(K)eine Gratwanderung!
Sicher in die Cloud

The Swiss Cyber Security Service
Security partner of successful companies that want to remain relevant in the digitized economy.

Marcial Rion
Senior Architect
United Security Providers AG
## Agenda

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our View on the Market Development</td>
</tr>
<tr>
<td>2</td>
<td>Cloud Security Challenges</td>
</tr>
<tr>
<td>3</td>
<td>Real World Use Case</td>
</tr>
<tr>
<td>4</td>
<td>Take Away</td>
</tr>
</tbody>
</table>
The Age of Digital

Digital transformation

Engage Your Customers
Empower Your Employees
Optimize Your Business
Transform Your Products

Ubiquitous use of new digital technologies

Dependency on Data Identities Access Value of Cloud

Importance of Security
Connecting → Increasing attack surface

Connecting → Increasing attack surface

Everything gets connected

More and more breaches

Estimated cost of cyber crime

$2.5 trillion

Source: Mike A. Thompson from rawpixel

Source: Juniper Research & Forbes
What’s Your Preferred Cloud Provider?

61 Swiss Cloud Providers

Plan for a hybrid multi-Cloud situation as your future “normal situation”
### Agenda

<table>
<thead>
<tr>
<th></th>
<th>Agenda Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our View on the Market Development</td>
</tr>
<tr>
<td>2</td>
<td>Cloud Security Challenges</td>
</tr>
<tr>
<td>3</td>
<td>Real World Use Case</td>
</tr>
<tr>
<td>4</td>
<td>Take Away</td>
</tr>
</tbody>
</table>
KEY SURVEY FINDINGS

1. **Cloud security concerns** – While adoption of cloud computing continues to surge, security concerns are showing no signs of abating. Reversing a multi-year downward trend, nine out of ten cybersecurity professionals confirm they are concerned about cloud security, up 11 percentage points from last year’s cloud security survey. The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).

2. **Biggest threats to cloud security** – Misconfiguration of cloud platforms jumped to the number one spot in this year’s survey as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

3. **Cloud security headaches** – As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top three security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent).

4. **Legacy security tools limited in the cloud** – Only 16 percent of organizations report that the capabilities of traditional security tools are sufficient to manage security across the cloud, a 6 percentage point drop from our previous survey. Eighty-four percent say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.

5. **Paths to stronger cloud security** – For the second year in a row, training and certification of current IT staff (57 percent) ranks as the most popular path to meet evolving security needs. Fifty percent of respondents use their cloud provider’s security tools and 35 percent deploy third-party security software to ensure the proper cloud security controls are implemented.

6. **Cloud security budgets increase** – Looking ahead, close to half of organizations (49 percent) expect cloud security budgets to go up, with a median budget increase of 28 percent.
What we often hear and observe

Handling Access Management

• **Business first**
  - Standard applications are published as advised in the manufacturer's manual
  - The application landscape has grown, many well-known "small" problem areas have emerged
  - The business projects are lagging behind, time to market is crucial
  - Clients are only willing to pay for more functionality, not for more security

• **Ignoring the risks**
  - We have no sensitive data / we are not a bank / there is nothing of interest to gain here
  - We have just invested in a new firewall
  - Our hosting provider has to take care of that
  - We never had a critical incident so far
  - Username and password is considered secure

• **Missing systems, lack of know-how, lack of time**
  - There is no infrastructure for protecting web applications
  - Little know-how about how to organize user administration and how to implement authentication
    → each business unit / application team helps itself
  - There is no monitoring system in place
  - Nobody has time to evaluate the logfiles ("what logfiles?")

