREAKABLE ENCRYPTION	FLEXIBLE AND COMPREHENSIVE USE
FREE FROM SURVEILLANCE LAWS	CUSTOMER OWNERSHIP-ENABLED

INTEGRATED SOLUTIONS.

BruitBlanc combines software and hardware cryptographic solutions in a flexible, modular and integrated architecture to address multiple use cases and the specific scenarios of each organization.

Organizations can establish secure network connections between multiple sites and remote users by combining dedicated encryption devices and applying unbreakable end-to-end OTP encryption over files and messages. A central graphical interface manages all.
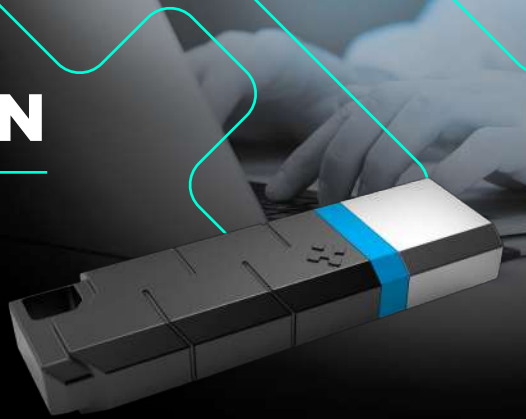

INFRASTRUCTURE AND FACILITIES

FIELD END-POINT DEVICES

Regional Office

Local Office

NETWORK ENCRYPTION BY **COMMGUARD**

NETWORK ENCRYPTION BY **COMMGUARD**

HQ

USER-TO-USER FILE ENCRYPTION (OTP) BY **KEYGUARDIAN**

MOBILE

NETWORK ENCRYPTION BY **CG APP**

ENDPOINT SECURITY BY **KEYGUARDIAN**

DIGITAL CERTIFICATION OF USERS AND DEVICES BY **KNET HSM**

ACTIVE NOC AND SOC BY **BB COMMAND AND CONTROL**

All Hardware is Tamper Resistant and accepts Own Algorithm

KEYGUARDIAN

ONE-TIME PAD (OTP) ENABLED PORTABLE CRYPTOCOMPUTER

KeyGuardian is a portable hardware security device designed to protect communications, encrypt documents and partitions, and securely store credentials on the go.

With a modern and compact design, KeyGuardian can be easily carried and used anywhere, offering the highest protection with OTP, customer-specific algorithms, Post-Quantum Cryptography, or standard AES, RSA.

COMMGUARD

NETWORK ENCRYPTOR

CommGuard 3 is a layer 2 and 3 network encryptor designed to meet the most stringent security requirements for serious communication among HQ, sites and remote operations, protecting all IP traffic.

CommGuard 3 supports standard and proprietary algorithms, and also offers an easy and autonomous way for organizations to customize algorithms.

UNBREAKABLE OTP ENCRYPTION

EASY-TO-USE

MULTIPLE FUNCTIONS

MULTI-PLATFORM

HIGH PERFORMANCE

POST-QUANTUM READY

COMPATIBLE WITH KEYGUARDIAN FOR SECURE REMOTE CONNECTION AND ACCESS

CUSTOMIZED ALGORYTHMS

EASY-TO-DEPLOY

ANTI-TAMPER PROTECTION

POST-QUANTUM READY

PROTECTION ANYWHERE.

- Secure storage of critical files and information on missions and at remote locations
- Protection of confidential documents
- Top-secret messaging using OTP
- Sign and protect the integrity of documents on the go
- Secure access to headquarters services including real-time communication
- Endpoint security based on hardware

HIGH-SECURITY IP COMMUNICATION.

- Flexible, full-mesh communication topologies
- Military operations
- Multi-platform management interface
- HQ and branches synchronization
- High-performance network encryption
- Counter-SIGINT

CG APP

NETWORK ENCRYPTOR FOR MOBILE AND LAPTOP

CG App is a layer 3 network encryptor designed for mobile and laptop devices with the same software capability of CommGuard to protect the exchange of classified communication during travels or missions.

• One touch configuration and connection

• Filter applications that will use the secure network

• It is capable to connect to physical CommGuard or Keyguards

• Support customer proprietary algorithms

• Support mobile and laptop operational systems

BB C2

COMMAND AND CONTROL SYSTEM

The Command and Control System includes Security Operations Center and Network Operations Center functionalities for monitoring and detecting incidents on corporate assets.

• Dashboards

• Key NOC and SOC functions

• Security alerts

• Certificate issuance

• BruiBlanc components can be configured with a single click

• Native integration with BruitBlanc components, with the ability to expand to other external IT assets

DEFENSE PROGRAMMES

Kryptus has extensive experience in Defense Projects, from tactical to strategic applications, with a unique technology transfer (ToT) approach, widely verifiable, to provide the customer's autonomy and the protection of nations' sovereignty.

Following are some examples of use cases for the Kryptus on-demand development and consulting competencies:

CRYPTO-COMPUTERS

IDENTIFICATION AND AUTHENTICATION SYSTEMS

STATE ALGORITHMS

RISK AND VULNERABILITY ANALYSIS

ENCRYPTION MODULES

SECURE COMMUNICATION.

RDS-DEFESA: VEHICLE SDR RADIO.

Kryptus is responsible for the risk analysis, assurance, development, and implementation of a crypto-computer to protect Software Defined Radio cryptographic keys and algorithms, promoting secure interoperability between communication equipment for the Brazilian Army.

LINK BR2: DATA LINK SYSTEM.

