ENCRYPTION CONSULTING
www.encryptionconsulting.com

360°
Encryption Services

What we do?

Encryption Consulting is a customer focused cybersecurity firm that provides a multitude of services in all aspects of encryption for our clients. Our expertise ranges from

- Public Key Infrastructure
- Transparent Data Encryption
- Hardware Security Modules
- Enterprise Key Management
- Cloud Key Management
- Element Level Format Preserving Encryption
- Tokenization
- Code Signing

Our knowledge and experience puts experts on your team to deploy the industry's best and proven encryption technologies. Our solutions will secure your sensitive data throughout its entire lifecycle.
At Encryption Consulting, our people and services enable organizations to succesfully achieve their data security goals in **Confidentiality, Integrity and Availability.**

Encryption Consulting in Brief

- Experts in Encryption and Data Security Space
  - **30+ years** of combined experience in cyber security
  - 70% of firm holdinng **CISSP, CCSP, CIPP/US Certified Information Security Professsional**
- **Strategic partners** with leading encryption technology providers
- **20+ clients** including some of the **Fortune 100** and **Fortune 500** companies
- Most of our consultants have a **Big 4 (Delloite, PWC, EY, KPMG)** consulting background

Why do Organizations Need Data Encryption?

The two main drivers for data encryption across most industries are compliance and business risk reduction. We focus on protecting Personally Identifiable Data (PII) or any other sensitive data.

Compliance Drivers

- PCI
- HIPAA
- General Data Protection Regulation (GDPR)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bille Act 1999 (GLBA)
- Fair Credit Reporting Act 1970 (FCRA)
- Family Educational Rights and Privacy Act (FERPA)

Business Risk Drivers

- Intellectual
- Property Theft
- M&A Information Leak Reputational Damage from Data Theft (E.g. Sony)
- Fines and Incident Response Costs with Data Breaches (E.g. Target)
- Damages resulting from Unsecure Internet of Things

Data-at-Risk

- Patient Health Records
- Education Records
- Compensation Data
- Credit card and bank account numbers
- Social security numbers
- Username and password
- Intellectual Property
- Internet of Things Data
- M&A Data

Focus Areas

Our specialty is delivering Assessments, Strategies, and Implementations for organizations who either lack the specialized resources or who simply value having a trusted advisor to assist them upgrade their data security posture. At Encryption Consulting, we have created a custom framework based on NIST 800-57, NIST 800-53 standards, FIPS and industry best practices to accelerate our client's data protection projects. In summary, we enable organizations to identify areas in their current encryption environment needing improvement by conducting an assessment, creating a roadmap, and implementing an encryption plan end-to-end.

Client Requests

- Sensitive Data Identification and Classification
- Enforcement of data protection controls - Encryption, Tokenization, or Masking
- Expert advice on Implementation strategy and services
- How to comply with encryption standards and follow industry best practices
- Encryption compliance & regulation, robust management, reporting and Integration
- Customized & focused training based on customer environment

Our Services

Encryption Advisory Services

Assessment: Evaluate organization's state of encryption and provide recommendations for current & future initiatives

Strategy:
Determine short term and long term objectives and roadmap.

RFP Development and Proof of Concept: Develop the request for proposal in detail and provide evaluations of bidding service providers . Coordinate the POC with client team and selected service providers and establish evaluation criteria.

Implementation: The design and implementation of encryption program governance, encryption and key management solutions, modernization of business processes, and management of project schedules to support the encryption strategy and roadmap.

With a phased approach to encryption implementation at an enterprise level we will :

- Develop detailed requirements and design
- Perform vendor evaluations and Proof of Concept (PoC)
- Install and configure encryption solutions
- Deploy and integrate solutions as well as migration
- Implement key management practice
- Assist with operational transition

