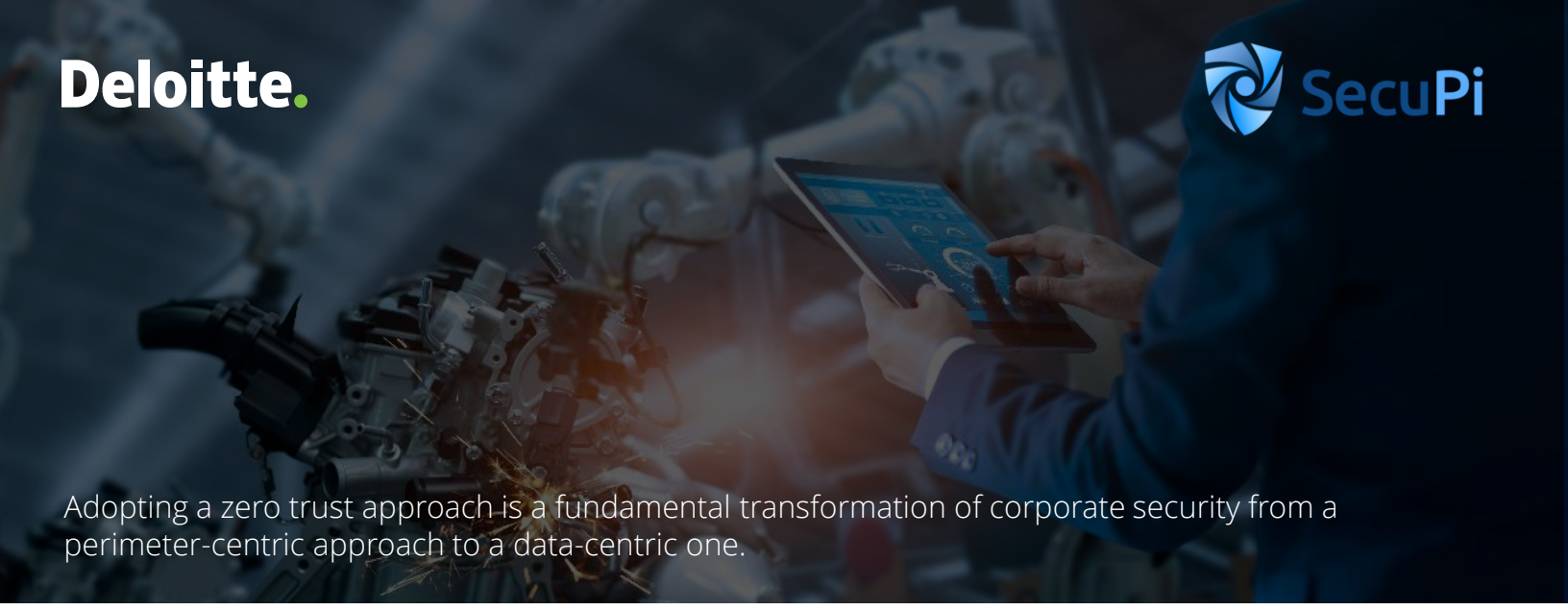


Adopting a zero trust approach is a fundamental transformation of corporate security from a perimeter-centric approach to a data-centric one.

Risks are increasing due to proliferation of data and complexity of use

Today's organizations store sensitive, personal and business-critical data in an increasing number and variety of platforms across a global enterprise. With data security breaches on the rise, and the need to comply with security and data privacy legislations (e.g.: GDPR, CCPA, HIPAA, PCI...), organizations must develop a data-centric risk based mitigation strategy.

The foundation of this strategy must also include the principle "Trust No One", even authenticated users can represent a risk to the organization's most valuable asset: data.

How SecuPi can help?

A data-centric privacy and protection solution providing a centralized view of risk exposure, capable to apply access control and protection mechanisms as required by governance policies and data privacy regulations.

SecuPi addresses security & compliance requirements by placing an agent on your application server layer, with no other changes: no source-code, database or network configurations changes required.

Data Discovery and Classification

Identification and classification of personal, sensitive data and data flows across business applications.

Dynamic Controls

Logical data minimization ensuring that all access to data is performed on a "*need-to-know*" basis (e.g.: logical erasure, dynamic masking, random anonymization, blocking, alert, encrypt, etc.)

User Activity Monitoring

Monitor data access activity with enhanced user context between the application and database layers based on classification and risk scoring

User Behavior Analytics (UBA)

Collect analytics of user access to sensitive data over time to monitor user behavior, alert and automatically act in defined cases.

