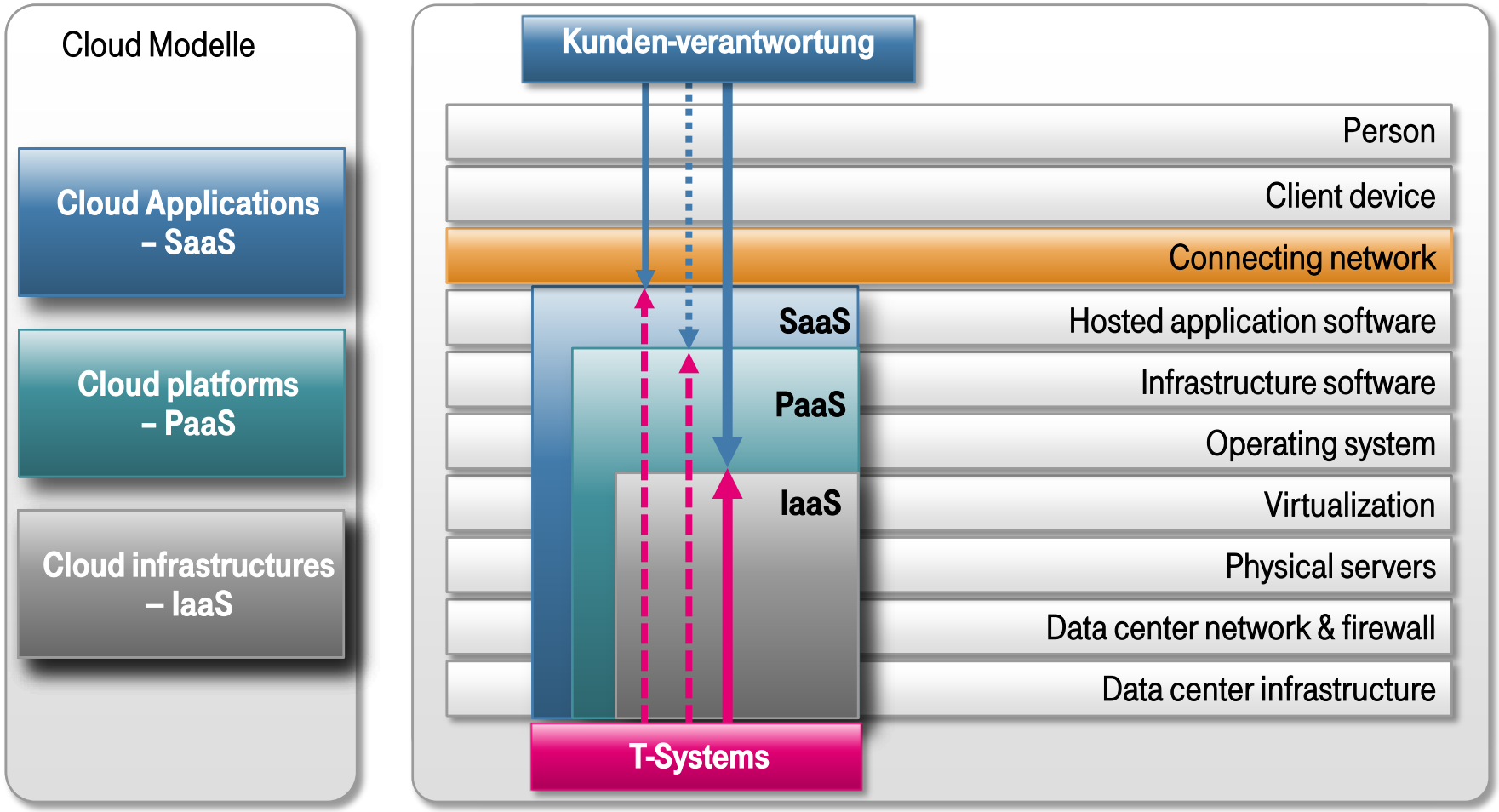
INNOVATIONSWORKSHOP 2014
CLOUD LÖSUNGEN

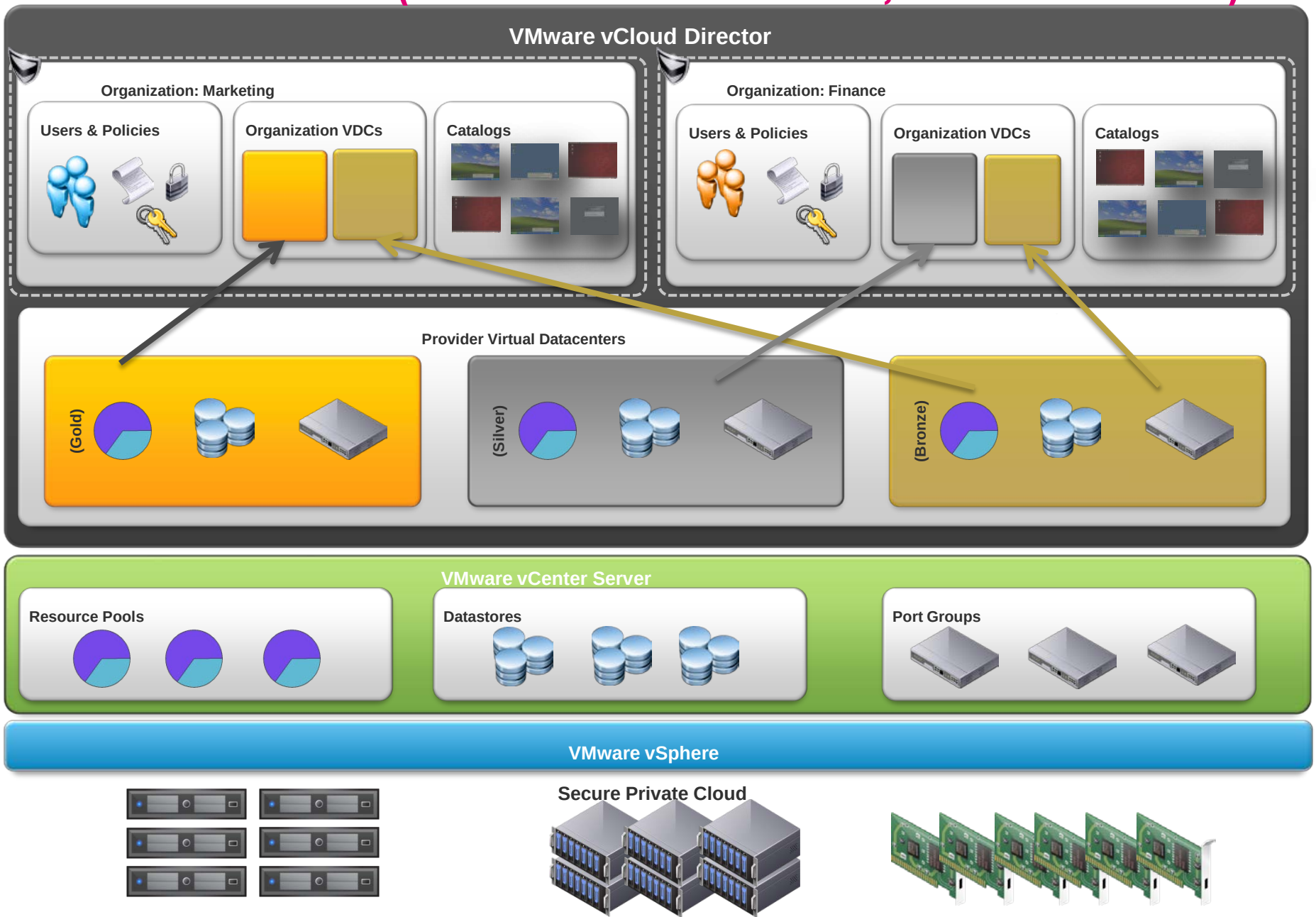
Juli 2013

T · · Systems ·

CLOUD MODELLE



vCloud brings additional abstractions layer und enable providers to sell “virtual Datacenters” (vDC bundles will be offered, called T-Shirt sizes)



T-SYSTEMS DYNAMIC CLOUD PLATFORM. DESIGN - ZIELE

Erlaubt verschiedenste Workloads on top auf der Standard Cloud Plattform

Erster Workload DCS 3

Verringert die Abhängigkeiten zwischen den Layern

DC Infrastruktur, Netzwerk, Hardware, Storage, Operating System, Application Service

Reduziert die Komplexität

Netzwerk - basierender Storage, Backup Integrated Storage, Replace instead of Repair

Komplette Virtualisierung

Vlans, Firewalls, Switches, Storage Systeme, Compute Systeme

Automation

Automation aller Platformaktivitäten

Standardization

Standard Hardware Komponenten und Standardprozesse

T · · Systems ·

DYNAMIC CLOUD PLATFORM AS ARCHITECTURAL BASIS, SUPPORTING JOINT SERVICES WITH PARTNERS.

E2E/SLA MANAGEMENT | BILLING ACCOUNTING | SECURITY MANAGEMENT | OPERATIONAL MGMT

INTEGRATION MANAGEMENT

DSI vCloud DC	Dynamic Services for UC (HCS)	Dynamic Services for Collaboration	Cloud Integration Center	Dynamic Services for SAP Solutions	Dynamic Services for other Solutions	Future Workplace (e.g. VDI)	Dynamic Services for SAP HANA
vmware	CISCO	Microsoft	ORACLE IBM SAP Microsoft	SAP	ORACLE IBM	Microsoft	SAP

COMPUTING SERVICES (COMPUTING & STORAGE)

DYNAMIC CLOUD PLATFORM

NetApp CISCO

NETWORK SERVICES (IP FABRIC/IPLS)

