SecuPi

Success Story

SecuPi Security & Privacy For Azure

GDPR Compliance and Data Loss Prevention for Business Applications and Analytics on Azure

The Problem

A British multinational energy and services company has been seeking a technology that would enable it to comply with the strict GDPR regulations, mainly addressing consent and "Right of erasure" requirements, as well as user auditing capabilities for monitoring user activity.

The Solution

After examining multiple solutions on the market, the customer has selected SecuPi platform for addressing GDPR "Right of erasure", Consent (opt-in/opt-out), column-level encryption at-rest/in-use, masking and real-time user activity monitoring.

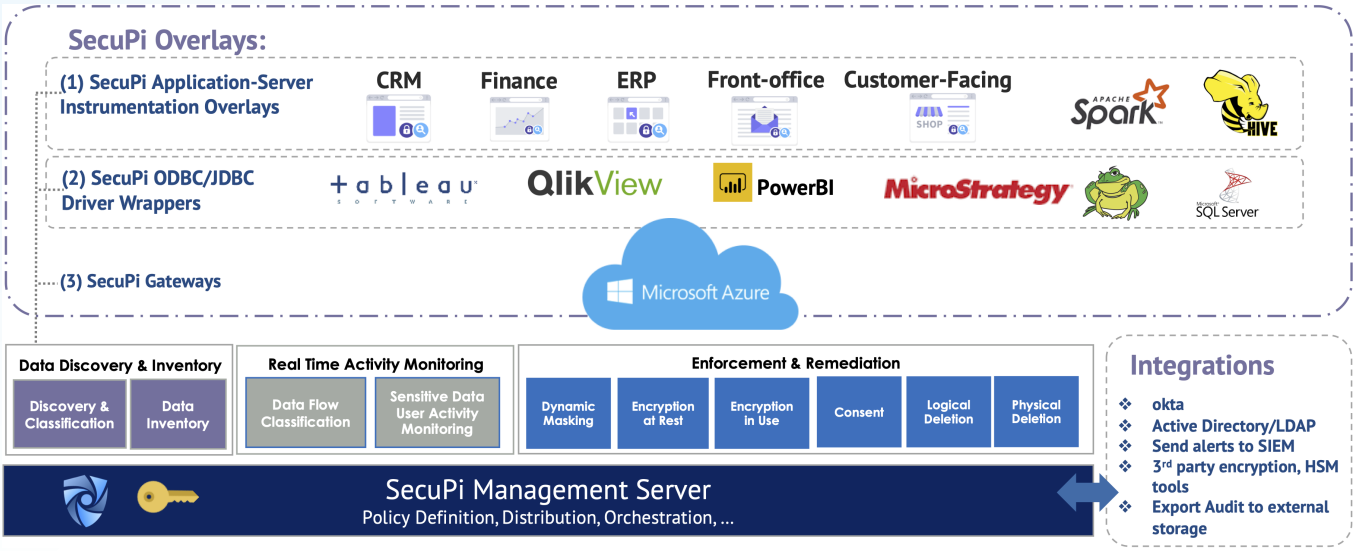
SecuPi was deployed in days on Azure where its application overlays (agents) were configured on dozens of packaged and home-grown customer management applications, as well as on DBA tools.

Customer-data anonymization, filtering and real-time monitoring policies defined in SecuPi Central Management server were polled and immediately applied by the application overlays - ensuring that all customers who have "Opted out", revoked consent or erased will not be exposed via all application screens, reporting, DBA activity and processes.

SecuPi Overlays were configured within days across packaged and custom applications as well as all DBA direct database access tool.

Benefits

- **Applying "Right of Erasure", Consent & Data Loss Prevention across hundreds of business & analytics applications**
- **A single centralized solution for protection and privacy compliance. Protect data in transit, in-use and at-rest.**
- **Applied within weeks without code-changes or database configurations**



Organizations today struggle to satisfy the ever-growing compliance requirements (e.g., CCPA, GDPR, Geo-Fencing) while preventing data leakage through privileged abuse and credential theft. Both challenges are addressed by SecuPi:

Discovery & Monitoring

Sensitive data discovery and classification.

All access to sensitive data is audited and monitored in real-time, labeled according to the sensitivity of the data exposed and assigned a risk score.

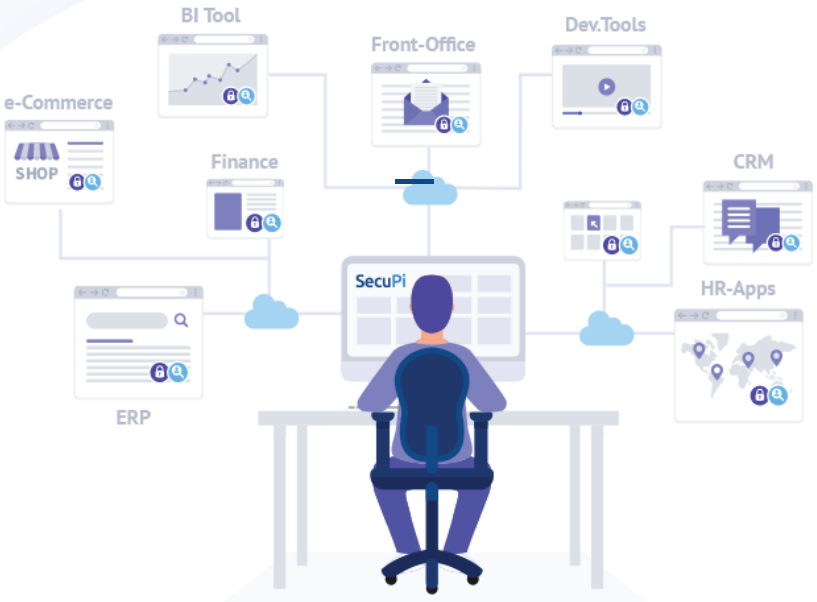
As authorization granted to end-users and administrators can be abused by careless or malicious insiders and stolen by hackers, SecuPi User Behavior Analytics module with self and peer comparison detects and alerts or blocks before damage occurs.

Anonymization & Remediation

Encryption at-rest while keeping keys on-prem.

Encryption in-use/dynamic masking sensitive data for restricting access on a "need-to-know" while applying to data-cross border controls.

Preventing "singling out" VIP clients or restricting abnormal extraction of sensitive data.



SUPPORT FOR ALL APPLICATIONS & NATIVE TOOLS

Column-level encryption at-rest & in-use with key Segregation for cloud compliance

Masking and Row-level Security

Real-time Monitoring, Forensics & Behavior Analytics

About SecuPi

SecuPi delivers data-centric security and compliance with data-flow discovery, real-time monitoring, behavior analytics, and protection across web and enterprise applications (on-prem and on-cloud) and big data environments. Organizations deploy SecuPi to ensure data is accessed on a need-to-know basis, providing an industry-leading privacy compliance technology, while protecting from careless and malicious abuse. Our policy engine centrally delivers row and field-level access controls, risk-based user activity auditing and monitoring across platforms. SecuPi was named a Cool Vendor by Gartner.

SecuPi

For more information visit us at: **www.secupi.com**

For sales inquiries contact: **sales@secupi.com**