eperi

Cloud Data Protection

Secure your most valuable asset - Your Data

**Nur mit Verschlüsselung gibt es Sicherheit in der Cloud:
Der einzige Weg, um rechtliche Anforderungen zu erfüllen.**

Agenda

1 - Executive Summary

2 – Question & Answers

3 – Data Encryption

4 – The eperi Gateway

eperi

- **eperi is your company's protective shield.**

- **eperi protects your business critical information with state of the art encryption and tokenization.**

- **In the case of a data breach any sensitive & critical data leaving the organization, is rendered useless.**

- **Maximize the benefits of cloud services whilst staying complaint without having to worry about data security.**

Agenda

What are the main differences between security on-premise and security in the public cloud?

https://aka.ms/sharedresponsibility

Page 5:
- Ensuring that the data and its classification is done correctly and
- that the solution will be compliant with regulatory obligations

is the **responsibility of the customer**.
Physical security is the one responsibility that is wholly owned by cloud service providers when using cloud computing.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Cloud Customer ■ Cloud Provider ■

Is there a need for other data protection solutions, when all hyperscalers—Microsoft Azure, Amazon Web Services, and Google Cloud Platform—have gone the extra mile to make their platforms secure?

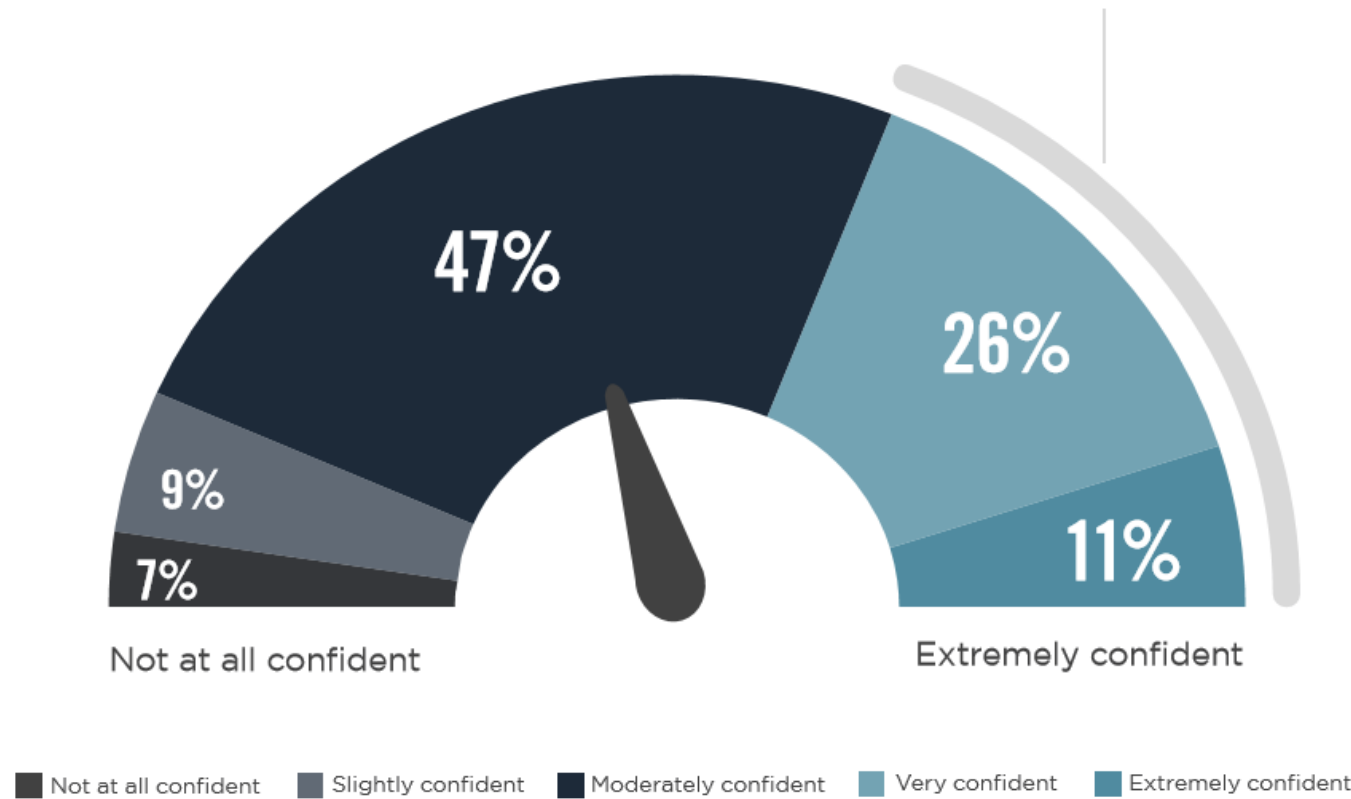**Rashi Mittal**

Director of Product Management

This is a great question, and the answer is simple! All hyperscalers do a great job of securing their own platforms. But contrary to what you may think, **protecting your most valuable assets (your data, customer information, and intellectual property) in the cloud is still your responsibility** , not theirs. The public cloud providers endorse this idea under the well-known "shared responsibility model" discussed below.

How confident are you in your organisation's cloud security posture?

Only about 1/3 are very confident or extremely confident in their organization's cloud security posture. **37%**

47%

26%

9%

11%

7%

Not at all confident

Extremely confident

■ Not at all confident ■ Slightly confident ■ Moderately confident ■ Very confident ■ Extremely confident

Source: Cybersecurity Insiders : 2019 Cloud Security Report.

eperi

What are the challenges when moving to the cloud ?

64% Data loss / leakage

62% Data privacy / Confidentiality

| 35% | **Legal & regulatory compliance** |

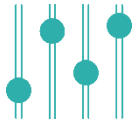| 29% | **Data sovereignty / residency / control** |