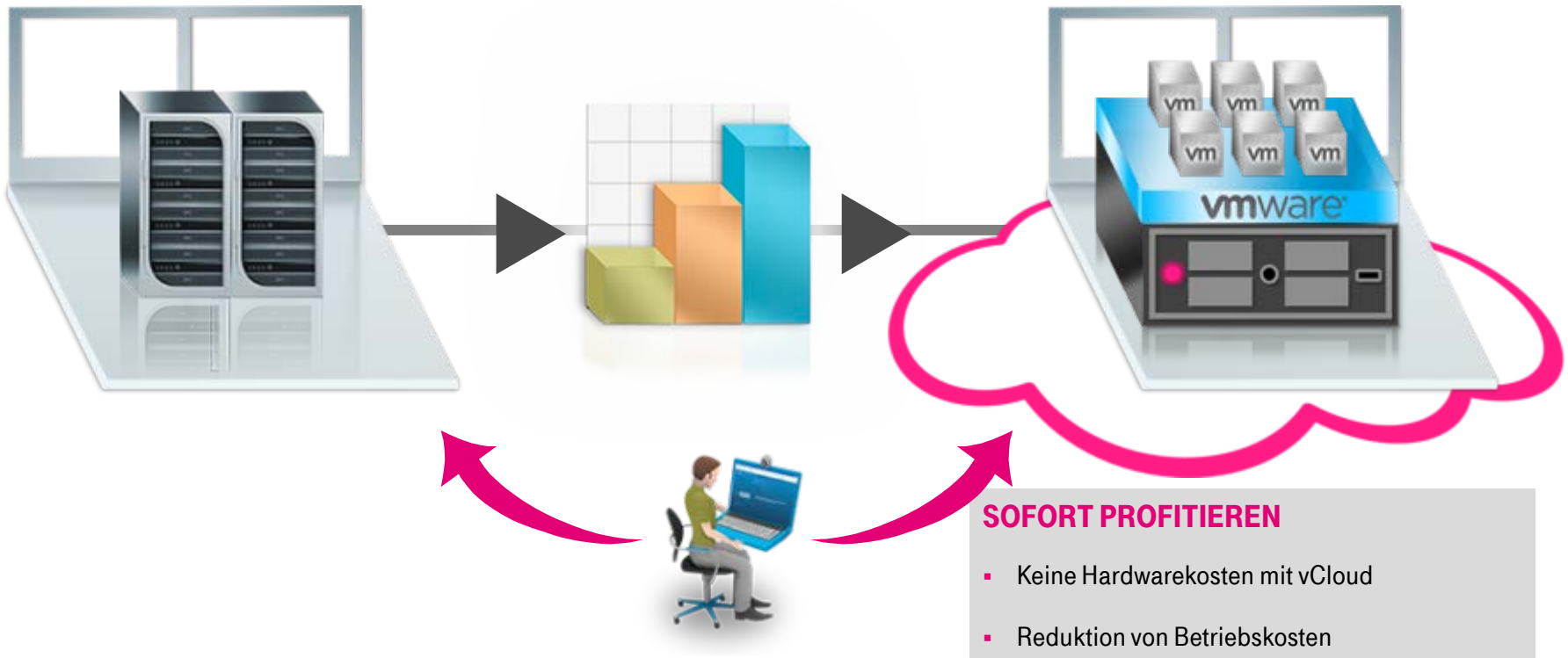
REMOTE BASED ACCESS | PUBLIC IP ACCESS | PRIVATE IP ACCESS

VCLOUD – EIN WEITERER EINSTIEG IN DIE CLOUD

VCLOUD DIRECTOR

RECHENZENTRUM KUNDE/HOUSING

T-SYSTEMS DSI VCLOUD



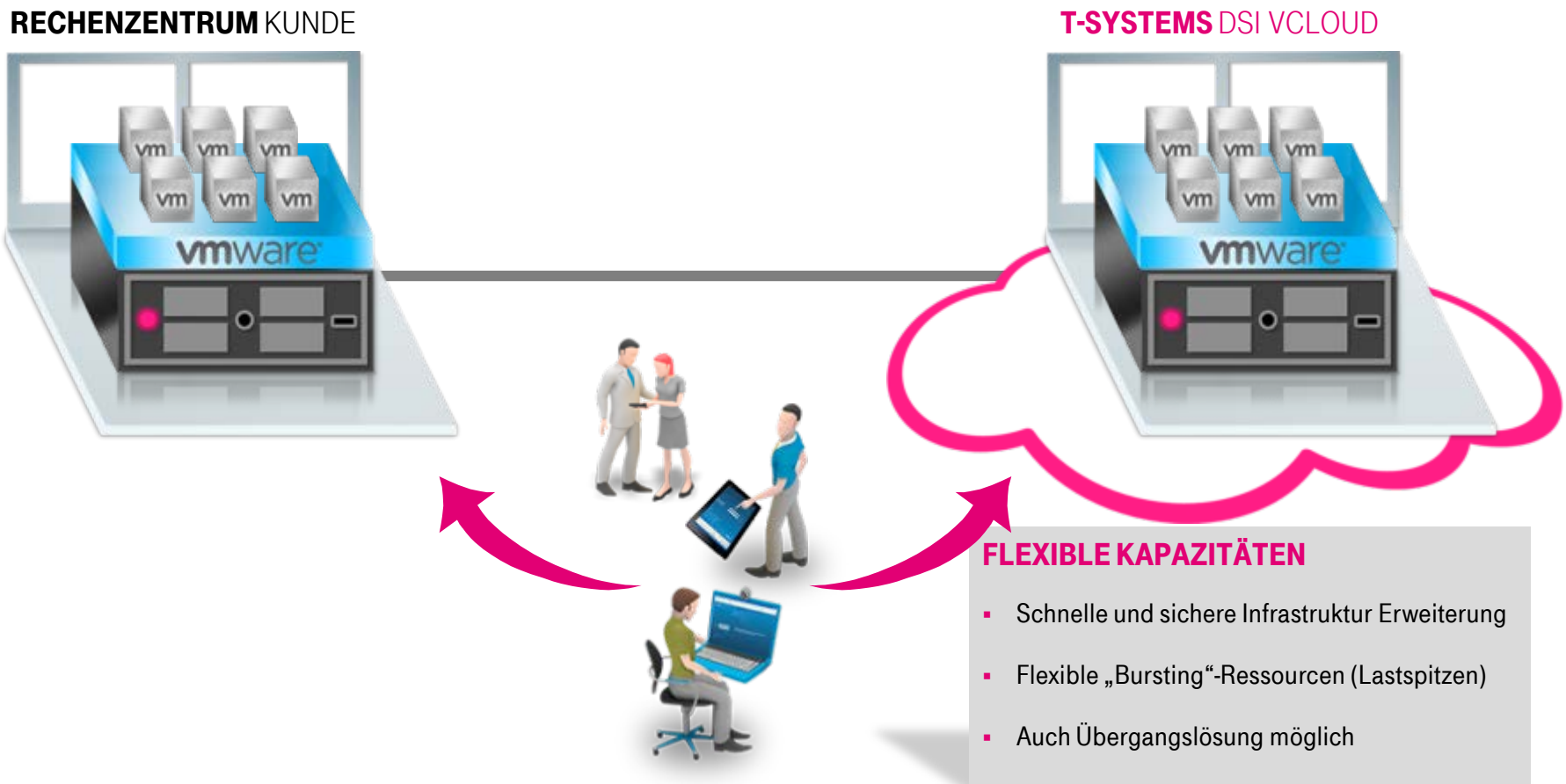
SOFORT PROFITIEREN

- Keine Hardwarekosten mit vCloud
- Reduktion von Betriebskosten
- Neue Geschäftsmodelle umsetzen
- Nur bezahlen, was gebraucht wird (OPEX)

USE CASES – IDEEN FÜR DIE PRAXIS

SCHNELLE ERWEITERUNG DER VORHANDENEN RESSOURCEN

vCENTER SERVER | vCLOUD CONNECTOR | vCLOUD DIRECTOR



