



.conf2015

# How Splunk Connects Business and IT at Swiss Bank PostFinance Ltd

Patrick Hofmann  
Head of IT Infrastructure, PostFinance



splunk®

# Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.



# .conf2015

## About Me – In a Nutshell



splunk®

# About Me – In a Nutshell



# Agenda

- PostFinance Ltd at a glance
- Splunk@PostFinance
- Use case 1 – Fraud detection and report generation for E-Payment
- Use case 2 – Online banking security and threat detection
- Wrap up



.conf2015

# PostFinance At a glance

splunk®

# PostFinance at a Glance

One of the leading **retail financial institutes** of Switzerland

Number one in Swiss **payment transactions**

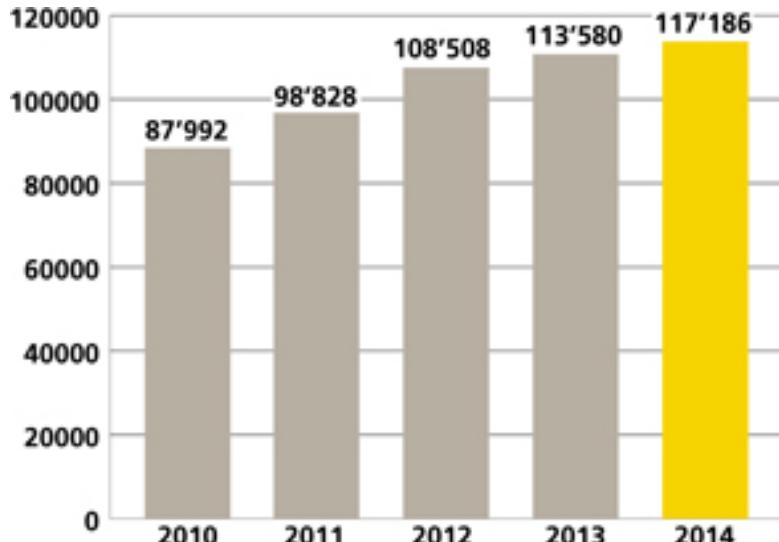
An ideal partner for customers who wish to **independently manage their finances**



# Assets and Transactions

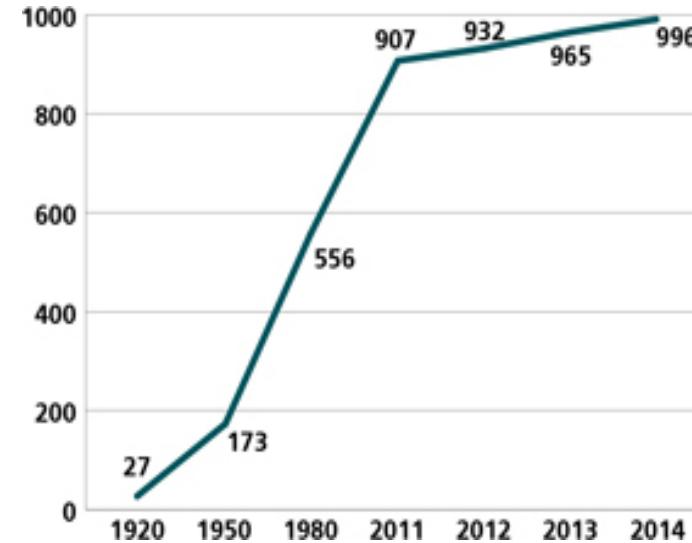
## Customer funds (in CHF millions)

More and more customers entrust PostFinance with their money.



## Transactions processed (in millions)

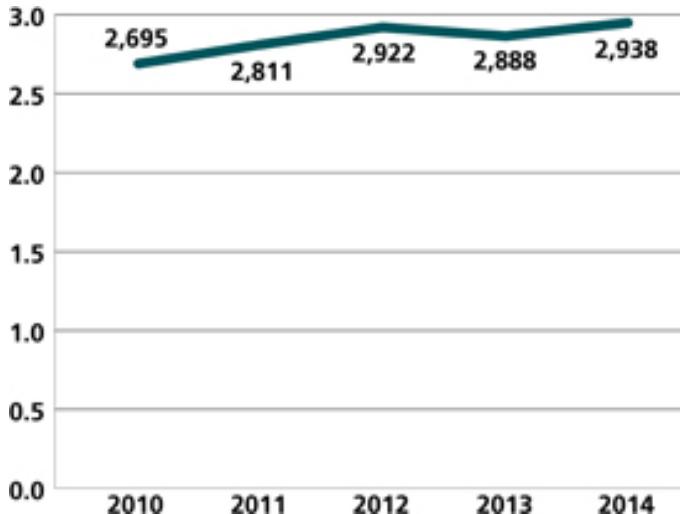
PostFinance is the market leader in Swiss payment transactions.



# Customers Total and Online

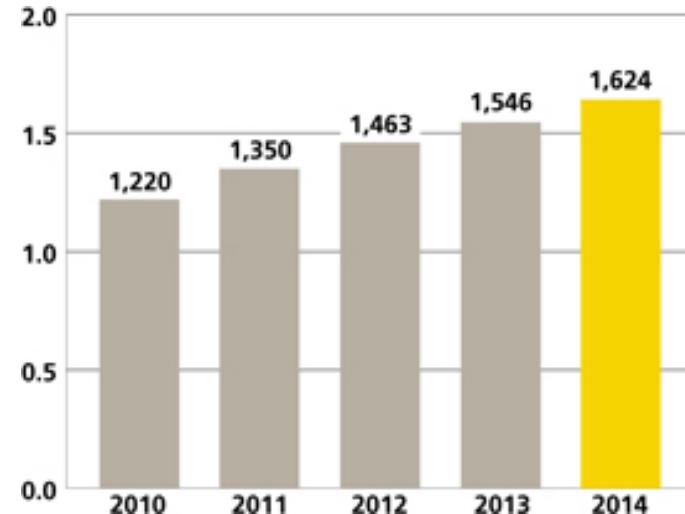
## Number of customers (in millions)

PostFinance is one of Switzerland's leading retail financial institutions.



## E-Finance users (in millions)

More than 1.6 million customers manage their finances online.



