# All-Hands-on-Deck

Der Kulturwandel hin zu dezentraler Security


Christoph Schuhwerk

CISO (EMEA), Zscaler


Yes
No


Complexity is the enemy of Reliability

Security

Experience

# Cyber Security Operations in the Good Old Days

Cyber operations teams were responsible for **managing cyber tools** and dependent **security infrastructure**

We **deployed our secu**
**stack** nsure we
**ade**

We built our castle, moat and **fortified our perimeter**

Those days are gone!

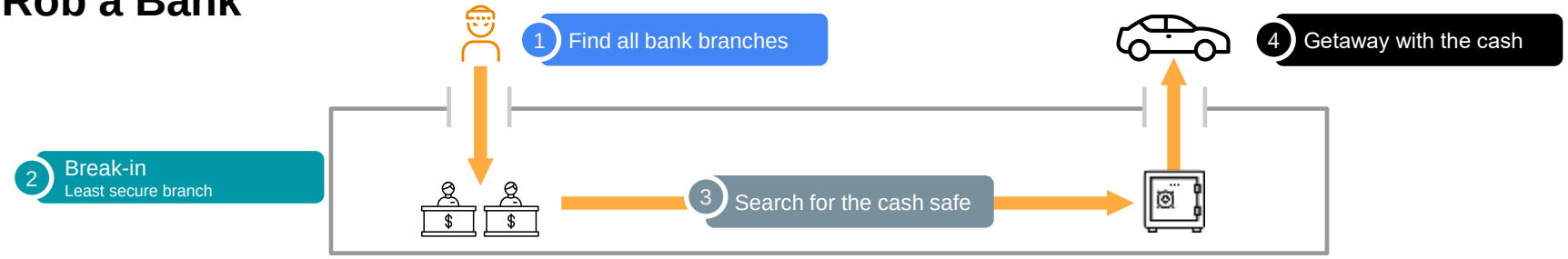
**We had the time** to manage, monitor, analyze and tune our **tools**

Everything **going in and out of the network** used the same path to **apply security policies**

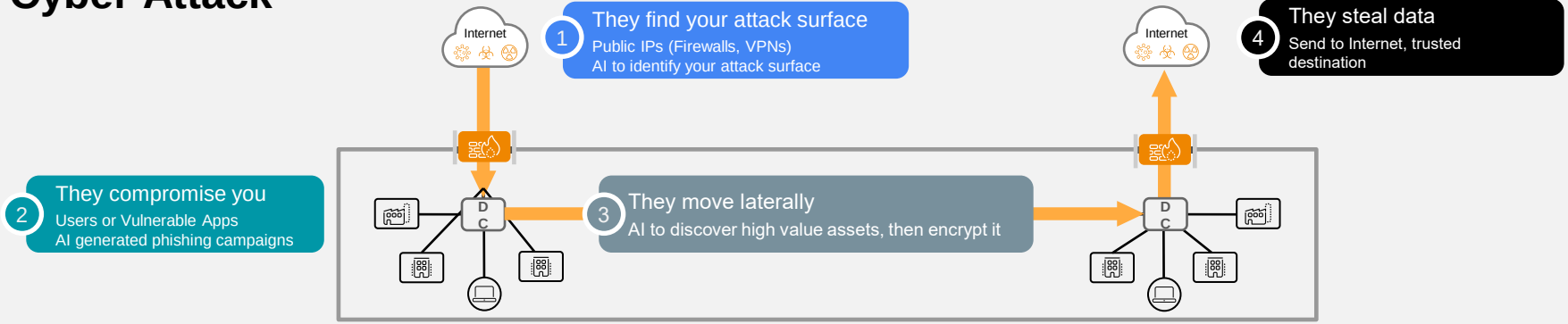
**Cloud** was largely IaaS and security was managed with the **same tools as in a Data Center**