FLEXIBLE KAPAZITÄTEN

- Schnelle und sichere Infrastruktur Erweiterung
- Flexible „Bursting“-Ressourcen (Lastspitzen)
- Auch Übergangslösung möglich
- Eigene Management-Oberfläche

DER VERNETZTE SPORTLER – RUNTASTIC ATMET vCLOUD

Fitnessportal + App für den persönlichen Fitnessplan

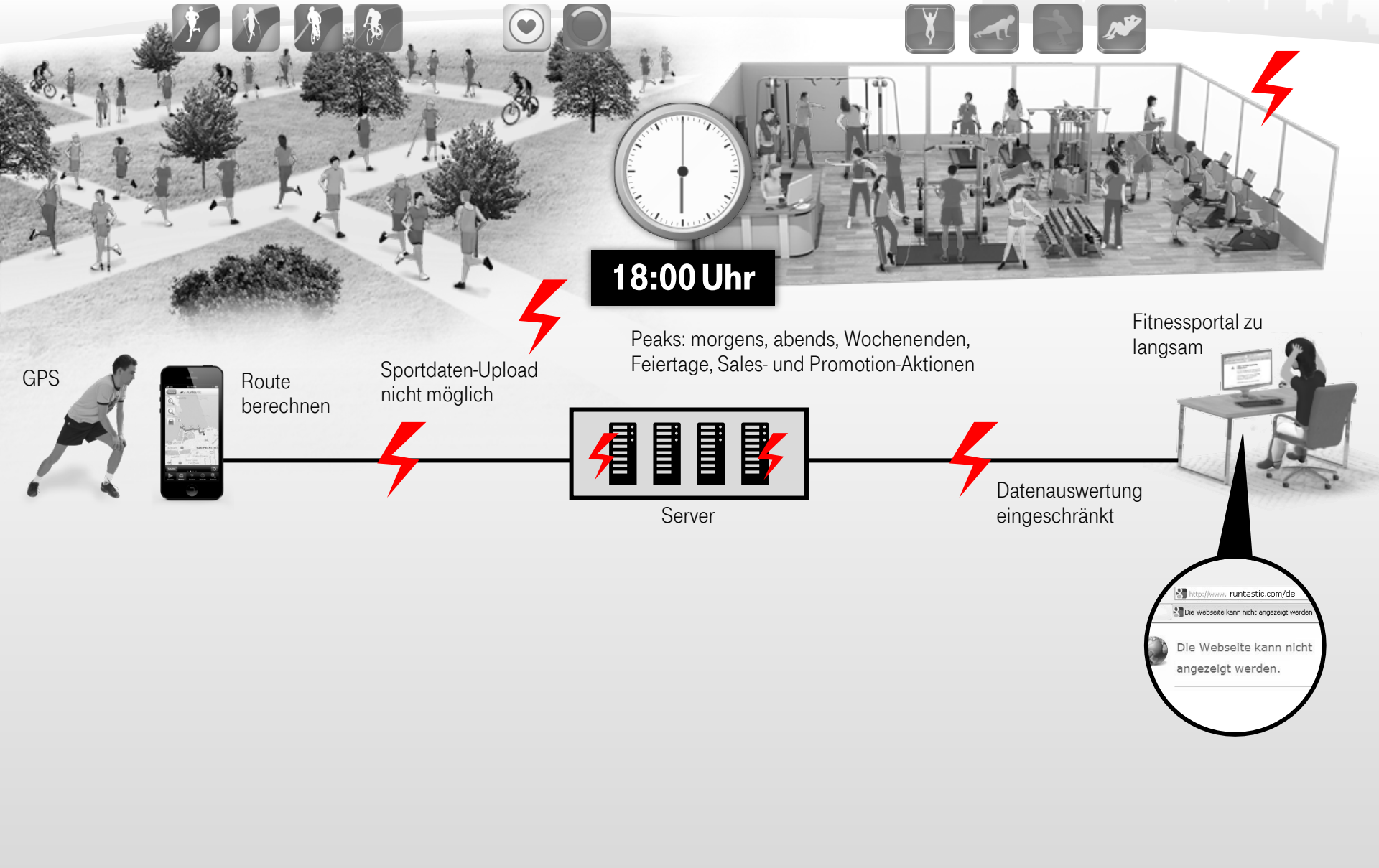
- 26 Mio. registrierte User (z.B. Tempo, Kalorienverbrauch, Puls & Strecken zu verwalten)
- Trainingspläne
- 60 Mio.+ Downloads p.a.
- Social Media Integration: 400.000 Facebook Fans