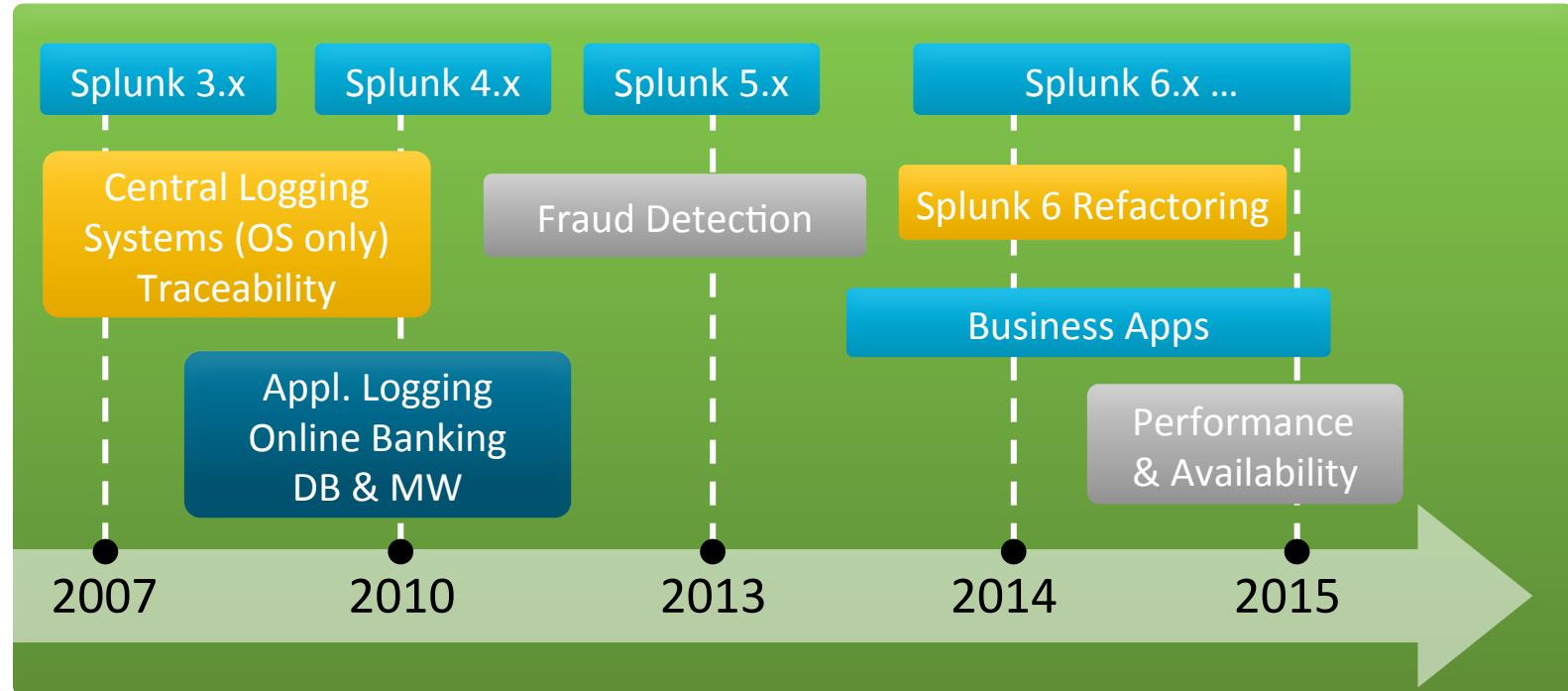


.conf2015

# Splunk @ PostFinance

splunk®

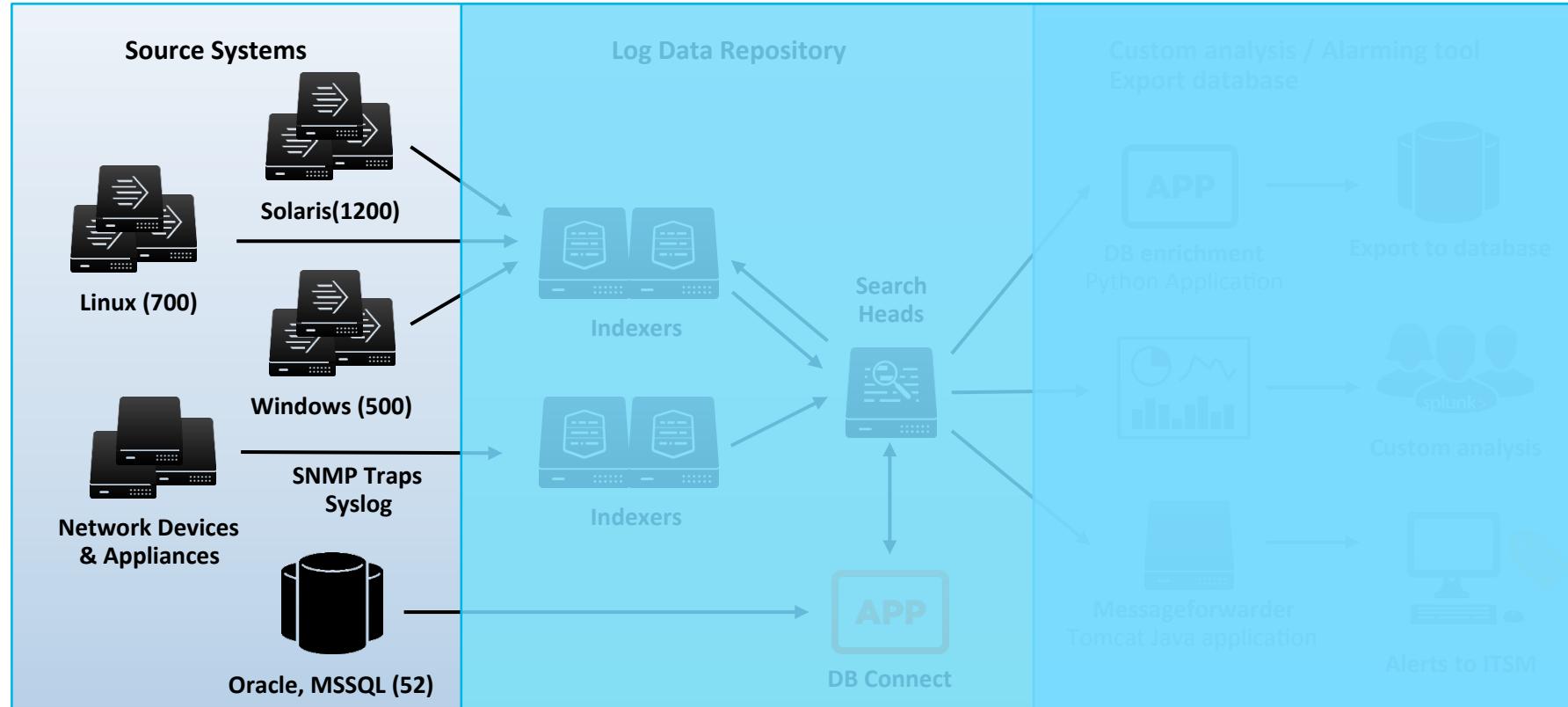
# PostFinance's Splunk Timeline



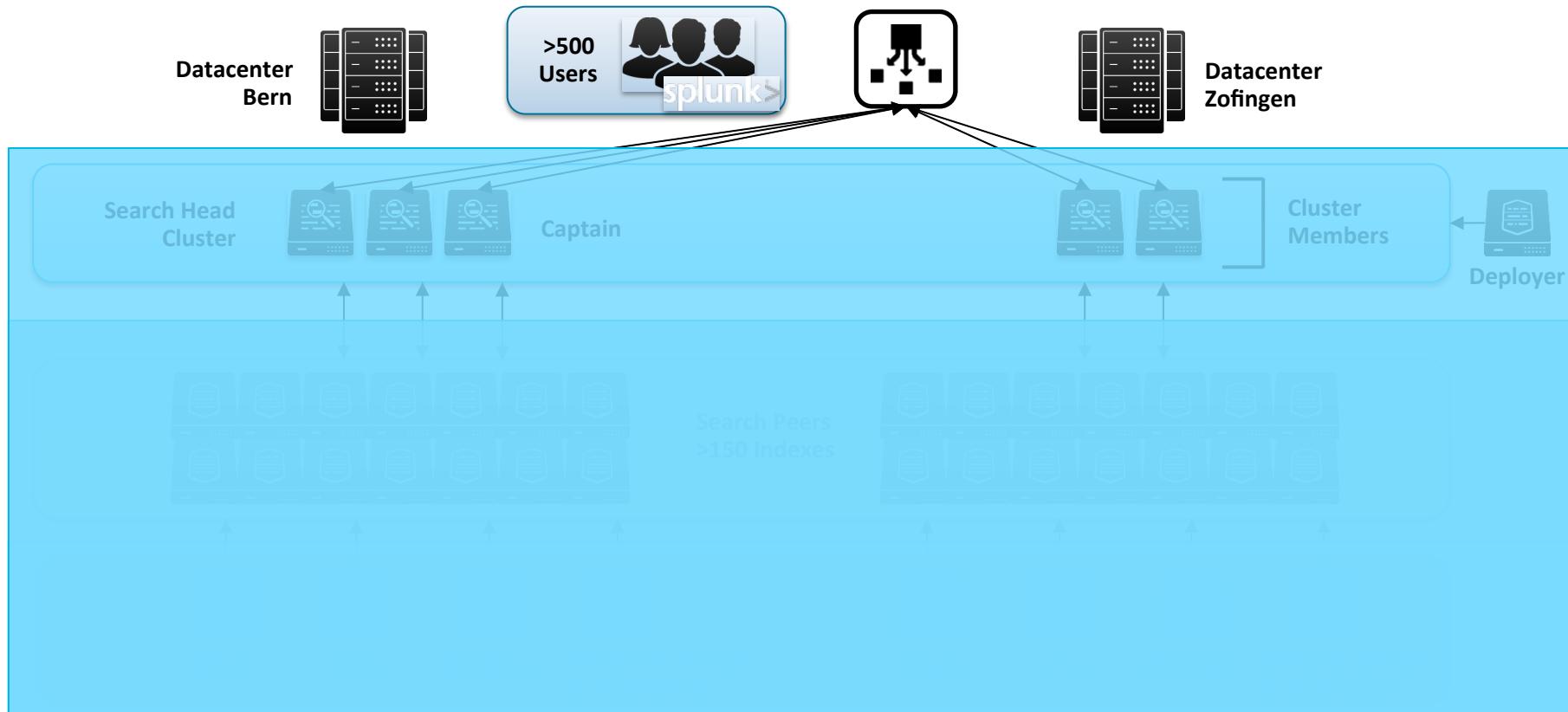
# PostFinance's Splunk Numbers

 <p>Indexing rate average 434 KB/s</p>	 <p>40 Terabytes SAN data (per site)</p>	 <p>Number of applications &gt; 30</p>	 <p>Number of roles 68</p>
 <p>Splunk apps &gt; 55</p>	 <p>28 Splunk indexers</p>	 <p>Cores 480</p>	 <p>800 Searches per minute</p>
