Cybersecurity als Architektur verstehen

Wie Hybrid IT und Zero Trust echte Integration treiben

Arnd Gille

Technischer Leiter Cybersecurity Sales
Cisco Germany
agille@cisco.com

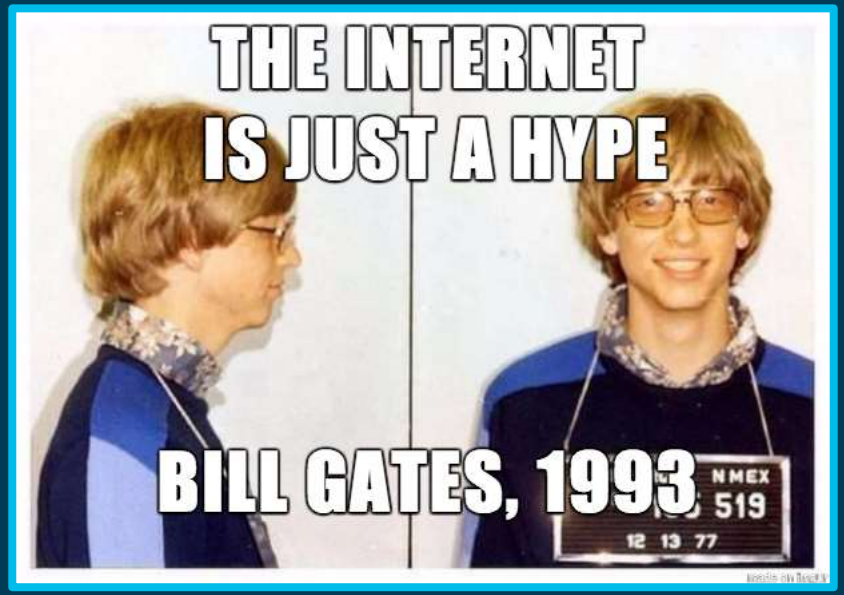
8. Oktober 2019

it-sa 2035: Die Zukunft von Cybersecurity
Built-in Security – Security by Design

- Erhält Informationen über Identities und Policies *(“Wer darf was?”, Whitelist Model)*
- Teilt Informationen über Kommunikation und Verhalten von Usern und Prozessen
- Zugriff auf zentrale Threat Intelligence ermöglicht vollständigen Kontext
- Unerlaubtes wird unterbunden *(Enforcement)*
- *Every app, every instance (physical, container, etc.)*

Anfänge der Cyber-Sicherheit

- Netzwerksegmentierung für bis dahin flache Netzwerkstrukturen
- Klar definierter Perimeter
- Dateibasierte Sicherheitsverfahren (z.B. Antivirus)



Zwischen den Welten: Cybersecurity 2019

Security wird keinesfalls automatisch in jede Applikation integriert

Einfachheit der IT-Strukturen der 90er-Jahre ist Vergangenheit

Bedrohung durch Cyber-Angriffe ist allgegenwärtig

Angriffsfläche von IT zunehmend größer

Cybersecurity 2019 – Alles ist hybrid!
Classic vs. Hybrid IT

Kreidler Flory

- 3 Gears Manual
- Slow
- Limited reach
- No Automation
- Lot´s of individual tuning

Jaguar XE

- Automatic Gearbox
- Semi-Automated Driving
- Leased
- Integration with other Devices