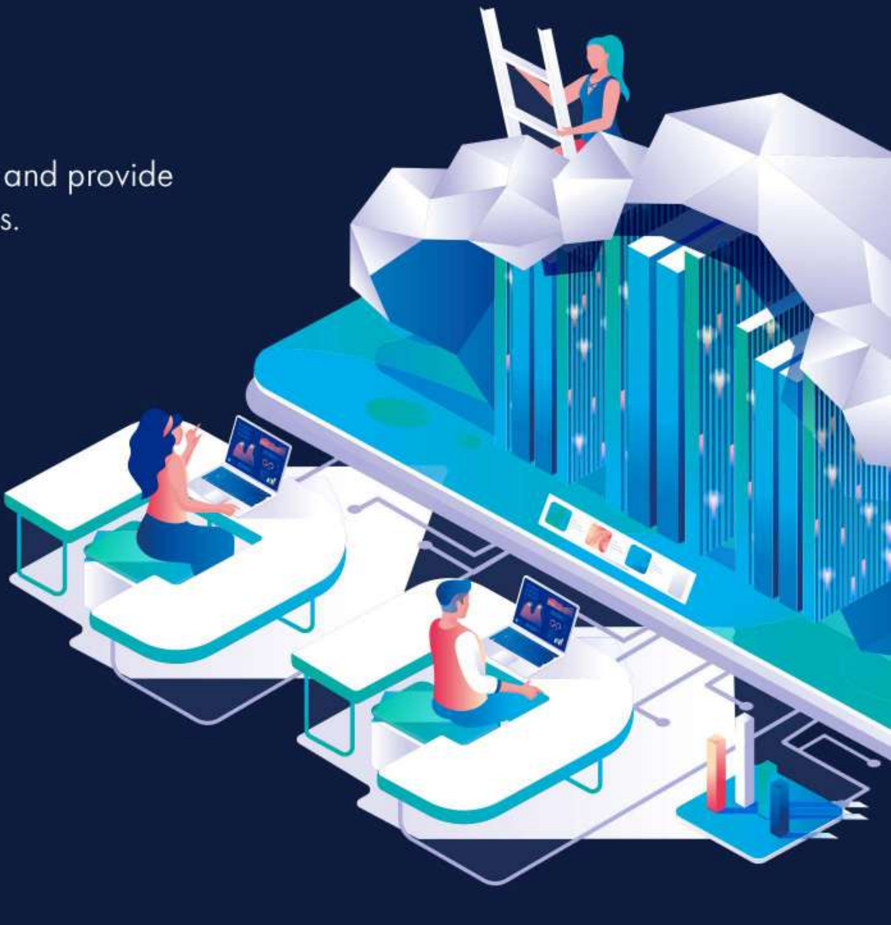
Public Key Infrastructure

Assessment: Evaluate the maturity of PKI state and provide recommendations for current & future initiatives.

PKI Design Implementation:
- Service Design
- Logical Design
- Physical Design

PKI Certificate Policies (CP) and Certificate Practice Statement (CPS) Development:

- Develop CP documents and CPS documents
- Outline associated security policies based on best practices



Hardware Security Module

HSM Infrastructure Assessment: Evaluate the maturity of HSM system state and provide recommendations for current & future initiative

HSM Design Implementation:

- Design & Implement Safenet, Thales, and Ultimaco hardware security
- Achieve FIPS 140-2/ L3

Migrating to Cloud HSM:

- Help customer migrate from on-premise to cloud HSM

Amazon Web Service Key Management Service (AWS KMS)

Assessment: Evaluate the maturity of the AWS key management system against a defined framework and comparative organizations. Provide recommendations for current and future key management initiatives.

Strategy: Create a long term strategy and roadmap for the program based on objective and scope set forth from executives and management.

Implementation: Create key usage policies for Customer Master Keys(CMKs) and Data keys. Import keys from third party key management and HSM (Hardware Security Module) solution to AWS by using bring your own keys (BYOK) feature.

Microsoft Azure Key Management Service (Key Vault)

Assessment: Evaluate the maturity of Azure key management system against a defined framework and comparative organization. Provide recommendations for current and future key management initiatives.

Strategy: Create a long-term strategy and roadmap for the program based on objective and scope set forth from executives and management.

Implementation: Create key usage policies. Import keys from HSM (Hardware Security Module) solution to Azure Key Vault by using Bring your own keys (BYOK) feature.

Microfocus Voltage Secure Data

Microfocus voltage is a leading vendor in Format preserve encryption, Tokenization and technology landscape

Assessment: Evaluate and review customers sensitive data types and determine the spread of sensitive data lineage across enterprise.

Strategy: Evaluate the business need to confirm which data protection method including FPE, tokenization or obfuscation would be best suited. Prioritize applications and databases and create a data remediation plan for the enterprise.

Implementation: Deploy Voltage SecureData appliance and perform pilot with one to two applications. Based on insights gained, develop the application onboarding process, and integrate it with existing business and technology practices.

Vormetric Data Security Manager

Vormetric is a leading vendor in data at rest encryption and centralized key management technology landscape

Assessment: Assess customer's existing environment and confirm different type of databases and data sources. Develop data at rest encryption use cases.

Strategy: Determine the footprint of data sources spread across on-prem and multiple cloud environments. Prioritize the data at rest encryption use cases and evaluate what can be achieved using Vormetric Data Security Manager and VTE.

Implementation: Develop a phased approach for the deployment of VTE agents. Determine the size of databases and plan the encryption time for them accordingly. Create encryption keys and policies in DSM in and apply them to databases.

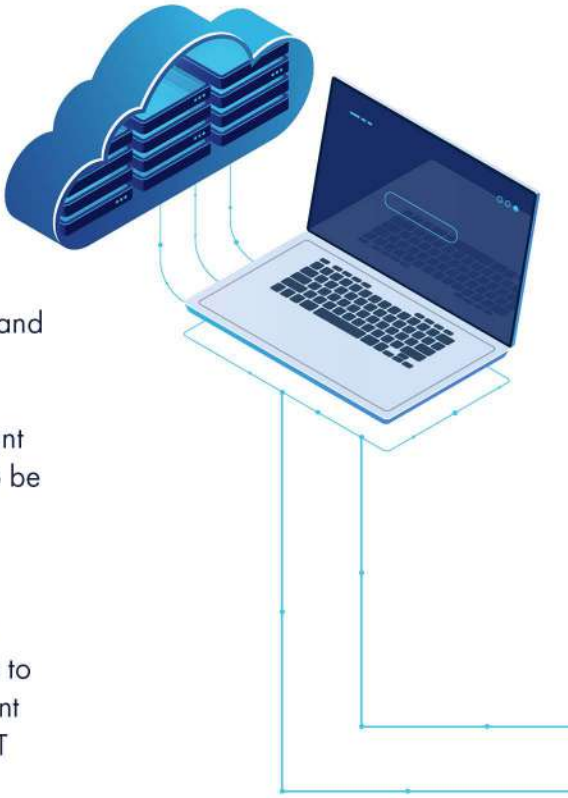
Protegrity Services

Assessment: Evaluate and review customers current state of selected business and IT businesses for Tokenization, Format-Preserving Encryption, Data obfuscation and other data protection controls.