Umgebung mit hohen Auslastungsschwankungen

➡ TRAININGSDATEN SICHER VERARBEITEN UND 60 MIO. USERN BEREITSTELLEN: **ZERO DISTANCE**

EIGENE INFRASTRUKTUR STÖßT AN GRENZEN

Z.B. BEI BEVORZUGTEN TRAININGSZEITEN & PROMOTIONAKTIONEN



FLEXIBILER RESSOURCENBEZUG FÜR MODERNE UNTERNEHMEN

DIE vCLOUD WÄCHST MIT DEN USER ZAHLEN

99,9 % Verfügbarkeit
der IT-Ressourcen auch bei Peaks

ZERO DISTANCE
Information – Customers – Employees

40 % Einsparpotenzial
Durch Abrechnung nach Verbrauch (CAPEX->OPEX). Kein Vorhalten von Ressourcen für Spitzenlasten

Zufriedene Kunden
dank schneller Datenübertragung und verlässlichen Services

Hohe Flexibilität
durch schnelle Ressourcen-Erweiterung für Spitzenlast und Wachstum

Sichere Datenübertragung
durch providerredundante Internetzugänge

INNOVATIONSWORKSHOP 2014
SECURITY LÖSUNGEN

Juli 2013

T · · Systems ·

UNTERSCHIEDLICHE TYPEN VON ANGREIFERN

ABER: GLEICHE METHODEN BEI DIVERGIERENDEN ZIELEN

	Klassische „Hacker“	Technische Betrüger	organisierte Kriminalität	Hacktivisten	Nachrichten-dienste
MOTIVATION	▪ Ruhm und Ehre ▪ Zeigen was man kann ▪ Spiel und Spaß	▪ Finanziell basiert	▪ Betrug ▪ Erpressung ▪ Geldwäsche	▪ Politische Meinungsäußerung	▪ Spionage ▪ Sabotage
RESSOURCEN	▪ zumeist Einzelpersonen	▪ zumeist Einzelpersonen oder Kleingruppen	▪ gut organisierte Gruppen ▪ hohe Arbeitsteiligkeit ▪ Weltweit Verteilt ▪ hohe Finanzmittel	▪ gut organisierte Gruppen ▪ hohe Arbeitsteiligkeit ▪ weltweite Verteilung	▪ staatlich gelenkt ▪ extrem hohe Finanzmittel verfügbar
BEISPIELE	▪ Verunstalten von Internetseiten ▪ Meldungen von Schwachstellen in Webseiten an die Presse ▪ ...	▪ Kreditkartenbetrug ▪ Manipulation von Bankautomaten ▪ „Zeus“ Trojaner ▪ ...	▪ Phishing-E-Mails ▪ DDoS auf Onlineshops / Onlinewetten ▪ SPAM ▪ ...	▪ DDoS gegen Banken, die Wikileaks Konten gesperrt hatten ▪ Anonymous Angriffe auf Unternehmen ▪ ...	▪ Stuxnet (Iranisches Atomprogramm) ▪ Red October (Regierungen im Ostblock) ▪ ...