 <p>Data volume per day 800GB – 1TB</p>	 <p>Search head cluster 5 Members 1 Deployer</p>	 <p>Memory 2816GB</p>	 <p>Source systems &gt; 2360</p>

# High Level Architecture



# Deployed in Two Datacenters





.conf2015

# Use Case 1: Fraud Detection and Report Generation For E-Payment

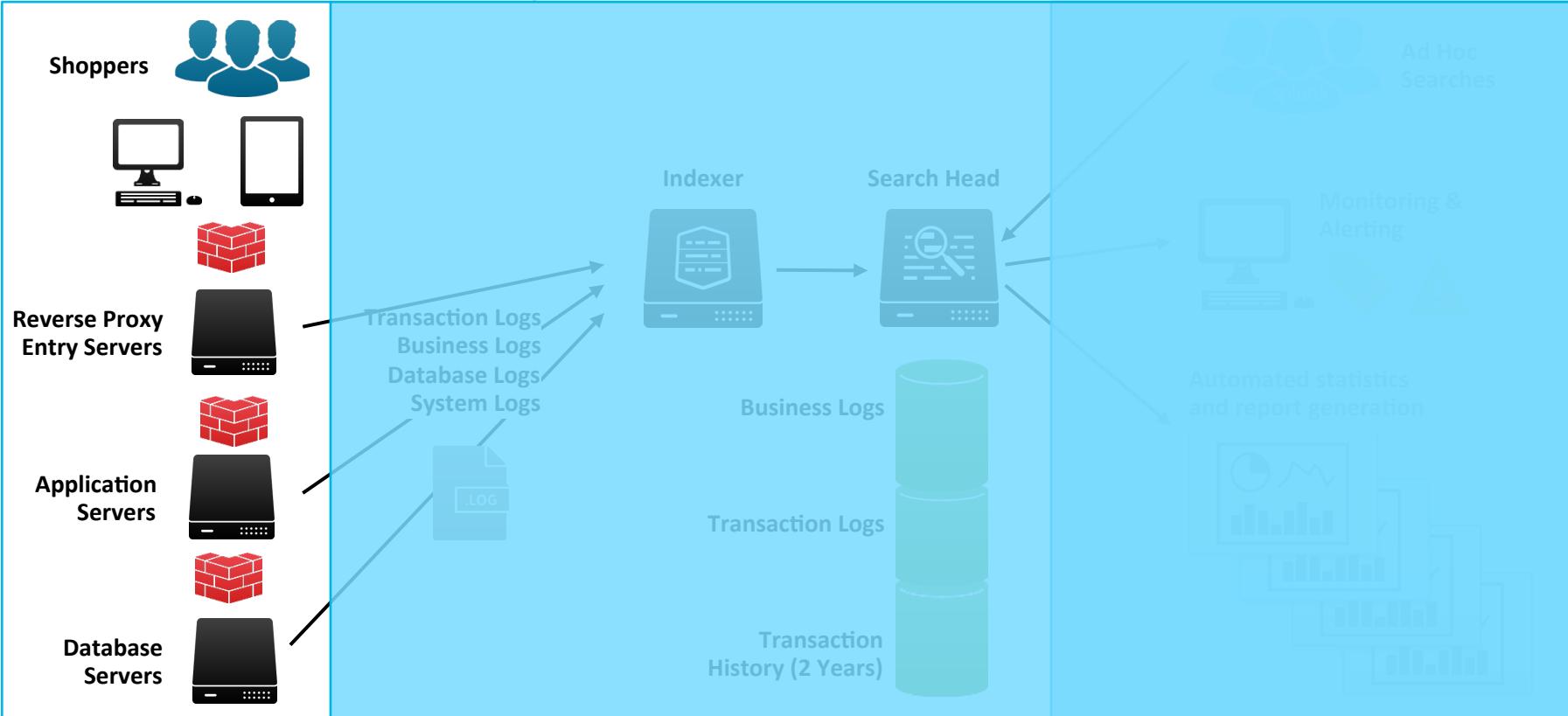
splunk®

# E-Payment - Introduction



E-Payment Platform Info  
Automated Fraud Detection  
General Support Info  
Ad Hoc Searches for Support