Integration

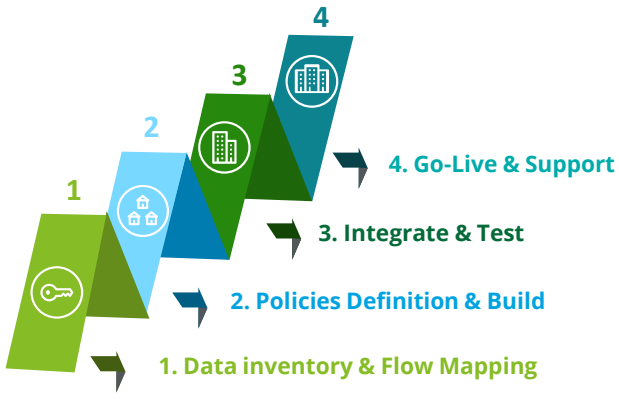
Integrates with SIEM and EDR solutions enriching the logs context in the use case definition but also with IAM solutions and Active Directory/LDAP for applying Purpose-Based-Access control.

Recommended approach

Deloitte's approach for the project includes a service methodology considering an application sprints process.

This approach can be summarized in the following steps:

1. **Data inventory & Flow Mapping:** Discover, classify & map sensitive data across *on-prem* applications and cross cloud data services.
2. **Policies Definition & Build**: Define behavioral use-cases, data access monitoring, audit & control rules.
3. **Integrate & Test**: Integrate with user permissions source and event management system.
4. **Go-Live & Support:** Real-time regulated data-flow monitoring & control with behavior analytics on high-risk processes and regulated data accesses.



Architecture

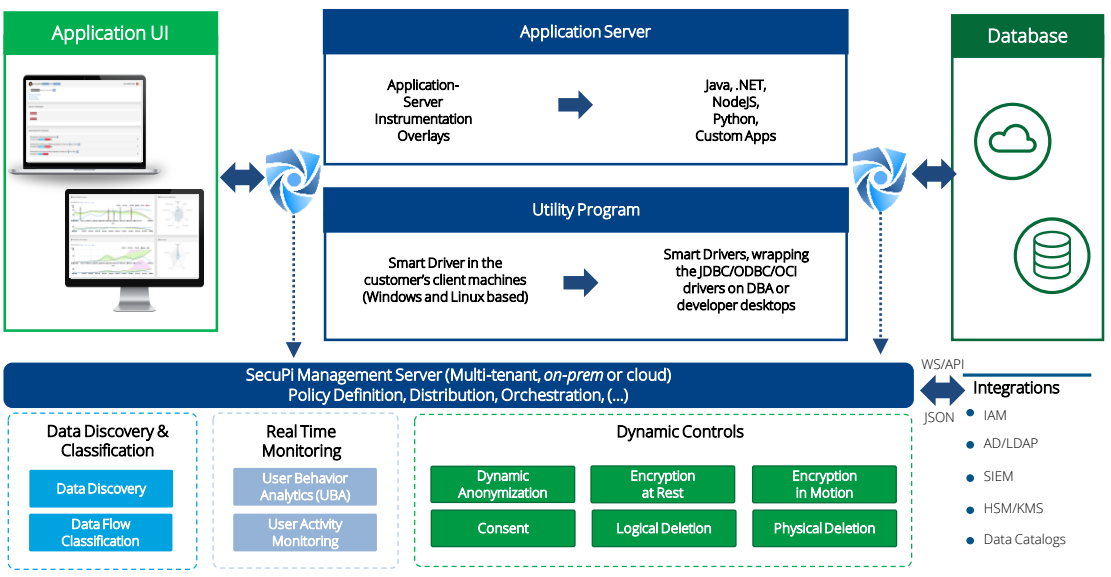
The diagram presented on the right summarizes the integration between the solution components and the target business applications and analytics environments.

Major Benefits

Provide a single platform for protecting sensitive data, whether applied for compliance or security purposes (or both).

Deliver a compliance-enforcement platform with granular visibility and Data Access Governance capabilities for being aligned with today's privacy regulations and comply with future ones.

Protect enterprise applications, data warehouses, and DBA client tools from attacks performed both from inside and outside of the security perimeter.



Contacts

Frederico Mendes Macias
Partner
+351 966850347
fremacias@deloitte.pt

André Riscado Pedra
Manager
+351 919605620
apedra@deloitte.pt