Primärfokus der Sicherheitsarbeit

Sekundärfokus /

TRANSPARENZ DURCH ANGRIFFSRADAR IN ECHTZEIT
WWW.SICHERHEITSTACHO.EU

TRANSPARENZ | KOMPETENZ | EINFACHHEIT | KOOPERATION

RUND 180 HONEYPOTS IM NETZ DER DEUTSCHEN TELEKOM

WACHSTUM: INTERNATIONALER ROLLOUT

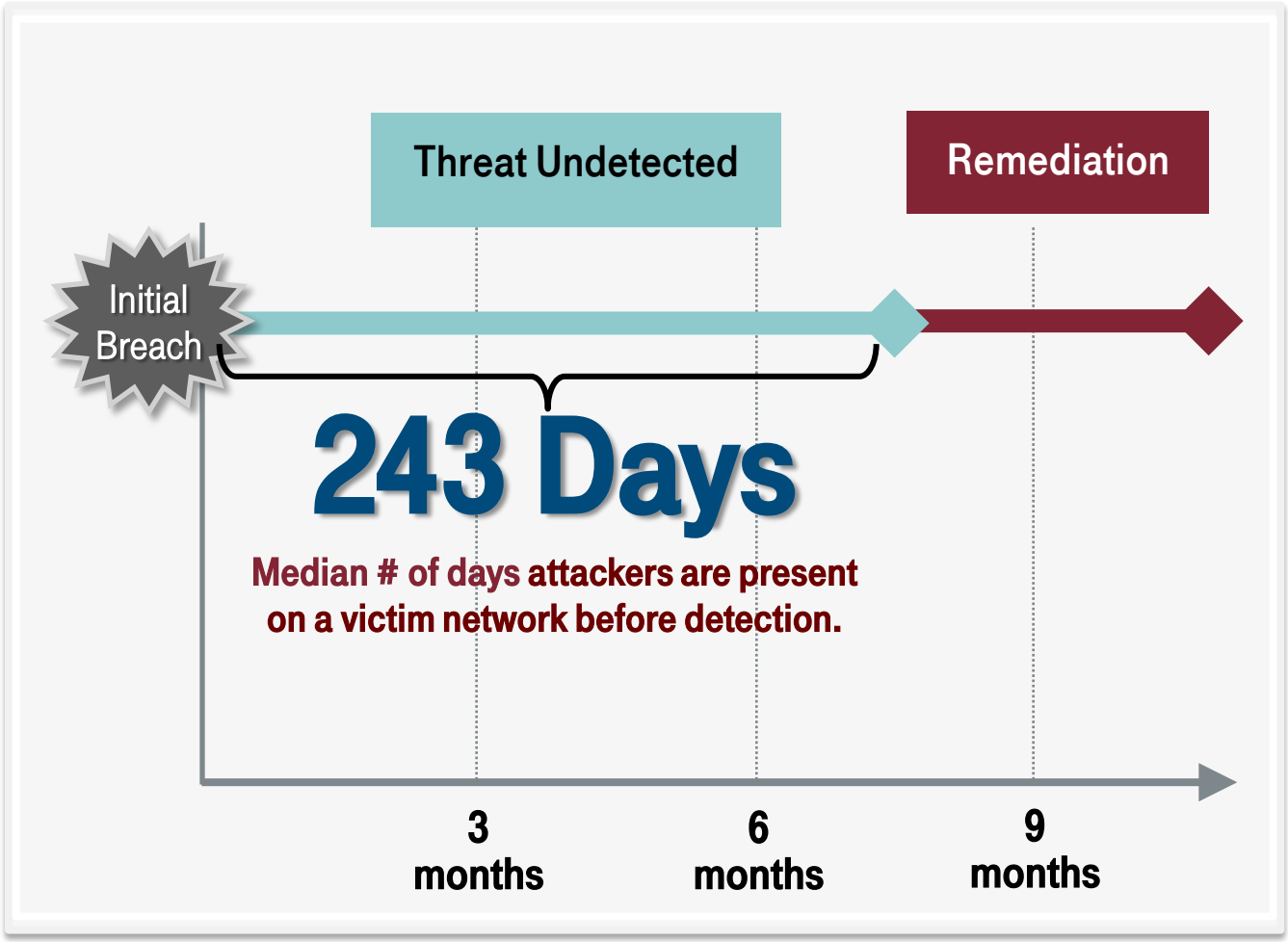
ENTDECKUNG VON BIS ZU 800.000 ANGRIFFEN TÄGLICH