# E-Payment - Architecture



# E-Payment - Overview of Splunk Usage

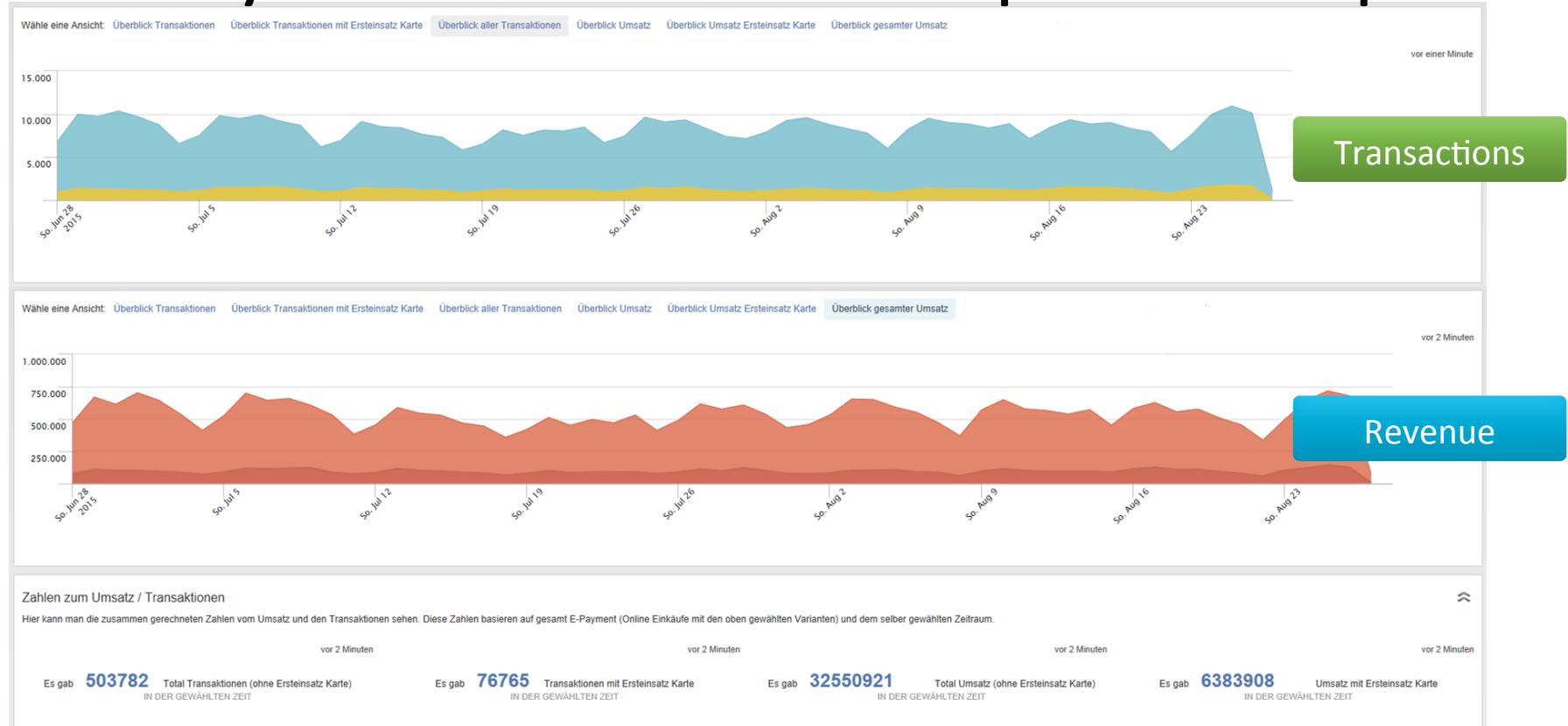
Two main types of Splunk searches:



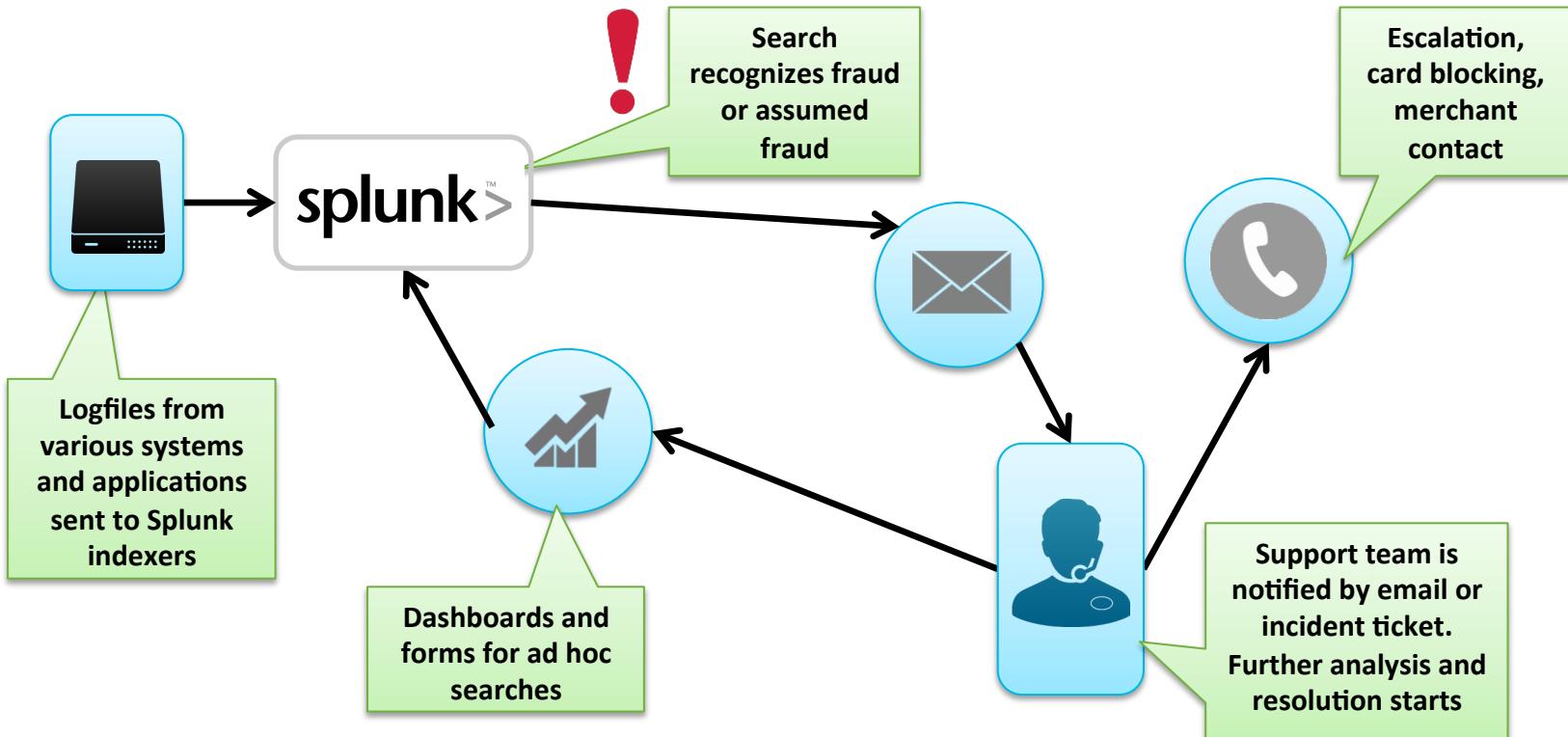
- Examples of global searches:
  - Attempted payments with wrong credentials
  - Payments with same card
  - Number of first time debit card users
  - Transactions close to the card limit
  
- Examples of merchant report searches:
  - Percentage of new buyers
  - Change of revenue