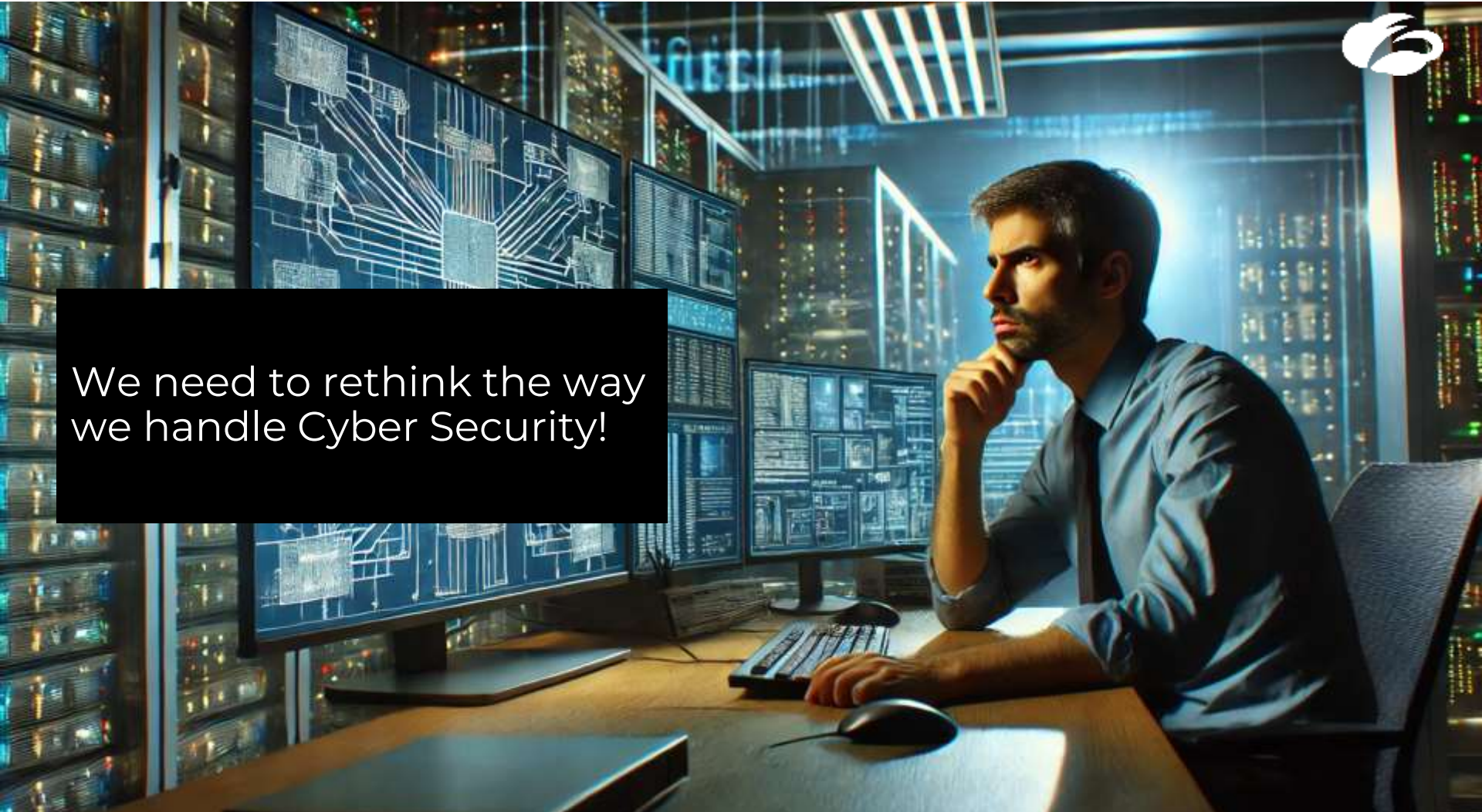
# How Cyber Breaches Happen

## 4 Steps to Rob a Bank

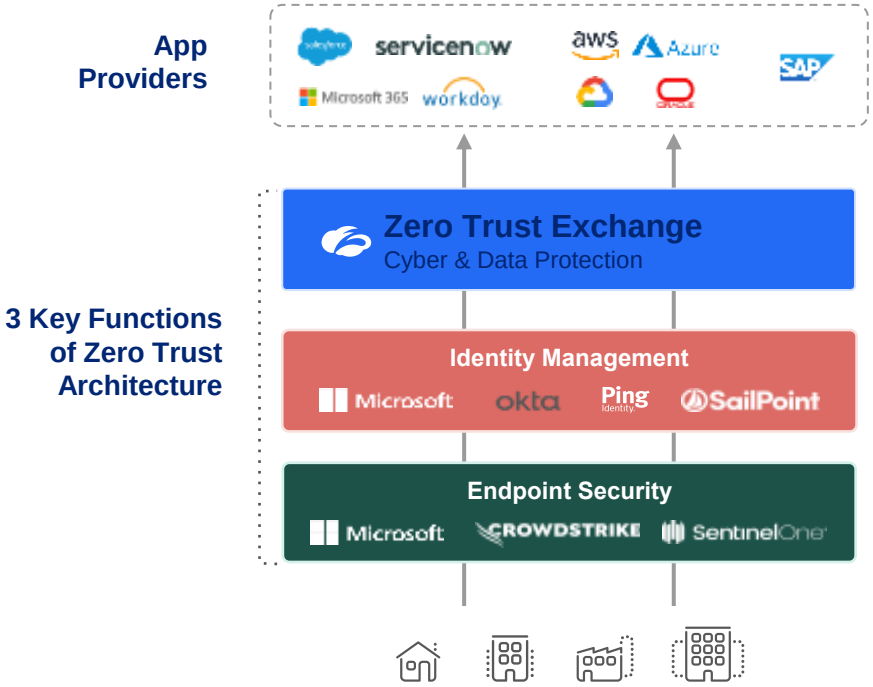



## 4 Steps for a Cyber Attack




We need to rethink the way we handle Cyber Security!