ECHTZEIT ÜBERBLICK DER ANGRIFFE, TOP 15 NACH LÄNDERN UND VERTEILUNG DER ANGRIFFSZIELE

ALS KUNDENINDIVIDUELLES SENSORNETZWERK UMSETZBAR

T · · Systems ·

ANGRIFFE WERDEN PROFESSIONELLER



63%

of Companies Learned They Were Breached from an External Entity

100%

of Victims Had Up-To-Date Anti-Virus Signatures

Source: Mandiant M-Trends 2013

STRUCTURE OF A MULTI-FLOW APT ATTACK

Exploit Server

1 Embedded Exploit Alters Endpoint

T · · Systems ·

STRUCTURE OF A MULTI-FLOW APT ATTACK

Exploit Server

Callback Server

1 Embedded Exploit Alters Endpoint

2 Callback

T · · Systems ·

STRUCTURE OF A MULTI-FLOW APT ATTACK

Exploit Server

Callback Server

Encrypted Malware

1 Embedded Exploit Alters Endpoint

2 Callback

3 Encrypted malware downloads

T · · Systems ·

STRUCTURE OF A MULTI-FLOW APT ATTACK

T · · Systems ·

DETECTION: STATE OF THE ART

ANALYSE

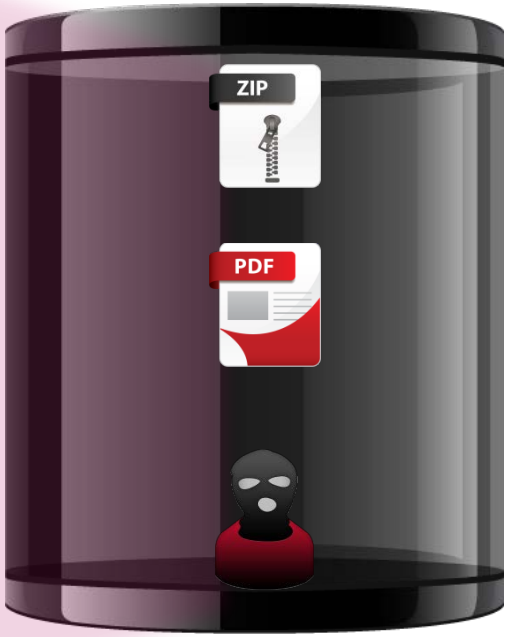
Network

Email

Mobile

Files

DETONATION IN GESCHÜTZER UMGEBUNG



FireEye™

Virtual Machine-Based Model of Detection

Purpose-Built for Security

Hardened Hypervisor

Skalierbar

Portabel

T · · Systems ·

PROFESSIONALISIERUNG DER ANGREIFER ERFORDERT ZUSÄTZLICHE KOMPETENZEN

PRÄVENTION

MINIMIERUNG VON ANGRIFFSFLÄCHEN

- Firewall, Mail Security
- Penetration Testing
- DDoS Mitigation strategies

ERKENNUNG

PROTOKOLLLIERUNG, ÜBERWACHUNG & SIMULATION

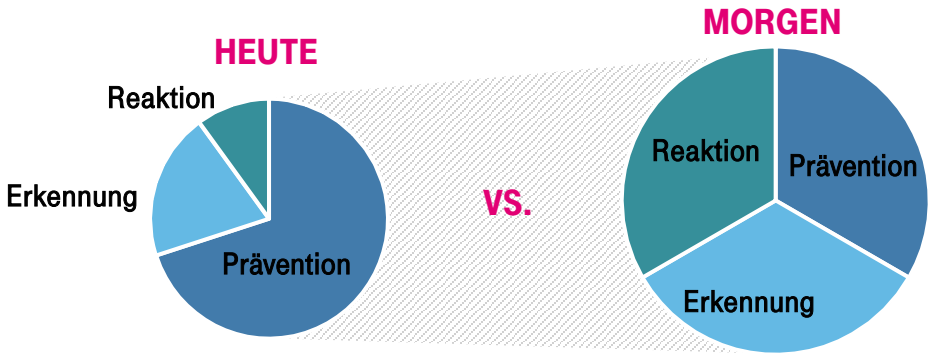
- Monitoring von Attacken
- Anomalie Entdeckung
- Security Operations Center

REAKTION

STRUKTURIERTE ABWEHRMASSNAHMEN

- Reaktionen auf Angriffe
- Forensische Analysen
- Computer Emergency Response Team (CERT)

Ressourcenverteilung für ICT Security



ADVANCED CYBER DEFENCE BY TELEKOM
KOMPETENZ FÜR UNSERE KUNDEN

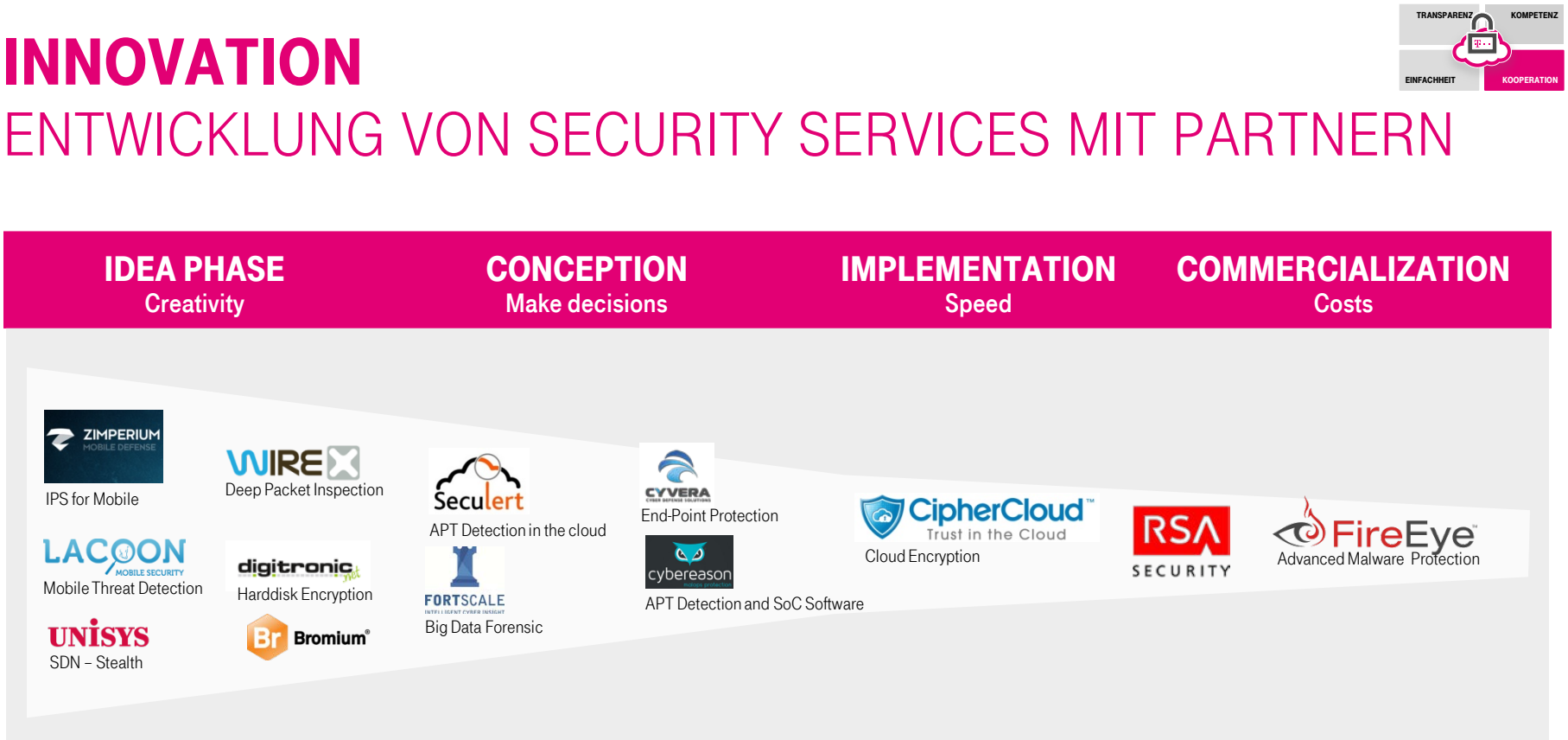
GEBÜNDELTE KOMPETENZEN

- Erstmalig Ende zu Ende Sicherheit durch Analyse von IT und Netzwerk
- Zielt auf die Entdeckung von gezielten Angriffen
- Schnellere Gegenmaßnahmen möglich
- Echtzeit Lagebild
- „Menschliche“ Experten für mehr Sicherheit