# E-Payment – Merchant Report Example



# E-Payment: Fraud Workflow



# E-Payment – Performance challenges

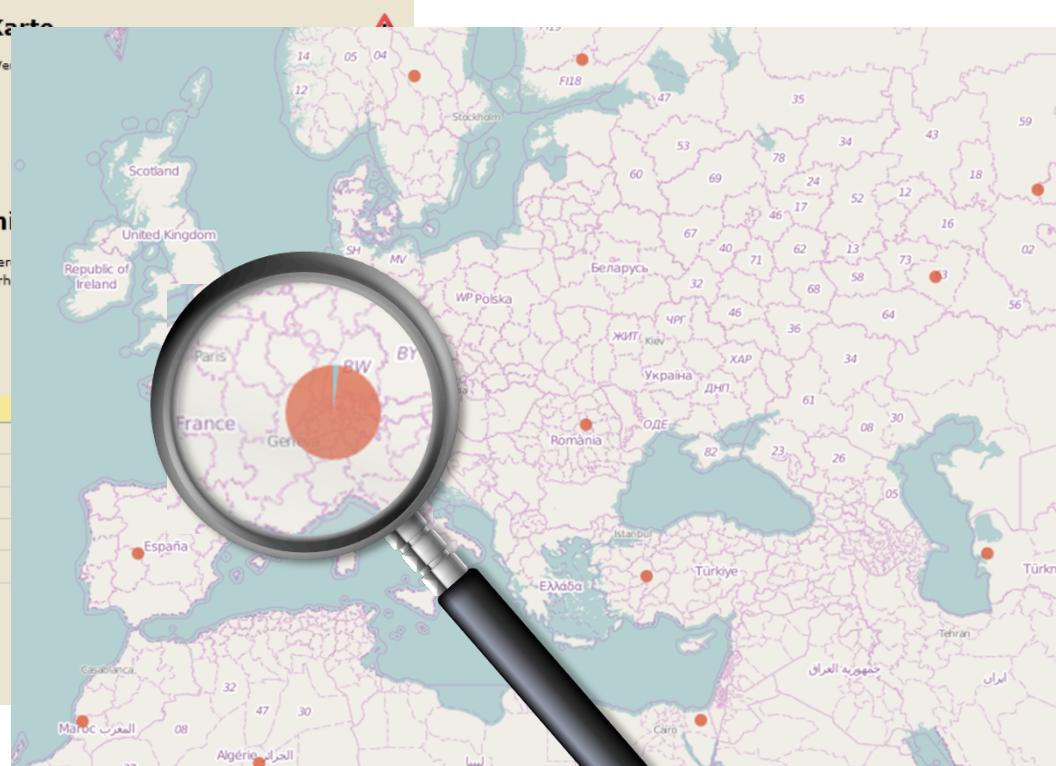
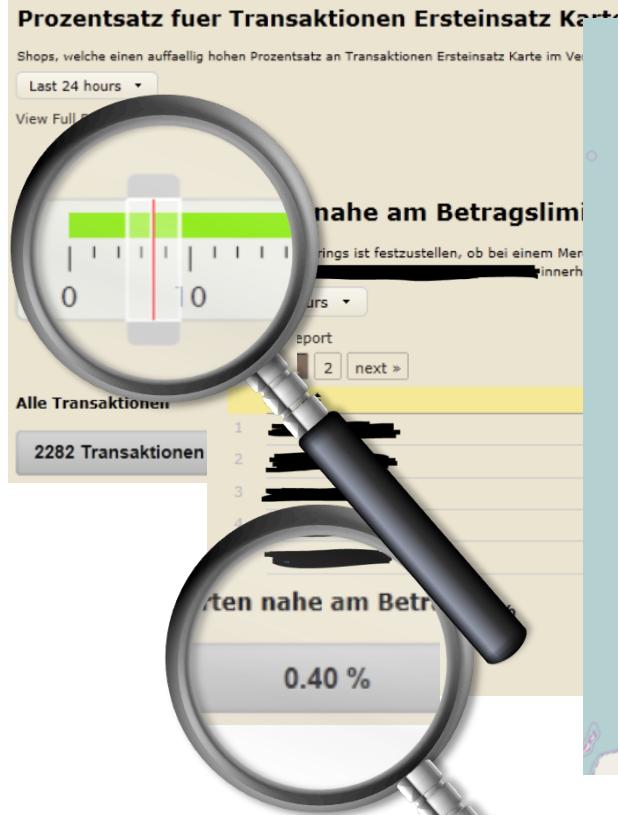
```
index=kgtspod autoResX="OK" (authTypLiteral=" STRING_2" OR authTypLiteral="STRING_1")|  
where trxTypLiteral="PURCHASE" | eval totalBetrag=case(waehrung=="CHF", betrag,  
originalWaehrung=="CHF", originalBetrag, waehrung=="EUR" AND originalWaehrung=="EUR",  
originalBetrag*$eurokurs$) | sistats sum(totalBetrag) as TxUmsatzTagGesamt, min(totalBetrag) as  
TxUmsatzTagMin, max(totalBetrag) as TxUmsatzTagMax, avg(totalBetrag) as TxUmsatzTagAvg by  
merchantId, merchantOrt, merchantName, authTypLiteral
```

```
index=sumkg_turnover_merch_24h_prod(authTypLiteral=" STRING_1" OR authTypLiteral="  
STRING_2") | dedup authTypLiteral, _time, merchantId | bucket_time span=1d | stats  
sum(totalBetrag) as Tagesumsatz by merchantId, _time | join merchantId [search  
index=sumkg_turnover_merch_24h_prod(authTypLiteral=" STRING_1" OR authTypLiteral="  
STRING_2") startdaysago=30] | dedup authTypLiteral, _time, merchantId | bucket_time span=1d |  
stats sum(totalBetrag) as sumTagesumsatz by merchantId, _time | stats avg(sumTagesumsatz) as  
Durchschnitt by merchantId] | eval Schwellenwert=round(Durchschnitt*$thresholdmult$) | where  
Tagesumsatz > Schwellenwert | where Tagesumsatz>$dailyRevenueLim$
```

# E-Payment – Searching for Fraud

```
index=kgtsp prod autoResX="OK" (authTypLiteral="STRING_2" OR authTypLiteral="STRING_1")  
transaction eComRetrievalNr keepevicted=true | where trxTypLiteral="PURCHASE" | eval  
totalBetrag=case(waehrung=="CHF", betrag, originalWaehrung=="CHF", originalBetrag,  
waehrung=="EUR" AND originalWaehrung=="EUR", originalBetrag*$eurokurs$) | stats  
sum(totalBetrag) as Betrag by merchantId, idNr, limiteVID | where (limiteVID<=$lim$ AND  
Betrag>=$amount$) | stats count as KAnzAuffaellig by merchantId | join merchantId [search  
index=kgtsp prod autoResX="OK" (authTypLiteral="STRING_2" OR authTypLiteral="STRING_1")  
transaction eComRetrievalNr keepevicted=true | where trxTypLiteral="PURCHASE" | stats count as  
KAnzGesamt by merchantId] | eval PzeAuffaellig=KAnzAuffaellig*100/KAnzGesamt | join merchantId  
[search index=kgtsp prod (authTypLiteral="STRING_1" OR authTypLiteral="STRING_2") | transaction  
eComRetrievalNr keepevicted=true | where trxTypLiteral="PURCHASE" | where (authResX="NOK"  
AND authResX="OK") | stats count(sourcetype) as KAnzLimit by merchantId] | eval  
PzeLimit=KAnzLimit*100/KAnzGesamt | where (PzeLimit >=$pzelim$ AND PzeAuffaellig  
>=$pzeauf$)
```

