SECURING SAAS
SECURE CLOUD TRANSITION FOR SOFTWARE AS A SERVICE

T-Systems
CLOUD MATTERS!

60% of enterprise workloads will be processed in the cloud end of 2019

Source: 451 Research
CHALLENGES THAT COME WITH CLOUD SERVICES

Proliferation of Cloud Apps
Variety of Endpoints

1. Shadow Data Problem
2. Compromised Accounts

Data Loss/ Leakage

DSGVO / GDPR

25% of cloud docs are broadly shared¹

¹ 1H 2016 Shadow Data Report

Risk Assessment
Intrusion Detection
Malware Detection
Proxy/Firewall
DLP
Incident Response
Investigations
Do you use SaaS / Cloud Services?

Cloud First Strategy
- Monitor cloud usage
- Ensure compliance & data protection
- Provide alternatives to Shadow-IT services

Cloud transition
- Assist transformation to the cloud
- Secure and control new SaaS applications
- Lessons learned from cloud usage

No cloud usage
- Permanent Shadow-IT monitoring
- Definition of blocking strategies
- Building own solution for demanded SaaS apps
STRUCTURED WAY FOR A SECURE CLOUD TRANSITION

Level of maturity on Shadow-IT Governance

- Define your cloud governance & strategy
- Create awareness and communicate
- Shadow-IT discovery & analysis
- Enforce and monitor compliance and security policies
- Replace Shadow-IT through secured alternative apps

Implementation effort

Facts

- 60% of companies use Cloud Computing
- Only 50% of companies have a cloud strategy
- 44% of employees use SaaS applications at work
- But only 10% of companies knows their Shadow-IT

TSystems
Organizations use 20 times more cloud apps than they think.

An enterprise has 928 cloud Apps in USE (average).
HOW TO ADDRESS SHADOW IT?

**Whitelisting**

- Most secure solution
- However massive effort to operate white lists
- Restrictions might have negative impact on employees performance

T-Systems
HOW TO ADDRESS SHADOW IT?

Category blocking by proxy

Lower effort than white listing

Vague solution as only one criteria is taken into account

However access to a service, administration, business rating, compliance certifications (e.g. GDPR), encryption, data handling & sharing and legal topics are NOT considered

Proxy

Enterprise Perimeter

Gambling  x  News  ✓
File sharing  ✓  Porn  x
Social media  ✓  ...
HOW TO ADDRESS SHADOW IT?

Cloud Access Security Broker
Shadow IT
Discovery & Controls

- Gain visibility and control shadow-IT
- Assess up- & download volume per cloud service
- >25k Cloud Services
- Enforce compliance rules and regulations
- >100 evaluation criteria
- Automatic blocking of very risky cloud services

Proxy
Enterprise Perimeter
Sec Events
HOW TO ADDRESS SHADOW IT AND EXTEND PROTECTION TO SAAS
Determine the apps that are best for your business

- View Business Readiness Rating based on 110+ metrics across 7 categories
- Customize prioritization of metrics to tailor analysis to your organization
- Perform side-by-side comparative analysis of alternative apps
Detect which cloud services are in use and see their specific risks.

Making sure companies compliance regulations are met.

Benefiting from economies of scale when merging to fewer SaaS.
SHADOW-IT SNAPSHOT CUSTOMER XYZ BANK (ONE WEEK ONLY)
SHADOW-IT SNAPSHOT CUSTOMER XYZ BANK (ONE WEEK ONLY)

- Data from/to 419 locations around the world
- 1292 SaaS services seen in a week period
- 27 file storage applications
- 25 file sharing applications
- 47 collaboration applications
- 22 Email applications
- 21 document management applications
- 3.7 TB of Data used in 1 week in SaaS alone
- 229.3 G Upload = 12 TB/Year
3 AREAS OF CLOUD PROTECT PRO USE-CASES

1. Shadow IT

2. Security and Compliance for Software as a Service

3. Security for Infrastructure as a Service
WHY USE CLOUD PROTECT PRO TO CONTROL YOUR SAAS APPLICATIONS IN ADDITION TO INHERENT TOOLS

- Keeping control: Benefiting from cloud services without sacrificing security
- Most SaaS Applications don’t have dedicated security solutions
- One unified platform for all SaaS applications in use with an overarching view
- Extend policy and compliance rules from a central point to various cloud services
- Use existing Data Loss Prevention solutions and apply that to 3rd party services
**CONTROL AND PROTECT THE DATA IN SAAS APPLICATIONS**

- **Control and encrypt sensitive data in the cloud**
- **Threat detection by behavioral based analysis and malware protection**

<table>
<thead>
<tr>
<th>Data Security</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Prevention of data loss using Cloud Protect Pro by classifying sensitive data, monitoring of vulnerable data and encryption of sensitive content.</td>
<td>- Cloud Protect Pro protects cloud user accounts by analyzing patterns of use. It’s looking for critical patterns of use and comes with integrated malware detection.</td>
</tr>
<tr>
<td>- Avoid sharing (un-/ intentionally) of sensitive, confidential or personal data</td>
<td>- Blocking, quarantining and alarming for malicious data and suspicious behavior</td>
</tr>
<tr>
<td></td>
<td>- Integration into SIEM systems</td>
</tr>
</tbody>
</table>
"Sharing of personal data has to be prevented."

"Detection and tracking of trusted content into the cloud."

"No uploading of sensitive data into the cloud."
“Identificatio
n of high risk
users.”

“Quarantine
hacked user
data.”

“Alerting IT
security in case
of suspicious
patterns of use.”
TAILORED TO YOUR NEEDS

Working together with market leaders

Comprehensive consulting services

Fully managed service

Competitive pricing

Planned: SOC/SIEM service
THANK YOU!

Paul Schöber
Head of Portfoliocluster Cloud, Data & Application Security
T-Systems International GmbH, Telekom Security
paul.schoeber@telekom.de