1970

2019

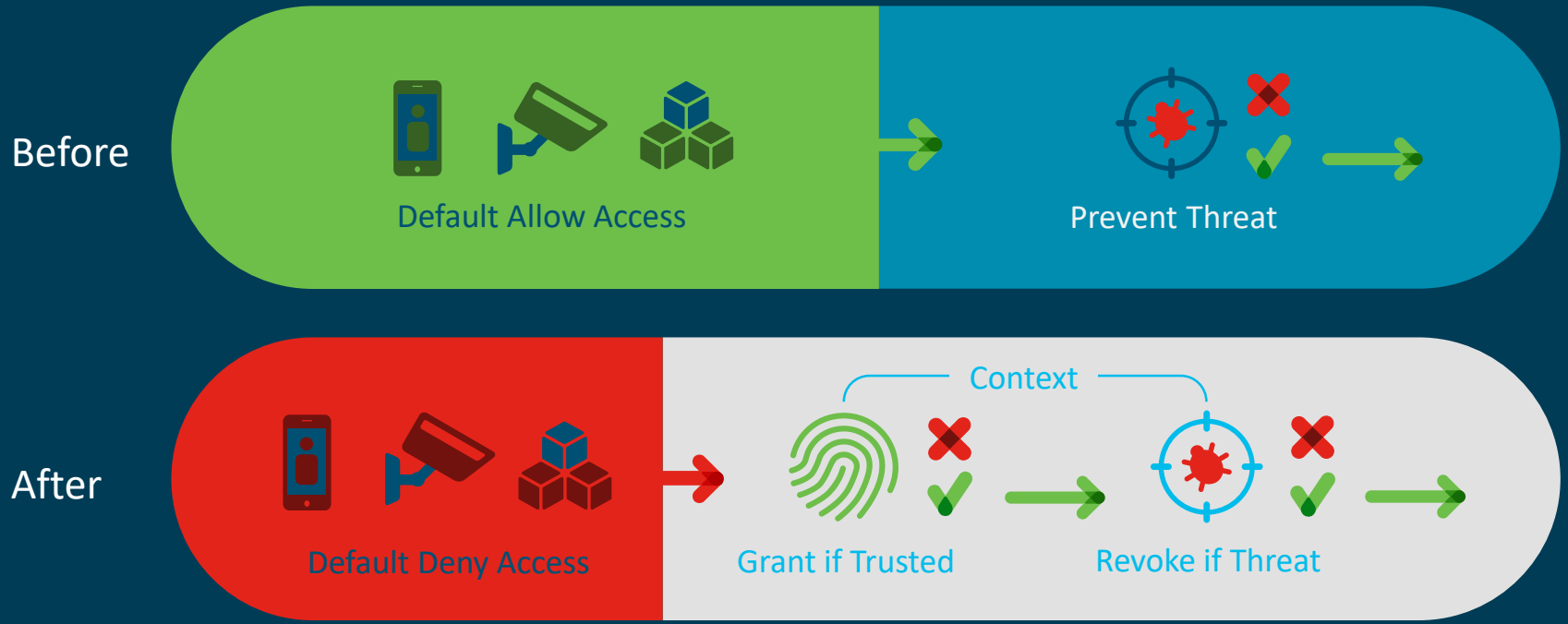
Classic IT

- Manual
- Slow
- On-Premises
- Lot´s of individual tuning

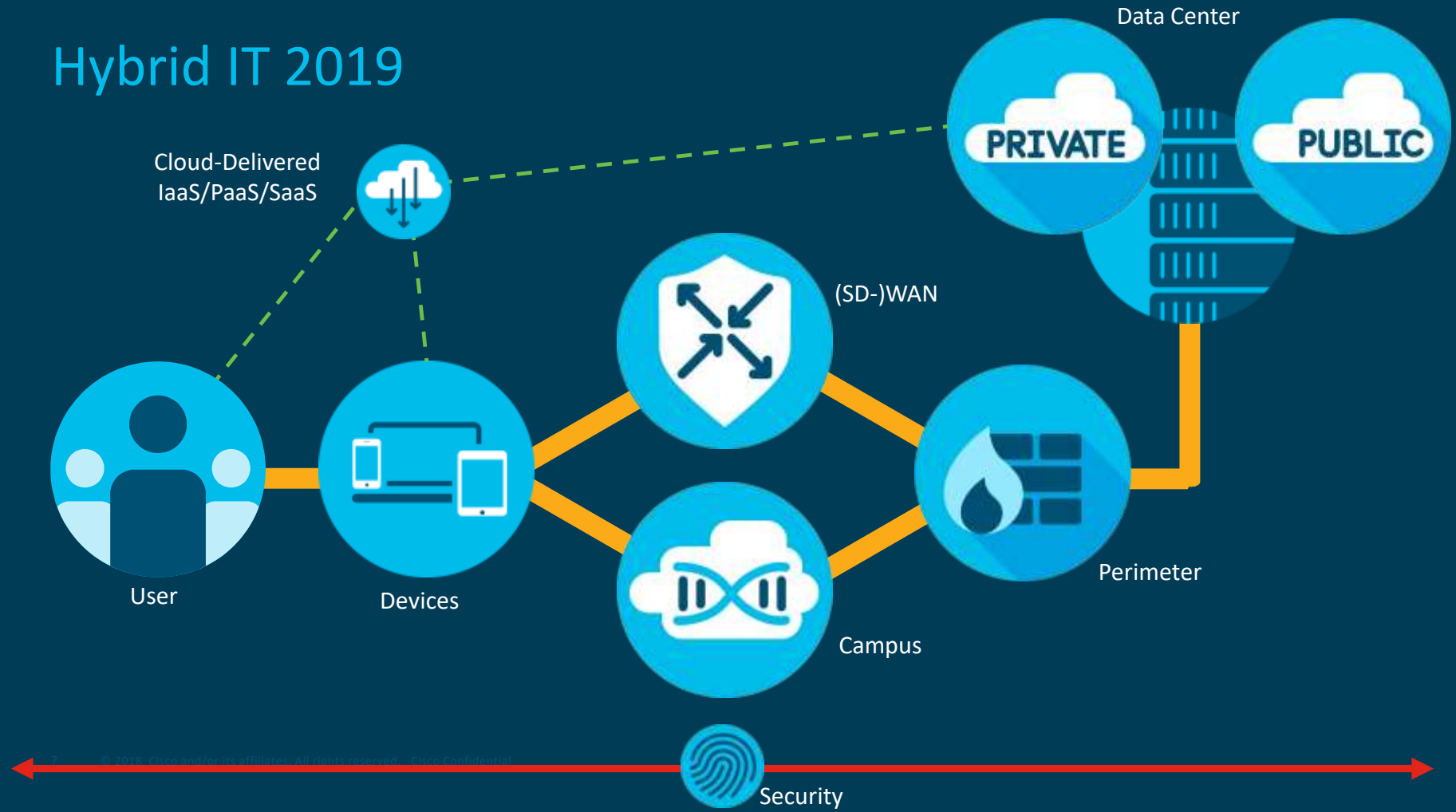
Hybrid IT

- Automated
- Integrations
- Services can run everywhere
- Users can work everywhere
- Standardized

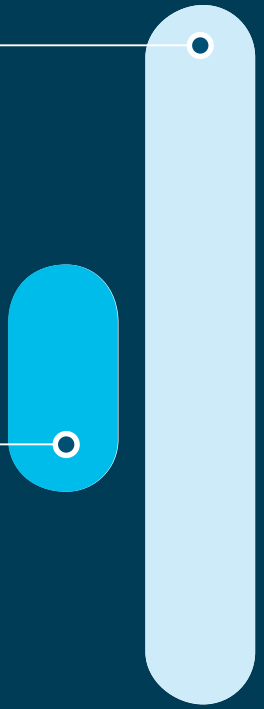
Zero Trust: Potentielle Angriffe durch jeden jederzeit



Hybrid IT 2019



Cybersecurity 2019



Hybrid IT

On-prem/cloud in beliebiger Kombination

Zero Trust

Potentielle Angriffe durch jeden jederzeit

Security is not built-in!

Cybersecurity muss auf die existierende IT aufgesetzt werden!