# E-Payment – Dashboard Examples



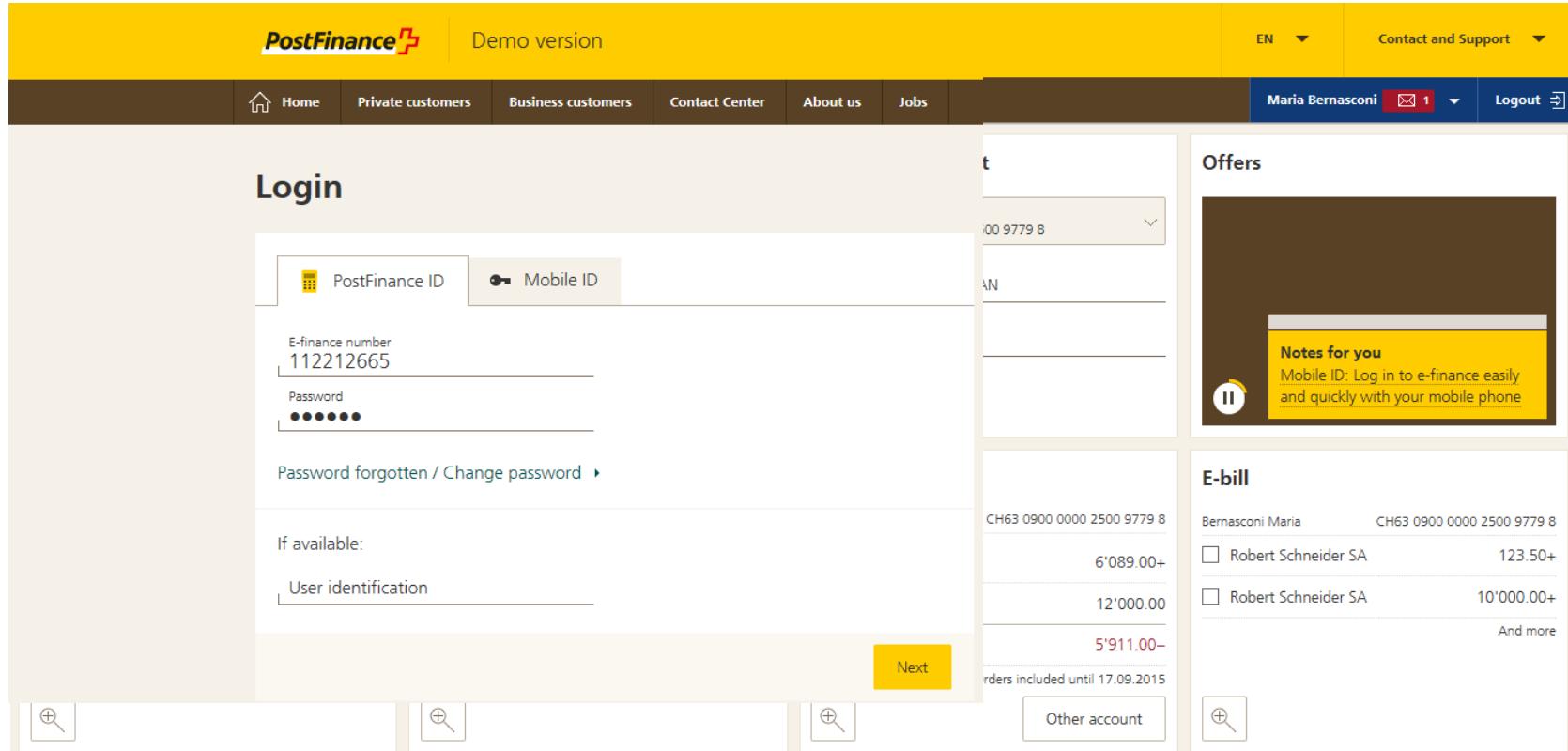


.conf2015

## Use Case 2: Online Banking Security and Threat Detection

splunk®

# PostFinance – E-Finance Introduction



The screenshot shows the PostFinance E-Finance login page. At the top, there's a yellow header bar with the PostFinance logo, a "Demo version" link, language selection (EN), and contact support links. Below the header is a dark brown navigation bar with links for Home, Private customers, Business customers, Contact Center, About us, and Jobs. A user profile for "Maria Bernasconi" is shown on the right, along with a "Logout" button.

The main content area has a light beige background. It features a "Login" heading. Below it are two input fields: "PostFinance ID" (selected) and "Mobile ID". Underneath these are fields for "E-finance number" (containing "112212665") and "Password" (with a masked input). To the right of the password field is a dropdown menu showing "CH63 0900 0000 2500 9779 8". Below the password field is a link for "Password forgotten / Change password".

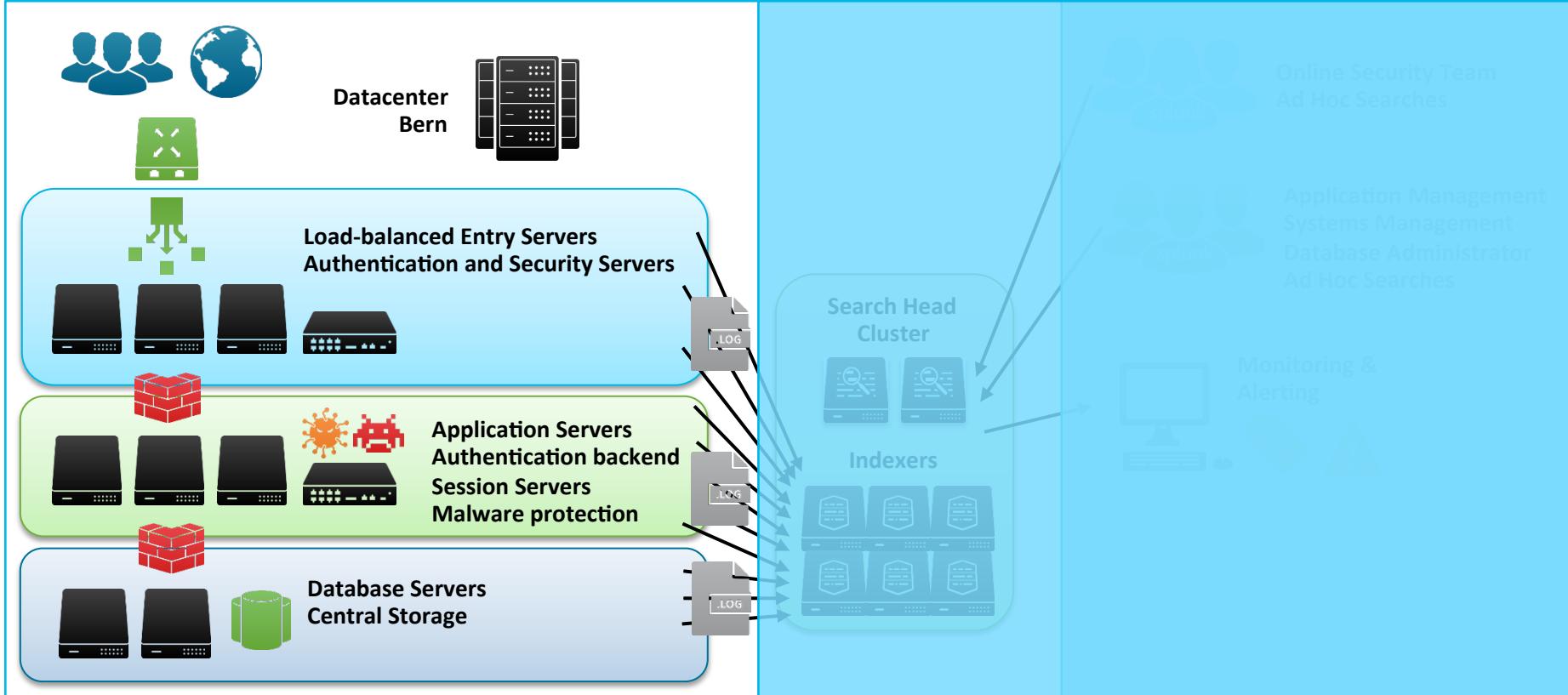
On the left side, there's a section for "User identification" with a dropdown menu showing "CH63 0900 0000 2500 9779 8". To the right of this is a "Next" button.