# Consolidate on a few Integrated Platforms




**Don’t depend upon a single security provider**
3 Key Functions from 3 separate providers

# What is common to all those platforms?

**They apply custom policies to enforce rules!**

# What makes a good policy?

- Least Privilege (Least Trust)
- Risk-based
- Enforcing compliance
- Effective against Threats
- Does not interrupt regular business tasks
- Clear responsibilities
- Regular review and update

# Now let’s define good policies...

# Global vs. Transaction-specific Policies

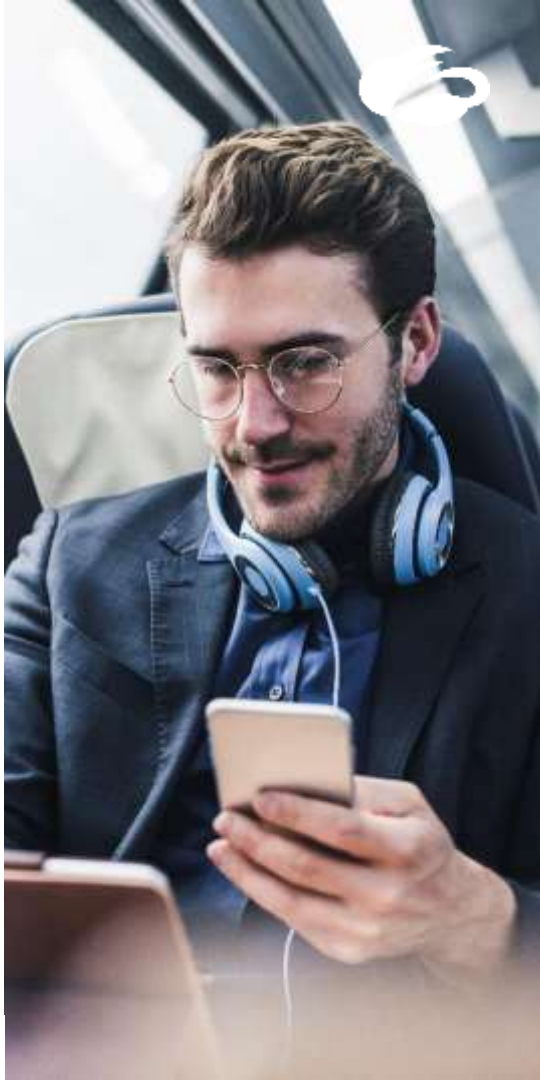
- Global Policies
  - Apply to **all** users and workloads alike
  - Can be defined by the **central teams** (e.g. Cyber Security, Network)
  - **Examples**:
    - No RDP to end user devices
    - No upload to the internet > 5 GB/day

- Application-specific Policies
  - Are tailored to **one** or a group of applications
  - Can only be **defined by** business (data) and **IT (application) owners** / experts
  - Goes hand in hand with the **authorization** concept within the app
  - Define **who** can access which **data** from which **device** at which **time** and from which **location**

Global Policies form the frame. Shift Left for app-specific policies.

# How can organizations unlock Shift-Left?

- **Empower** employees
- Form a „Security first“ **Culture**
- Leaders need to do **motivation** talks at every possible occasion (Guild meetings, Application Owner conferences, Townhall events, …)
- Security Platforms give insights to form policies based on the status quo (using **ML**)
- Make sure they are regularly reviewed and **challenged**
- Publish a **Reward** Program for Policy Improvement



# Executive Summary

- The modern **threat** landscape continues to evolve
- Classic IT architectures increase **complexity** to cope with it
- Modern **zero trust architectures** offer a lean way out, splitting security from network
- Deploying few centralized **platforms** is the foundation for proactive defense
- To make use of these platforms, the **policies** within are essential
- Creation and maintenance of „good“ policies takes time and continuous **improvement**
- Motivation and **empowerment** of employees is key to establishing policies that can successfully defend cyber attacks

- **Plan for the Security Culture change to benefit as an entire organization**

# Zero Trust Learning Resources

**Seven Elements of Highly Successful Zero Trust Architecture**

**7 Questions Every CXO Must Ask about Zero Trust**

# Thank you!

Enjoy it-sa!

Visit Zscaler in Hall 6 - 324