T · · Systems ·

INNOVATION

ENTWICKLUNG VON SECURITY SERVICES MIT PARTNERN



SCOUTING

- Scouting in Tel-Aviv, Silicon Valley, Europa
- Early /Late-Stage Startups

CYBER SECURITY BOOTCAMP

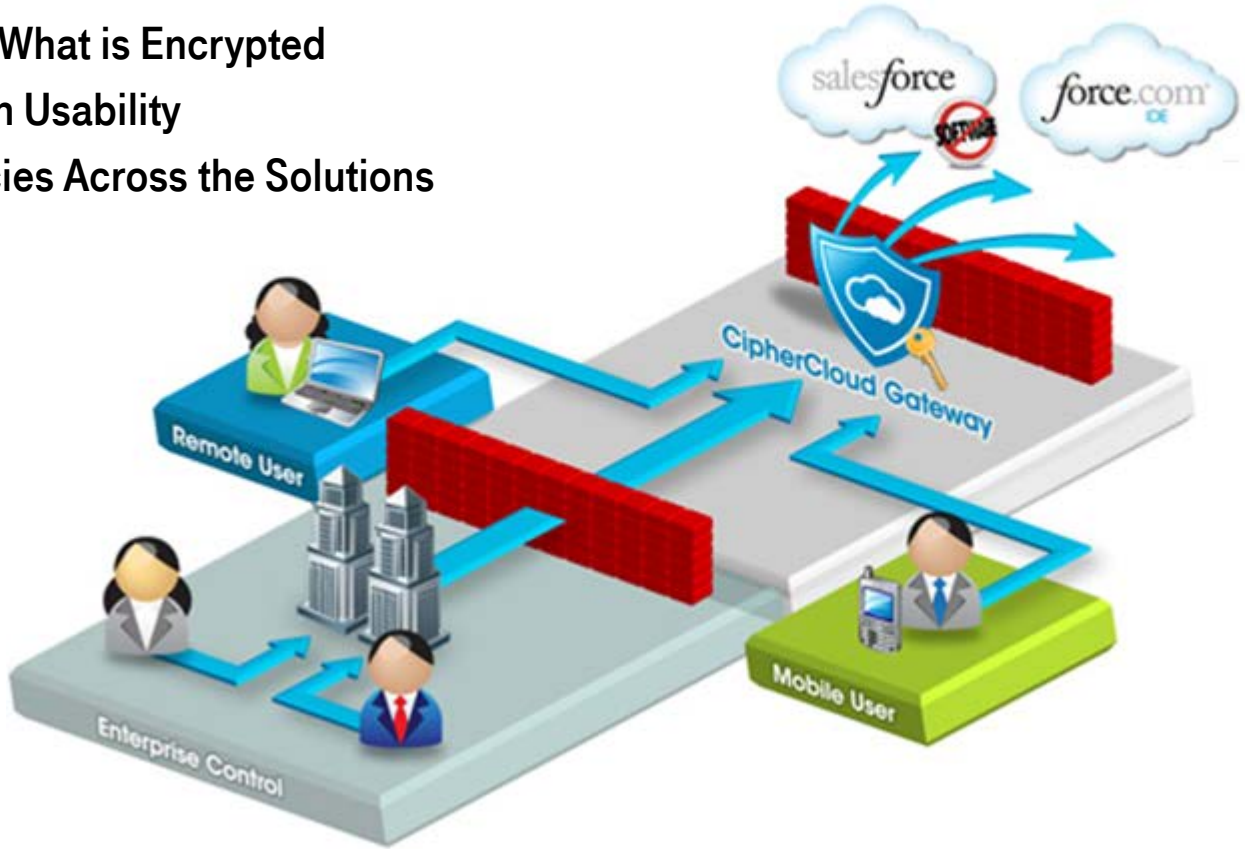
- Cyber Security Bootcamps im September in Berlin
- Ziel: Generierung und Identifizierung neuer distruptiver Ansätze für neue Produkte

T · · Systems ·

THE CIPHERCLOUD GATEWAY

Encrypt Sensitive Data in Real-time, before it's sent to the Cloud and decrypts the Data as the User requests it

- Encryption Preserves Data Formats & Operations
- You Choose What is Encrypted
- No Impact on Usability
- Unified Policies Across the Solutions



T · · Systems ·

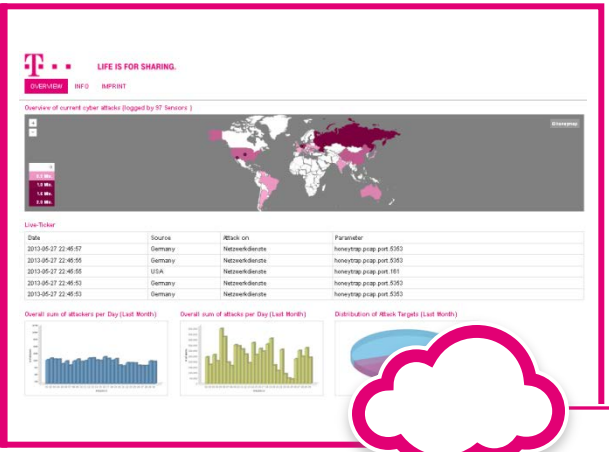
FRAGEN?

THOMAS SCHMITT
T-SCHMITT@T-SYSTEMS.COM

BACKUP

DIE WACHSENDE BEDROHUNGSLAGE ERFORDERT IN ZUKUNFT NEUE KONZEPTE FÜR SECURITY

TRANS-PARENZ



KOMPETENZ

CYBER SECURITY @ DEUTSCHE TELEKOM

EINFACHHEIT

INNOVATION