| 39% | **Incident response** |

63% are not confident with their organization's cloud security policy.

Source: Cybersecurity Insiders : 2019 Cloud Security Report.

eperi

Major issues when moving to the cloud

Personnel Responsibility

The C-Level has the legal responsibility to protect customer data using advanced technology to prevent data breaches.

Data Residency

When implementing a global CRM solution for e.g. in China we are not allowed to share restricted data with the rest of the world.

Legal Regulations & Liability

In our vertical we are forced by the regulator to protect our customers data with state of the art technology

GDPR

We would like to use PII Pseudonymization to descope the cloud from GDPR

eperi

What companies do so far

Hope that nothing will happen.

- Hope that breaches do not happen in my Industry / Sector / Department / Country etc.
- Data breaches and cyber attacks have become more expensive.

Not move to the cloud.

- Resulting in high maintenance cost with on prem-solution and systems.
- Reduced functionalities , features and support as more & more application & service become cloud based.

Use traditional on premise security solution for the new cloud security problems

- Only securing IT-Systems is no longer sufficient, data too needs to be safeguarded.
- Firewalls are not sufficient to contain data.

Cloud Service Provider security mechanisms are not helping or are not sufficient.

- CSPs security solution only works with their respective service. While organizations are looking for an overall solution which covers their entire cloud services portfolio.
- By owning the encryption process, the company prevents the cloud providers access to its unencrypted data.

eperi

Do breaches happen in reality?

Microsoft O365 Hack:
- https://www.theverge.com/2019/4/13/18309192/microsoft-outlook-email-account-hack-breach-security
- https://blog.eperi.com/en/attack-on-microsoft-web-mail-services

Mastercard:
- https://m.manager-magazin.de/unternehmen/banken/mastercard-das-datenleck-ist-offenbar-groesser-als-gedacht-a-1282997.html
- British Airways:
- https://www.cnn.com/2019/07/08/tech/british-airways-gdpr-fine/index.html
- https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
- Capital One:
- https://www.securityweek.com/capitalone-discloses-massive-data-breach-106-million-impacted
- Mariott Hotels:
- https://www.securityweek.com/marriott-faces-123-million-fine-uk-data-breach
- American Medical Collection Agency (AMCA):
- https://www.komando.com/happening-now/570553/data-breach-exposes-millions-of-medical-records