On the right side, there are two sections: "Offers" and "E-bill". The "Offers" section contains a large brown box and a yellow box with the text "Notes for you: Mobile ID: Log in to e-finance easily and quickly with your mobile phone". The "E-bill" section shows a table of bills:

Bernasconi Maria	CH63 0900 0000 2500 9779 8
<input type="checkbox"/> Robert Schneider SA	123.50+
<input type="checkbox"/> Robert Schneider SA	10'000.00+
And more	

At the bottom, there are search and filter icons, and a "Other account" button.

# E-Finance - Architecture



# Online Banking - Phishing

Von: "PostFinance" <[online](#)>  
Betreff: BetreffAW: Sicher  
Datum: 30. Dezember 2014  
An: [REDACTED]

Sehr geehrte Kundin,  
Sehr geehrter Kunde,

Wie Sie wissen, ist die Frist zu abgelaufen. Im Rahmen dessen geändert und Ihr Zugang hat Zugangen manche der neuen. Diese Fehler können manuell schon alle neuen Features des. klicken Sie bitte untenstehen.

[Klicken Sie hier ->](#)

Nach Ausfüllen des Formulars Finance -Abteilung generiert, einem/einer unserer Mitarbeiter Fehler zu beheben. Bitte führen um Ihr E-Finance auch weiter.

Wir danken Ihnen für Ihre Zu-



# E-Finance - Phishing Attack Workflow

Von: "PostFinance" <[online.sicherheit@postfinance.ch](mailto:online.sicherheit@postfinance.ch)>

Betreff: BetreffAW: Sicherheitsinformation

Datum: 30. Dezember 2014 21:28:28 MEZ

An:



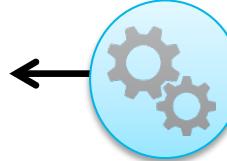
The online security team is notified about a new phishing attack by email



Security team analyzes the new attack patterns

All transactions are rated using CEP rules

Operationalize the findings for use in daily business



Date	Posting details	Details
22.08.2015	E-FINANCE 25-9034-2 ROBERT SCHNEIDER SA 2503 BIENNE	16590213 14:44:08.401 de Authenticate N_2000 WebAuth.E.1 16590213 14:44:08.401 de ProcessAuthenticationCheck N_2000 WebAuth.E.1 21060213 08:35:41.401 de Authenticate N_2000 WebAuth.E.1 04690213 09:35:50.701 de Authenticate N_2000 WebAuth.E.1 04690213 09:35:51.701 de ProcessAuthenticationCheck N_2000 WebAuth.E.1