  **Adversity is the school of wisdom!**
## Agenda

<table>
<thead>
<tr>
<th></th>
<th>Agenda Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our View on the Market Development</td>
</tr>
<tr>
<td>2</td>
<td>Cloud Security Challenges</td>
</tr>
<tr>
<td>3</td>
<td><strong>Real World Use Case</strong></td>
</tr>
<tr>
<td>4</td>
<td>Take Away</td>
</tr>
</tbody>
</table>
Real World Use Case

Clients are moving their applications to (public) cloud providers
At the same time, they are changing their development processes
More agile development, DevOps oriented deployment approaches

-> We had to bring our Web access management solution to the Cloud
The Challenge
Implications of agile application development and DevOps

Understanding the Hybrid Multi Cloud Security Challenges

**Corporate security baseline**
Security wants to enforce a common baseline for all applications, regardless the distributed architecture and the deployed application infrastructure.

**Application-centric deployment**
Agile development processes combined with DevOps approaches in deployment require that WAF / authentication enforcement is deployed within the applications environment and shares its life cycle and delivery chain.

**Dynamic orchestration and automation**
Scaling-up arbitrarily and dynamically is an important requirement for some apps. New releases need to be introduced into the deployments from a central deployment point. An API for connecting and automating deployment and easing off maintenance is required.

**Central detection and reporting**
Corporate detection and reporting capabilities are crucial in the context of growing cyber security risks (not all current SIEM-based solutions are able to cope with dynamically orchestrated instances).
Solving the Magic

1. Deconstruct solution to components, check path to Cloud for each of them
2. Provide SaaS-based, multi-tenancy capable user interface
3. Embrace container technologies
4. Prepare for automation via self-service APIs
5. Solve centralized logging, detection and reporting
Corporate security baseline and application-centric deployment

**Distributed Configuration Management & Operations**

1. SaaS provides Containers in Registry
2. Security specialist provides configuration
3. Application Owner deploys WAF with downloaded config. Behavior is adapted through parametrization.

Customer

(Cloud-based) SaaS

- Central Configuration Management
- Platform Deployment
- Platform Build

Security Service Owner

Application Owner

User Interface

Container "Runtime"

Container Registry
Central detection and reporting

Anomaly Detection & Reporting for on Prem & Cloud

4 All WAFs logs to central SaaS log data store used for reporting
Central detection and reporting

Anomaly Detection & Reporting for on Prem & Cloud

Customer

User Interface

Security Service Owner

Application Owner

(Cloud-based) SaaS

Central Configuration Management

Platform Deployment

Platform Build

Log Environment

Container "Runtime"
Centralized Authentication

Security Service Owner

Application Owner

User Interface

Customer

(Cloud-based) SaaS

Authentication delegation via SAML or OpenID Connect

Central Configuration Management

Platform Deployment

Platform Build

Container "Runtime"

Authentication
Dynamic orchestration and automation

**API-enabled Self Services**

![Diagram of API-enabled Self Services]

1. **User Interface**
2. **Self Service API**
3. **Container "Runtime"**
4. **Log Environment**
5. **Central Configuration Management**
6. **Platform Deployment**
7. **Platform Build**
8. **Security Service Owner**
9. **Application Owner**

(Cloud-based) SaaS

- **Automated configuration changes / deployments via API**

22.01.2019 Meet Swiss Infosec
## Agenda

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our View on the Market Development</td>
</tr>
<tr>
<td>2</td>
<td>Cloud Security Challenges</td>
</tr>
<tr>
<td>3</td>
<td>Real World Use Case</td>
</tr>
<tr>
<td>4</td>
<td>Take Away</td>
</tr>
</tbody>
</table>
Take Away

• Enterprises all over the world are struggling to mitigate the growing cyber risks
• The importance of data an Cloud grows, and so does importance of security
• Enterprises should plan for a hybrid, multi-Cloud environment

• Value of traditional security tools to Cloud is limited
• Misconfiguration of cloud platforms is a key threat to Cloud security

• Maintaining a corporate security baseline and central detection and reporting while using various onboard tools is nearly impossible

• Embrace containerization

• Journey to the Cloud often requires solution deconstruction into components and re-engineering of existing operation models
The Swiss Cyber Security Service

Security partner of successful companies that want to remain relevant in the digitized economy.