Huge fine for data breaches

$5 Billion

$100 m

$575 m

$57 m

$124 m

$230 m

eperi

Agenda

1 - Executive Summary

2 – Question & Answers

3 – Data Encryption

4 – The eperi Gateway

eperi

The eperi Gateway secures your data

Stolen data is not readable in the cloud. The eperi Gateway encrypts data before it is stored in the cloud. ("Data in use" – Protection)

eperi technology eliminates negative issues regarding Data Breach, Data Residency and Regulatory Compliance by:

- Anonymizing / pseudonymizing critical data in the cloud
- Applying toughest data security standards
- Preserving required cloud functionality

Transform your weakness into your strengths

Use worry & liability free cloud applications

CISO / Data Privacy Officer / Workers Council

From Cloud Blocker to Cloud Enabler

Management

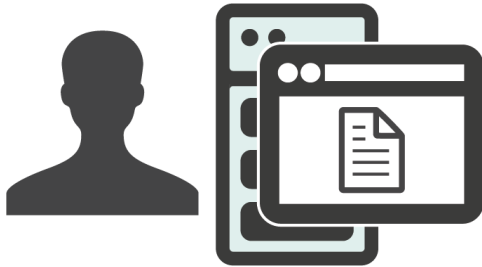Reduce personal responsibility

Line of Business

Freedom to use best of breed IT solutions

eperi

GDPR
The Challenge

Data Controller

Data Processor

Internal and External Users

Sensitive PII Data

Sensitive PII Data

Web Browser

salesforce
servicenow
Office 365
successfactors — An SAP Company
Microsoft Dynamics 365
CUSTOM APPS
amazon web services | S3 — File Shares
Azure

PII and sensitive PII data in scope for GDPR

PII and sensitive PII data in scope for GDPR

eperi
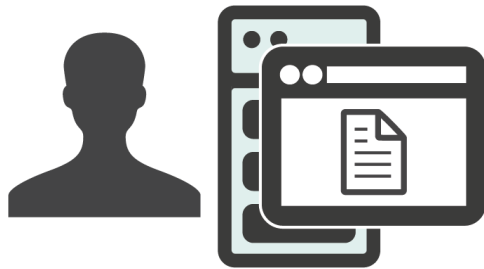
GDPR
Tackling the Challenge with eperi

Data Controller

Data Processor

Internal and External Users

Data Protection Policy

Sensitive PII Data

eperi

Pseudonymized Data

Web Browser

salesforce
servicenow
Office 365
successfactors
An SAP Company
Microsoft Dynamics 365
CUSTOM APPS
amazon web services | S3
File Shares
Azure

PII and sensitive PII data in scope for GDPR

Pseudonymized data out of GDPR scope

eperi

No one can prevent data being stolen,
but the eperi Gateway can prevent the use of
stolen data.

Agenda

1 - Executive Summary

2 – Question & Answers

3 – Data Encryption

4 – The eperi Gateway

eperi

Achievements
Customers, Partners & Awards

Traction	Customers	Partners	Awards

Traction

- 60 enterprise customers
- 50 employees
- Mio $ Dealsize
- Market Influencer
- Multiple Patents
- Avg. Deal Size: $250 K

Customers

Deloitte. · verimi · Deutsche Telekom · JAMESTOWN · ITAS GmbH · Henkel · PORSCHE · Roche · Klinikum Fürth · Deutsche Asset & Wealth Management · Basell · CURRENTA Leistung für Chemie und Industrie · SIEMENS Healthcare · European Union EXTERNAL ACTION · EVONIK KRAFT FÜR NEUES

Partners

IBM · Microsoft · Deutsche Telekom · COMPAREX Software · Consulting · Services · netskope · NTT · ooredoo · SEPPMAIL · SKY EXPRESS · Telefónica · REPLY STORM · MariaDB · CGI

