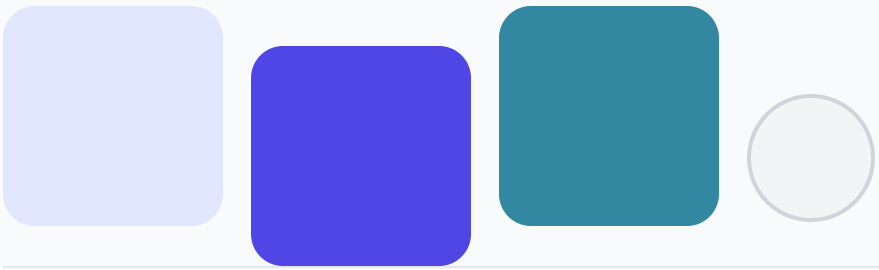
MAINFRAME SECURITY

Securing legacy mainframe data with DataStealth

Customer Profile: a financial services or telecommunications company operating IBM DB2 instances on a mainframe environment.



THE CHALLENGE

Unlocking mainframe data securely

Organizations in sectors like financial services and telecommunications often rely on mainframes to store vast quantities of historical customer data. While critical, this data frequently resides in cleartext, posing a significant security risk. The inherent complexity and age of mainframe code (e.g. COBOL) make modifications high-risk, expensive, and time-consuming — compounded by a scarcity of skilled mainframe developers.

Scarcity of COBOL developers

Cleartext at rest

Replication to external systems

Organizations typically avoid installing agents directly on mainframes: doing so can impact performance and is often unsupported. Sensitive data is often replicated to other systems, increasing the attack surface — especially when downstream systems incorporate external enrichment data that must be protected with the same rigour as the original.

TN3270 TERMINAL SESSIONS

Legacy protocols, modern risk

Accessing data on mainframes introduces unique security challenges due to legacy protocols like TN3270, still widely used for terminal-based sessions. These legacy access methods allow users to interact directly with sensitive data, often out of reach for modern security controls. Because TN3270 transmits data in real-time to user screens, protecting information at the point of display becomes essential.

This requires role-based enforced dynamic masking, and the ability to apply policies inline, all without disrupting the user experience — achieving unified visibility and control across both database replication and terminal access.

THE SOLUTION

DataStealth's agentless mainframe protection

The company implemented DataStealth's Data Discovery and Classification (DDC) and Data Tokenization (DT) to address these challenges without requiring intrusive code changes to its legacy mainframe environment.

Agentless Mainframe Interaction

DataStealth's approach is rooted in agentless mainframe interaction. The solution was deployed inline, enabling communication with the mainframe using native protocols such as TN3270 for terminal access and relevant database protocols for DB2 — eliminating the need for high-risk software installation or code alteration on the mainframe itself.

IN-PLACE TOKENIZATION

Protecting data at rest, without moving it

A key component was in-place tokenization, protecting sensitive data at rest and in use without changing its format or location. DataStealth endpoints read data from the mainframe DB2; vaulted tokenization replaced original values with tokens stored in the database, with no mathematical relationship to the original data — never exposed in clear text, format-preserving, and inherently quantum-resistant.

ORIGINAL

```
Card Holder: Mark Smith
Number: 4242 4242 4242 4242
Exp: 12/30/2027
```

TOKENIZED

```
Card Holder: John Doe
Number: 4012 8888 8888 1881
Exp: 12/15/2025
```

An alternative approach — keeping data in clear text and applying protection dynamically during access — was considered but not chosen, due to added complexity and the risk that protection might not always be applied.

FORMAT PRESERVATION

Passing business logic checks, uninterrupted

Format preservation is crucial for legacy systems like mainframe DB2, where altering schemas is risky or unsupported. Many mainframe databases run integrity checks, such as Luhn checks for credit card numbers, before committing updates. DataStealth's vaulted tokenization generates tokens that preserve the original data's structure and pass these rules, so downstream systems never break.

LUHN CHECK — FORMAT-PRESERVING TOKEN

Original: 4012 8888 8888 1881 sum = 90

Token: 4242 4242 4242 4242 sum = 80

✓ Both pass — multiple of 10

CONTROLLED REPLICATION

Secure data movement across systems

DataStealth endpoints intercepted replication flows from the mainframe DB2 to downstream systems — such as an Oracle database used for fraud detection — enforcing data protection policies in transit. Vaulted tokenization keeps mappings unique to each vault, enforcing strict data boundaries between environments.

Pass-through

Target shares the same vault — tokenized data passes through directly.

Controlled detokenization

Cleartext access under strict policy, audit logging, and time-limited windows.

Re-tokenization

Detokenized from the source vault, re-tokenized into the target vault.

TERMINAL ACCESS CONTROL

Dynamic masking, identity-aware

Dynamic Data Masking (DDM) provides real-time protection without disrupting existing applications. Through integration with IAM systems like Active Directory and Entra ID, DataStealth identifies users and enforces masking policies by role, attribute, and permission — supporting both ABAC and RBAC.

Vaultless tokenization

Deterministic algorithms, no vault to manage — but not quantum-resistant, and offers limited policy control.

Vaulted tokenization

Strong separation between environments, meets PCI requirements, policy-driven control over token resolution.

HOLISTIC VIEW OF DATA FLOWS

Mapping every source, consumer, and path

At the core of the solution was a complete understanding of how data moves across systems — mapping all data sources, consumers, and the pathways between them, so consistent policies for discovery, classification, and protection could be applied universally.

VAULT MANAGEMENT

Vaults securely manage the relationship between original data and tokens. Depending on configuration, the system used single or multiple vaults, allowing detokenization from one vault and re-tokenization into another. This approach is distinct from encryption: tokens contain no mathematical relationship to the original data, making it inherently resistant to threats like quantum computing.

OUTCOMES AND BENEFITS

Effective mainframe data protection

Complete protection, no risky rebuilds

Sensitive data was secured without modifying COBOL applications or existing infrastructure — significantly reducing cost, risk, and demand on scarce developers.

Reduced risk of exposure

Minimized exposure of cleartext data during replication, access, and transmission, significantly strengthening data security.

ENHANCED COMPLIANCE SUPPORT

By protecting sensitive data within legacy systems, DataStealth enabled the organization to meet stringent compliance requirements without changing existing infrastructure.

FACILITATED MODERNIZATION

DataStealth enabled secure data sharing between legacy mainframes and modern systems — a bridge for digital transformation efforts.

CONTROLLED DATA ACCESS

Sensitive data accessed through legacy terminal sessions was protected using dynamic masking and selective detokenization, governed by user roles, attributes, and session context — ensuring users only saw data they were authorized to access.

About DataStealth

DataStealth (datastealth.io) is a patented Data Security Platform (DSP) and PCI Level 1 Service Provider focused on helping enterprises discover, classify, and protect their sensitive data across any environment. Our DSP integrates data discovery, classification, and protection via vaulted tokenization and dynamic data masking in one platform solution.

Deployment requires no code changes, no agents, or a need to rearchitect legacy systems. DataStealth operates transparently at the network layer, enabling seamless protection across hybrid, cloud, SaaS, and even mainframe environments.

Learn more at datastealth.io