Kryptus is responsible for the cybernetic security and airborne encryption solution that aims to provide secure communication (confidential and authenticated) between aircraft and ground stations of the Brazilian Air Force, based on the operational concept of the Air Force's digital link communications system.

SENSOR AND MONITORING.

SISFRON: INTEGRATED SENSING SYSTEM.

Kryptus supplies the encryption subsystem of the SISFRON project, Integrated Border Monitoring System of the CCOMGEX (Brazilian Army Electronic Warfare and Communications Center), including link encryption equipment with national technology (CommGuard).

IFFM4BR: IDENTIFICATION, FRIEND OR FOE.

Kryptus developed the Cryptographic Module for the Brazilian Air Force friend or foe identification system by employing proprietary algorithms to generate challenges and responses signals which allow a secure classification of military platforms in air, land, and sea.

INTEROPERABLE NETWORK.

NOVA ROD: DEFENSE OPERATIONAL NETWORK.

Kryptus is responsible for the restructuring, cryptographic security, monitoring and technical support of the Defense Operational Network that provides voice, data and support services to military decisions in an integrated and secure way.

CYBER DEFENSE

Kryptus has experience in delivering turn-key Cyber Defense Operation Centers with protective, intelligence, and offensive capabilities, from planning to assisted operations.

OFFENSIVE CYBER OPERATIONS.

Kryptus assists Defense clients in achieving appropriate readiness levels for current and future cyber warfare challenges from a strategic to a tactical and operational standpoint.

- Cyber Operation Command: project, deployment, and operation services
- Advanced labs for malware and forensics
- Development of custom cyberweapons
- Advisory services

DEFENSIVE CYBER OPERATIONS.

Kryptus offers multiple solutions and services to protect, monitor, analyze, and respond to cyber threats, disruptions, unauthorized activities, cyber-attacks, and degradation of services.

- Cyber Operation Command: designing, deploying, and operating services
- Evaluation of the cybersecurity status
- Deployment of incident response Technologies
- Co-development and full technological offset

INTELLIGENCE CYBER OPERATIONS.

Kryptus integrates open-source intelligence (OSINT), social media intelligence (SOCMINT), and human intelligence (HUMINT) into clients' technological environments, providing them with all the needed information for their decision-making.

- Staff training
- Deployment of cyber intelligence solutions
- Integration and subscription of intelligence feed services
- Continuous searches of social, deep, and dark web sources, underground forums, and black markets.

BladeRunner

COUNTERINTELLIGENCE PLATFORM IN YOUR HANDS.

Blade Runner is an innovative counterintelligence platform designed for the preventive protection of individuals, organizations, and nations against actions of terrorism, cybercrime, espionage, and misinformation.

Using artificial intelligence algorithms and machine learning techniques, Blade Runner assists public and private organizations by collecting and analyzing information from the behavior of profiles in social networks to identify potential threats, vulnerabilities, and abnormal connections that may impact the organization or specific individuals.

Blade Runner can combine open data from social networks with corporate sources and intelligence professionals' knowledge into an intuitive and friendly interface to generate relevant discoveries and insights.

Highly customizable, it can be easily configured to meet various use cases, allowing preventive actions and reducing the risk of compromise. In addition, Blade Runner is a stand-alone platform and free from surveillance practices.

- ✓ Analysis of connections and interactions in multiple social networks
- ✓ Exposures and vulnerability assessments for potentially compatible members from the organization
- ✓ Automatic detection of malicious avatars
- ✓ Suspicious approach alert
- ✓ Profiles' classification (human vs. avatars)
- ✓ Identification of adversary intelligence activity
- ✓ Detection of influencers
- ✓ Analysis of influence campaigns
- ✓ Automatic management of operative and functional avatars

CYBER SECURITY

KRYPTUS cultivates a team of accredited experts in cybersecurity to find and mitigate vulnerabilities in any type of organization.

STRATEGIC SERVICES.

360° EVALUATION.

Identification of the main gaps in terms of maturity on information security and regulatory compliance, taking into account people, processes, and technology.

CODE REVIEW.

An essential practice in the secure software development cycle, Kryptus conducts secure code reviews for any language and platform available in the market.

PENTEST.

Identification and mapping of existing vulnerabilities in applications and infrastructure elements, assessing potential damage in the event of actual exploitation or invasion and recommending measures and procedures for risk mitigation and remediation.

VULNERABILITY ANALYSIS.

Kryptus helps organizations to identify flaws and vulnerabilities present in the environment automatically.

BUILDING-A-SOC.

Kryptus helps organizations design and implement a SOC - Security Operations Center - with all the necessary infrastructure for the internal IT and cybersecurity teams to detect, analyze, and respond to threats and security incidents.

MANAGED SERVICES.

SOC AS A SERVICE.

Remote execution of managed services at Kryptus Security Operations Center (SOC) or in the customer's environment.

- 24/7 operation for incident monitoring, detection and response

- Red and Blue team, imitating invaders and counterattacking

- Threat hunting in infrastructure elements and cloud environments

- Next-generation tools as a service

- Compliance Management

- Flexible to meet the concept of Cybersecurity mesh

WE ARE INNOVATIVE.
WE BUILD TRUST.

Recognized as a trustworthy partner in the most different scenarios, **KRYPTUS** leads technology to the next level to change the world.

- ✓ Cutting-edge technology is in constant evolution
- ✓ Reliable competencies for critical projects
- ✓ Customizable solutions with unbreakable cryptography
- ✓ Neutral positioning, free from surveillance law

KRYPTUS
shaping trusted bonds

INNOVATION AND TRUST
ALWAYS AHEAD OF THREATS