Awards

IBM Beacon Awards Winner · Microsoft · 2017 Computing Security Awards FINALIST · finalist Cyber Security Awards · TechXLR8 AWARDS WINNER 2017 · itsecurity · AWARD 2017 · INNOVATIONSPREIS-IT BEST OF 2017 initiative mittelstand IT-SECURITY
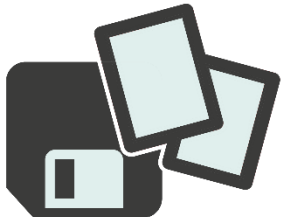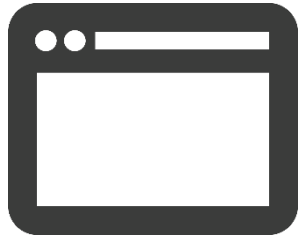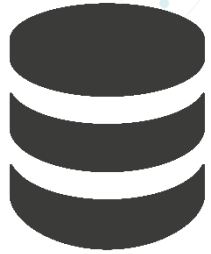
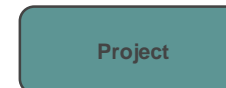# The eperi Gateway - Patented template architecture works with cloud services across the board.

Your benefits as a partners
using the eperi SDK Adapters

Benefits for partners

- ✓ Partners need **integrated security solutions** to offers SaaS-solutions with integrated consulting services

- ✓ Partners are the **experts of the cloud application** and its technical & functional capabilities, eperi is the expert of the cloud data security solutions

- ✓ With a joined cooperation, eperi and its partners can **scale quick enough to fulfill the market** demand for new adapters

- ✓ Partners can offer the **outsource support** for application-specific Adapters to Partners

- ✓ Make use of patented templating approach, which was **proven by eperi themselves** by developing Adapters for Salesforce and Office365
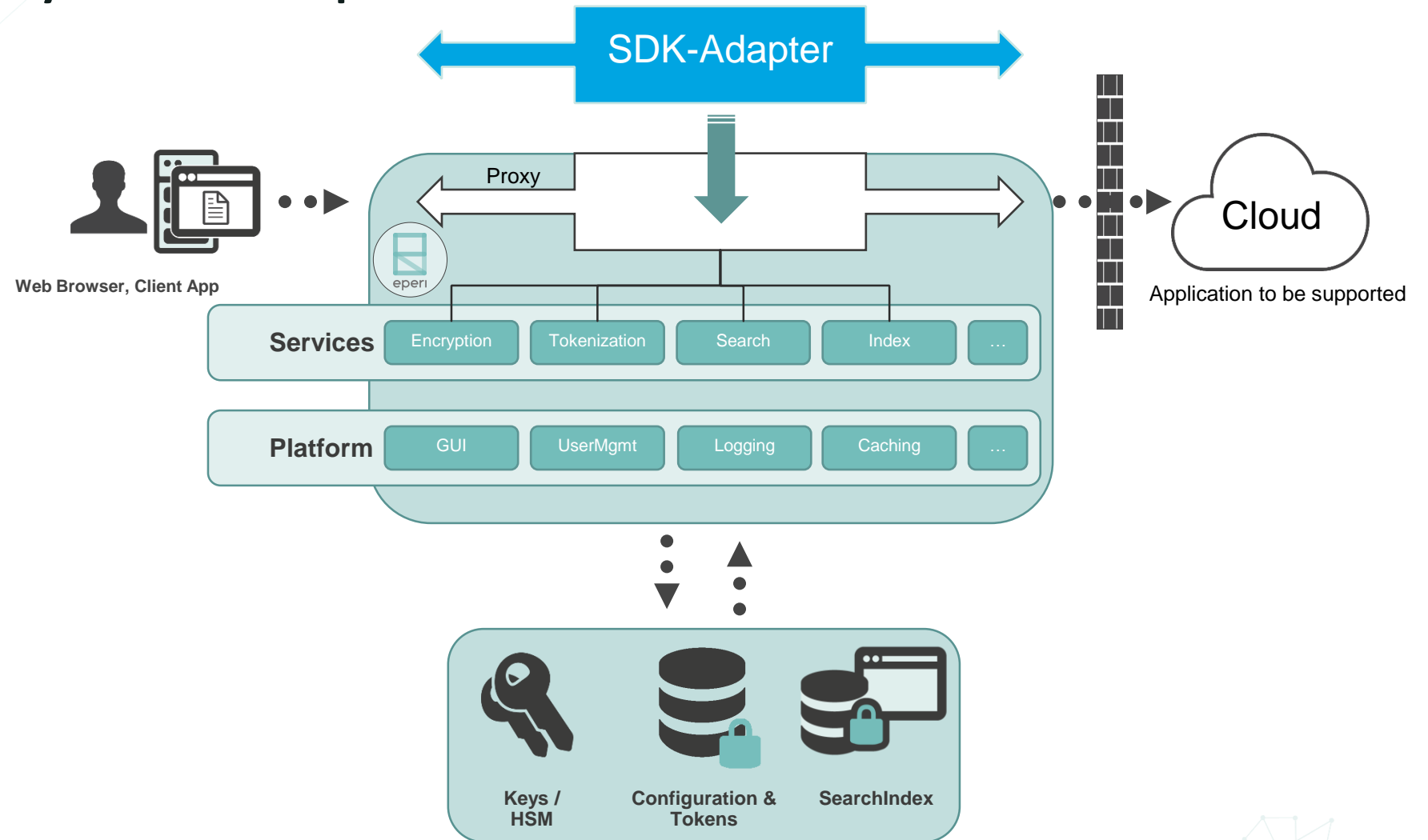
Benefits for your customers