Strategy: Develop a strategy and roadmap to build a robust data encryption program using MicroFocus Voltage Secure Data technology that is integrated with the existing security program to address gaps and achieve desired maturity.

Implementation: Understand requirements and develop cryptographic policies and rules in alignment with business requirements. Then begin by designing, implementing, and transferring sustainable supporting processes focused on efficiently and effectively responding to NIST 800-57 framework.

Hashicorp Vault



Assessment: To be able to run the effective platform assessment service, it is essential to review the current state of the selected business context and its IT context, and their readiness for Secret Management, encryption -as-a-service, and identity access management.

Strategy: We perform an evaluation on leading vault vendors, based on relevant evaluation framework, and documents the top three most suitable candidates to be further selected by the customer.

Implementation: We build platform specific manuals and maintenance guides specific to our clients. In addition, we provide engineering and support services to customers during the rollout phases, i.e., integration of vault's secret management and encryption service with the customer's mission-critical business processes, IT software & solutions, and application landscape.

Comforte Data Security Platform

Assessment: To be able to roll out the efficacious platform assessment service, it is quintessential to review the Client's business and IT context, and their readiness for data-centric security, Format-Preserving Encryption, Data masking, and other data protection controls.

Strategy: We develop a strategy and action plan that leverages the data discovery, classification, integration, and protection strengths of the comforte's Data Security Platform to achieve data security objectives set by the customer's leadership team.

Implementation: We believe that to execute the objectives outlined in the implementation roadmap, defining the process known as an implementation plan is a must to bring the roadmap to life. After understanding the business and service risks and concerns obtained from the customer, we develop a plan and deliver the solution for achieving the desired

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and integrating our solutions with their products and services. We also pride ourselves on our flexibility and are always open to help our clients achieve their data security success with the technology of their choice. If you have products and services already deployed or are considering, we'd be glad to help you evaluate these to get the most out of your investment.

NCIPHER

nCipher Security, a leader in the general purpose hardware security module market, is now an Entrust Datacard company, delivering trust, integrity and control to business critical information and applica tions.

THALES

Thales-e-Security is a leader in encryption, advanced key management, tokenization, privileged user control and meets the highest standards of certification for high assurance solutions.

Fortanix

Fortanix is a leader in runtime encryption and it protects applications even when the infrastructure is compromised.

KEYFACTOR

Keyfactor has its roots in the trenches of IT security, deployment and operations. We understand how companies work because of our deep industry experience-we know firsthand the challenges of competing agendas, budget constraints and time pressures.

Microsoft

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington.

MICRO FOCUS

Micro Focus and HPE Software have joined to become one of the largest pure-play software companies in the world.

CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile.

gemalto
security to be free

For those shaping the digital interactions of tomorrow, we provide the digital security that enables the trusted connections of today.

FORNETIX

Fornetix Key Orchestration TM is a scalable and flexible solution designed to simplify key management. Granular policy tools, user access controls, and powerful automation enable organizations to manage hundreds of millions of encryption keys while integrating seamlessly with existing technology investments.

appviewX

AppViewX is revolutionizing the manner in which NetOps and SecOps team.

PrimeKey

PrimeKey's technology is used by organiza-tions and enterprises to securely implement PKI solutions used for ePassports, eBanking, ePayment, mobile/Internet security, IoT and more.

UNBOUND
(MATH OVER MATTER)

Unbound protects secrets such as cryptographic keys, credentials or private data by ensuring they never exist in complete form

VENAFI

Venafi Cloud helps organizations prevent outages and secure their keys and certificates

utimaco

Utimaco is a leading manufacturer of Hardware Security Modules (HSMs) that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector.

protegrity

The Only Data-First Security Solution. Protect sensitive enterprise data at rest, in motion, and in use with Protegrity's best-in-class data discovery, de-identification and governance capabilities.

PrimeFactors
— APPLIED DATA PROTECTION —

Prime Factors software products help business leaders implement and manage enterprise-wide data protection policies to secure sensitive information being used by or stored in virtually any application or system.

comforte

Secure your data, minimise risk, and meet compliance and regulation requirements. Find out more about comforte's Data Security Services.

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING
www.encryptionconsulting.com

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure

Hardware Security Module – HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

See it in action

Encryption Consulting LLC is a customer-focused cyber securtiy consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

linkedin.com/company/encryptionconsulting

facebook.com/encryptionconsulting

twitter.com/encryptioncons