PostFinance Demo version

Login

PostFinance ID or Mobile ID

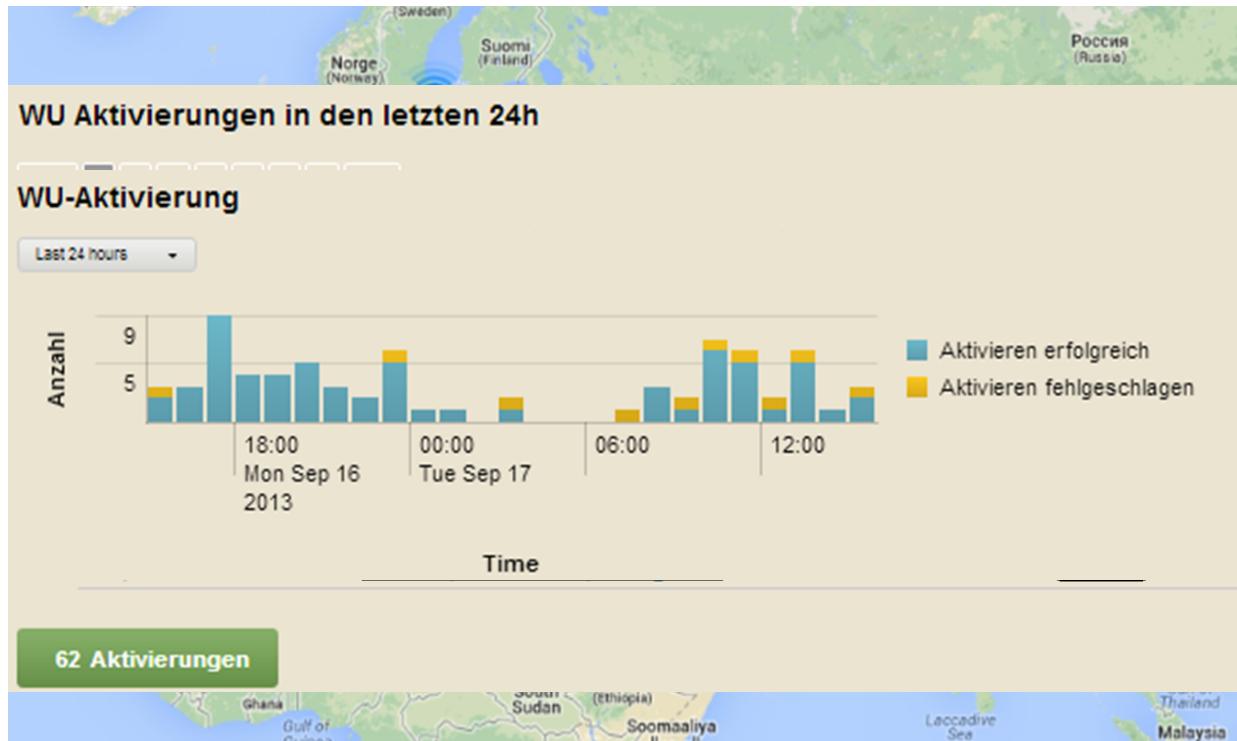
E-finance number 112212665

Password

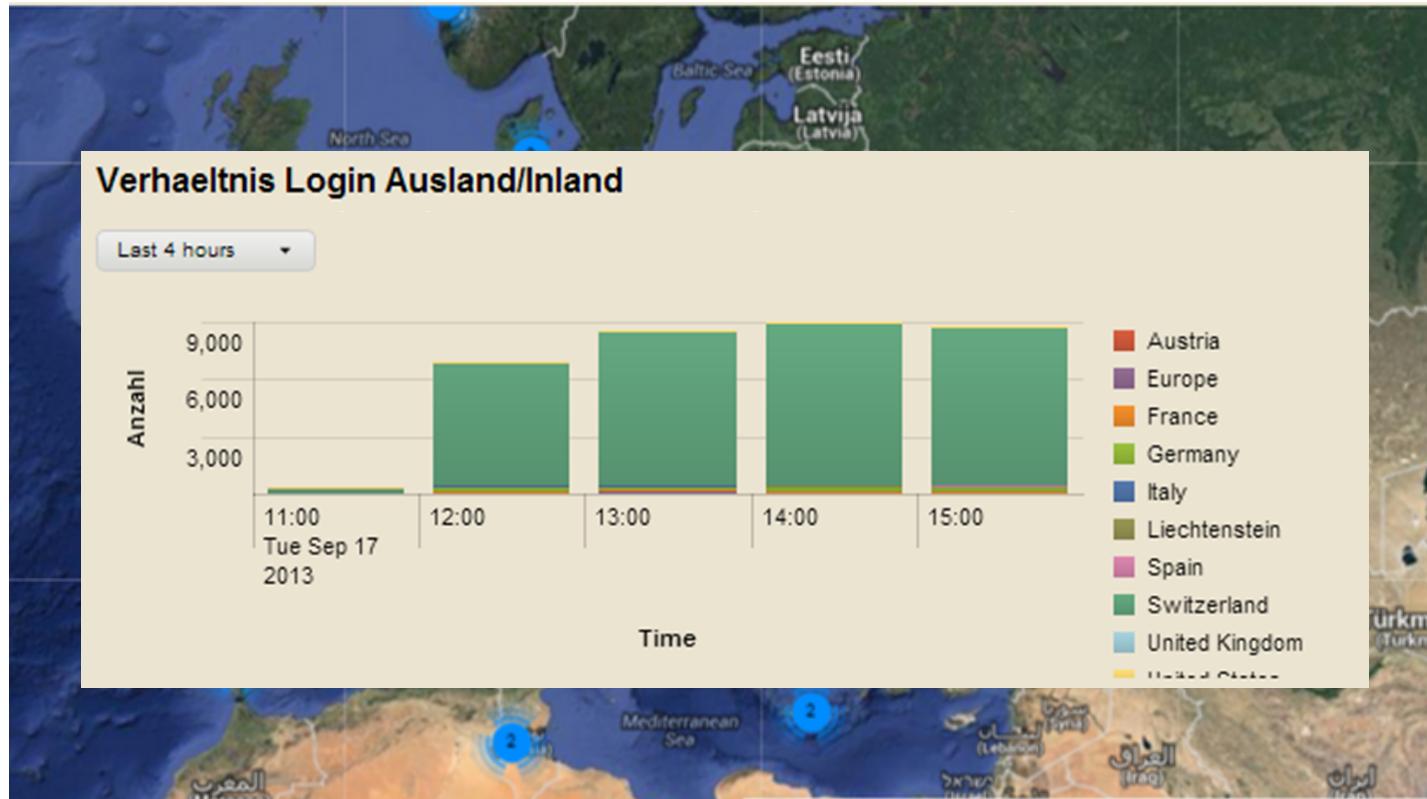
Forgot password / Change password

splunk®

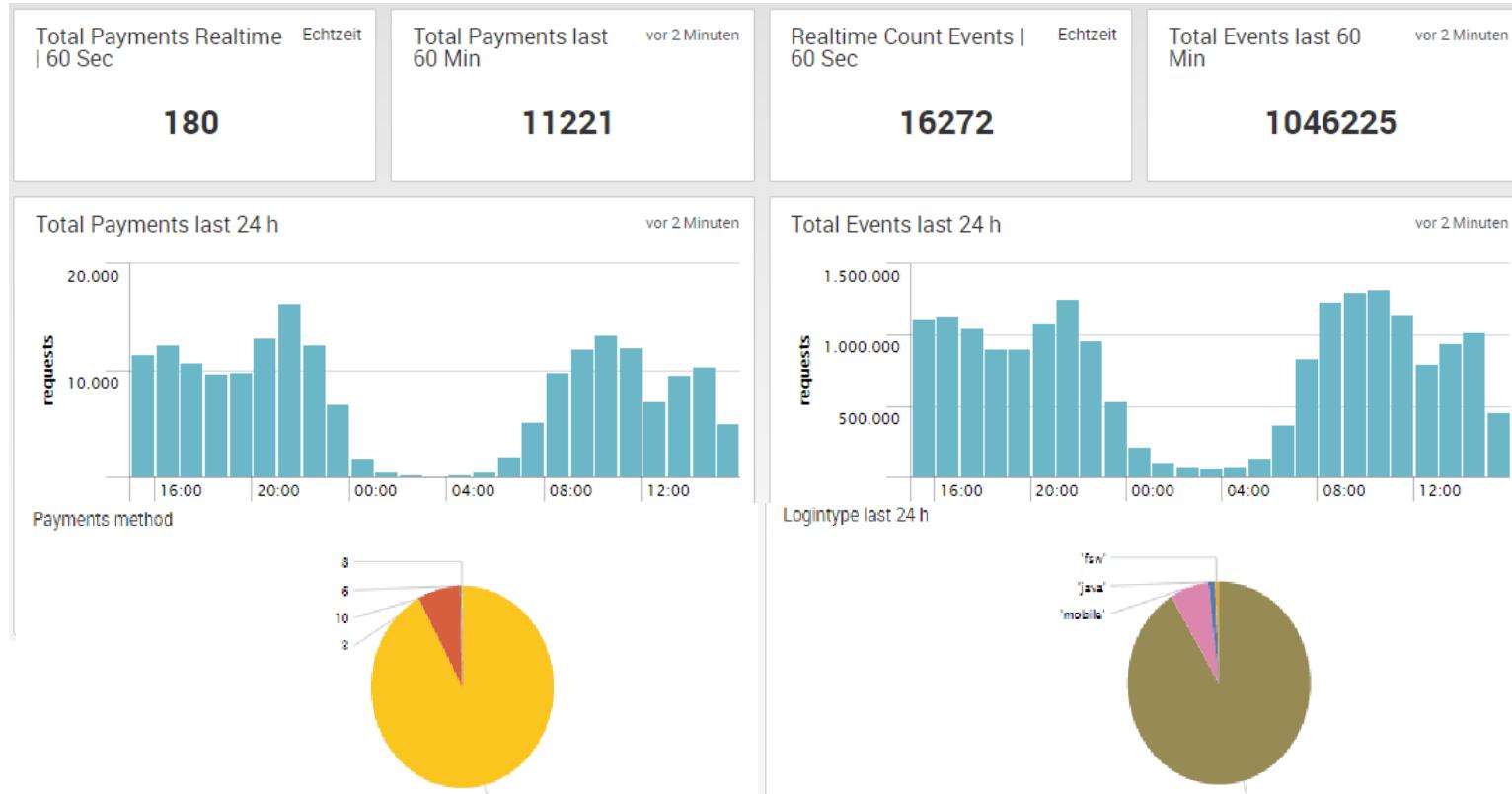
# Online Banking Security – Western Union



# Online Banking Security – Login Behavior



# Online Banking Security – OI





# .conf2015

## Wrap-Up



splunk®

# Wrap-Up: Success Factors

- Start small, think big
- Dedicated «virtual» team
- Business value always in mind
- Show & tell
- Have security on priority list
- Regulatory tightening
- Management support



.conf2015



THANK YOU

splunk®