- ✓ Customers use various cloud technologies and need data protection **solutions without breaking important cloud functionalities** to be flexible and agile

- ✓ **Financial and reputative damages** due to cloud data breaches from third parties (hackers, states, secret services etc.) increased within the last years

- ✓ Organisations need to **regain control of their data** and thus operate securely in a flexible cloud environment

- ✓ eperi SDK allows a **short time to implement** with an easy-to-adapt solution and therefore a **quick time to value**

- ✓ Customers receive **an "all-in-one-hand" solution**, when Partners offer them the full cloud package (implementation, consulting, security & support)

The eperi SDK…

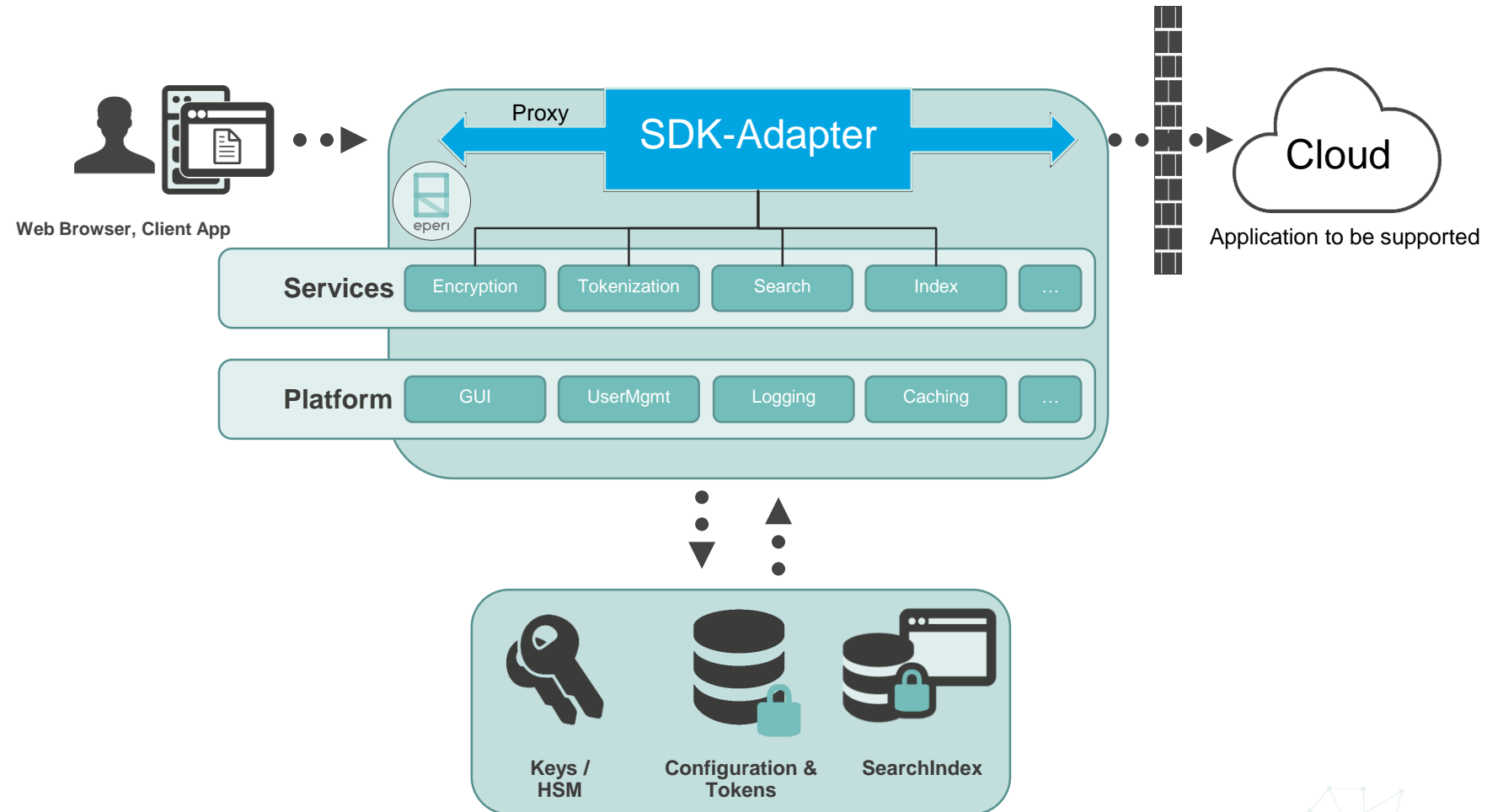## … enables you to build your own Adapter

