Case study

Policy-based protection of data on premise and in the cloud secured by Intel SGX

Market need

Today’s enterprises house sensitive and regulated data in servers, databases and laptops on premise and in the cloud. Organizations are required to establish strong and comprehensive defense for the assets they contain in their applications to satisfy compliance requirements. This usually requires technical skills and significant effort in code changes and key management which results in a great cost impact for enterprises.

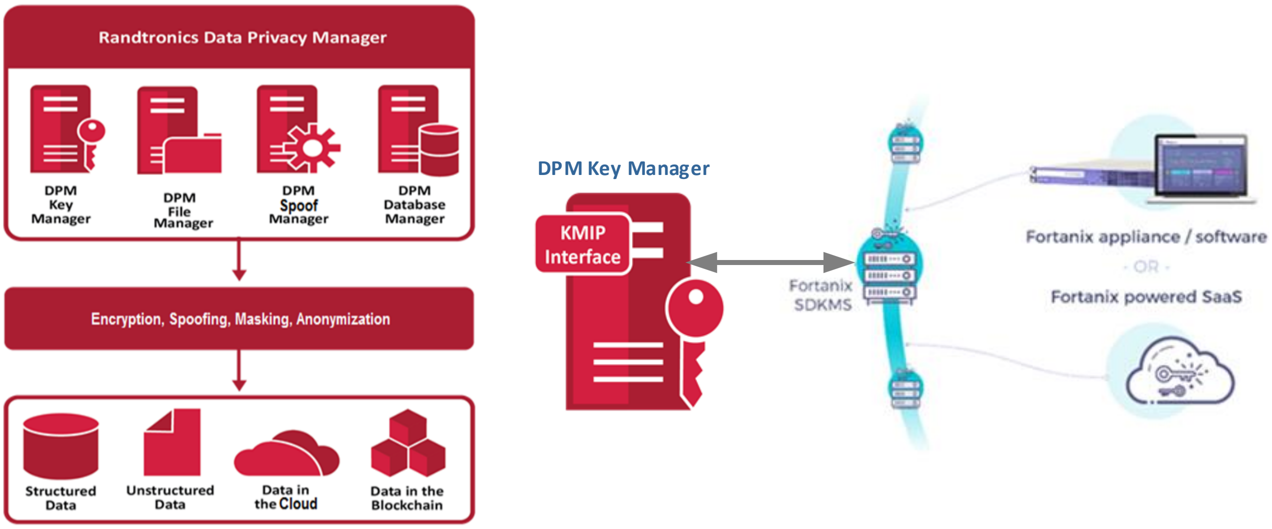
Data privacy management that covers the entire enterprise allows organization to minimize the risk of compromised data whether it is structured or unstructured. Encryption is required as “the last line of defense” to avoid compliance fines. However, the underlying cryptographic keys have to be securely stored, managed and protected on premise or in the cloud to ensure the high assurance of the entire cryptosystem.

Solution overview

The combined Randtronics + Fortanix solution offers comprehensive data protection for laptops, desktops, servers and databases, both physical and virtual, secured by an encryption key with Intel SGX. Transparent integration with no code changes facilitates quick deployment of data privacy on premise, in the cloud or in hybrid environments.

Randtronics Data Privacy Manager (DPM) plug and play connectors and APIs for files, folders, databases, web and application servers provide easy deployment, use and maintenance. Features such as policy-based key management, encryption, tokenization, pseudoanonymization, anonymization, masking, access control and auditing facilitate compliance with internal security policies as well as government and industry regulations.

Integration with the Fortanix Self-Defending Key Management Service (SDKMS) provides HSM grade security with software-defined simplicity. Fortanix SDKMS is the world's first cloud solution secured with Intel® SGX. SDKMS can be deployed globally and for hybrid or multi-cloud environments.



Fortanix and Randtronics DPM solution benefits

- Comprehensive enterprise data protection using encryption, masking, tokenization, pseudoanonymization and anonymization engines
- Transparent protection with no code changes for files, folders, databases and applications
- Centralized policy based control of cryptographic services and access control
- Secure auditing for compliance
- Key Management and Protection of master keys with Intel SGX technology

About Randtronics

DPM offers an innovative and easy to use approach to data protection. DPM features policy based protection using encryption, spoofing, masking, pseudoanonymization and anonymization to transparently protect data with no code or business process changes.

DPM is a software-based solution that runs on Windows or Linux in the cloud, on premise or hybrid. Access control, auditing, privileged user control, separation of duties, support for all data types and a policy based integrated certificate and key management are the key features of the DPM platform.

For more information, visit www.randtronics.com

Fortanix Self-Defending Key Management Service (SDKMS)

Secured with Intel® SGX, Fortanix SDKMS delivers HSM-grade security with software-defined simplicity. SDKMS provides flexible consumption options - a hardened appliance, HSM as a service, or software running on commodity x86 servers.

SDKMS offers central management, tamper-proof logging, rich access control, REST APIs and massive scalability. Organizations use SDKMS to secure their sensitive cloud and traditional applications, including digital payments, PKI systems, IOT applications, silicon manufacturing, and remote TLS terminations - all while drastically reducing integration complexities and expenses.

For more information, visit https://fortanix.com/