- You can develop an encryption adapter for the desired application

- eperi SDK utilizes hardened gateway services

- eperi provides training material and onboarding

- Services are available via nexus maven

- eperi provides the gateway as runtime environment

SDK-Adapter

Web Browser, Client App

Proxy

Cloud

Application to be supported

Services

| Encryption | Tokenization | Search | Index | … |

Platform

| GUI | UserMgmt | Logging | Caching | … |

Keys / HSM

Configuration & Tokens
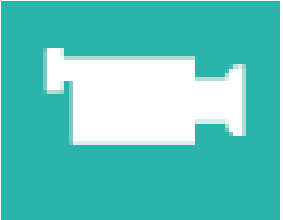
SearchIndex

eperi

The eperi SDK...

... enables you to build your own Adapter

- You can develop an encryption adapter for the desired application

- eperi SDK utilizes hardened gateway services

- eperi provides training material and onboarding

- Services are available via nexus maven

- eperi provides the gateway as runtime environment

Web Browser, Client App

Proxy

SDK-Adapter

Cloud

Application to be supported

Services | Encryption | Tokenization | Search | Index | ...

Platform | GUI | UserMgmt | Logging | Caching | ...

Keys / HSM

Configuration & Tokens

SearchIndex

eperi

Supporting Material
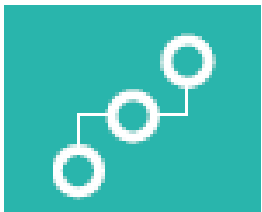## Learn to Write your own Adapter in days

Video Tutorials

- Exemplary Functionality Demonstration of Adapters
- Reverse Engineering
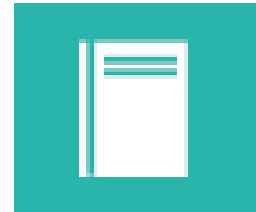- Encryption vs. Tokenization
- Deploying your own Adapter

Onsite Training

- eperi training & consulting services
- Development Support
- Enable your Java developers for Adapter creation

Templates

- Template of an Adapter
- Illustrates Best Practices
- Works with the Test Application provided by eperi

Documentation

- How to Build & Deploy
- How to Consume Services
- How to use the Index & Search

eperi

Thank You!

eperi.com
info@eperi.com

@eperi