Komplexität

Alle Trends führen zu immer komplexeren Herausforderungen

Die “Integrationsfalle” der IT-Sicherheit

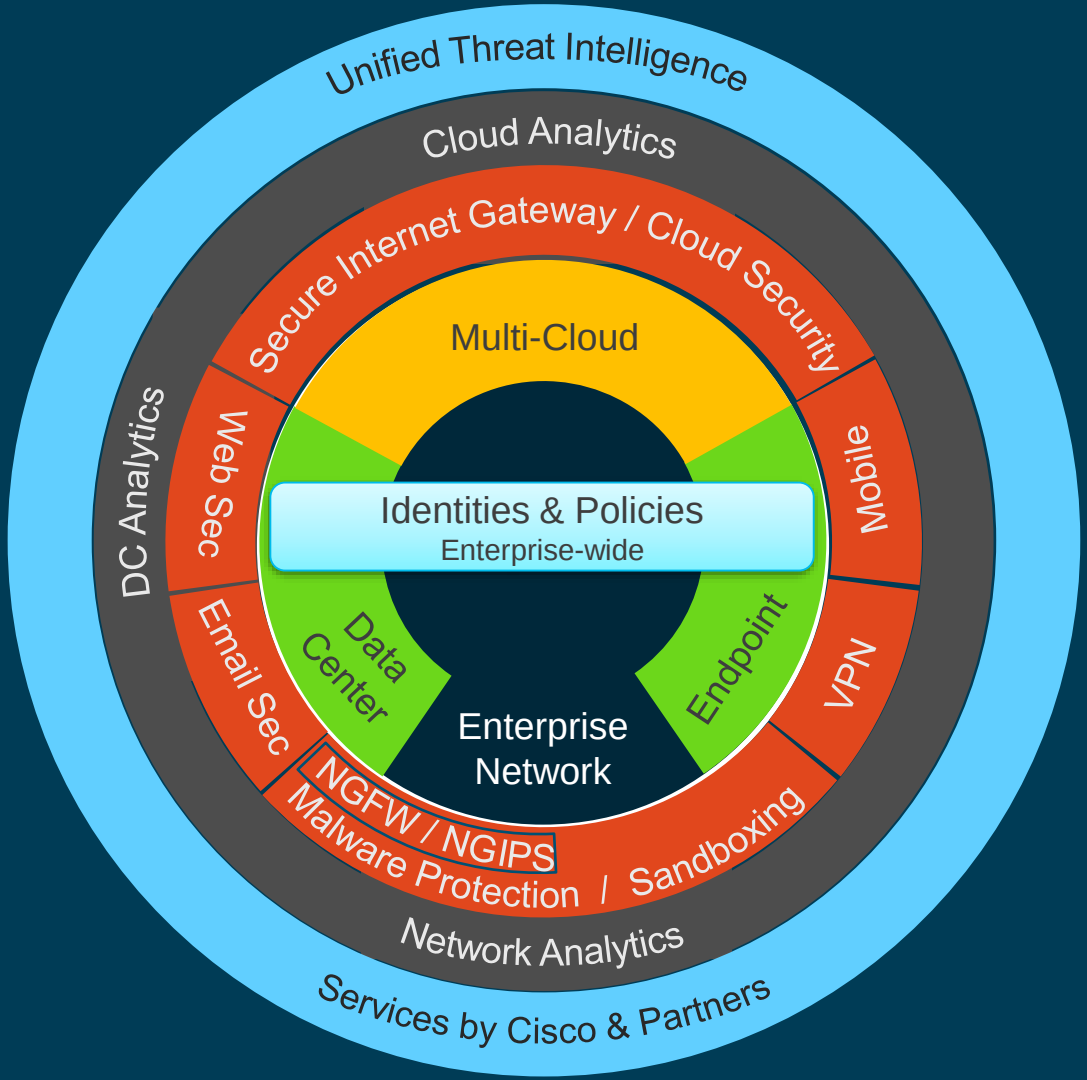
- Integrierte Security-Architektur als Antwort auf die steigende Komplexität
- *Best-of-Breed* ist nicht unwichtig, verliert aber an Bedeutung
- **Problem: Alle Hersteller positionieren sich damit, wie kann ich Unterschiede erkennen?**

Integration ≠ Integration

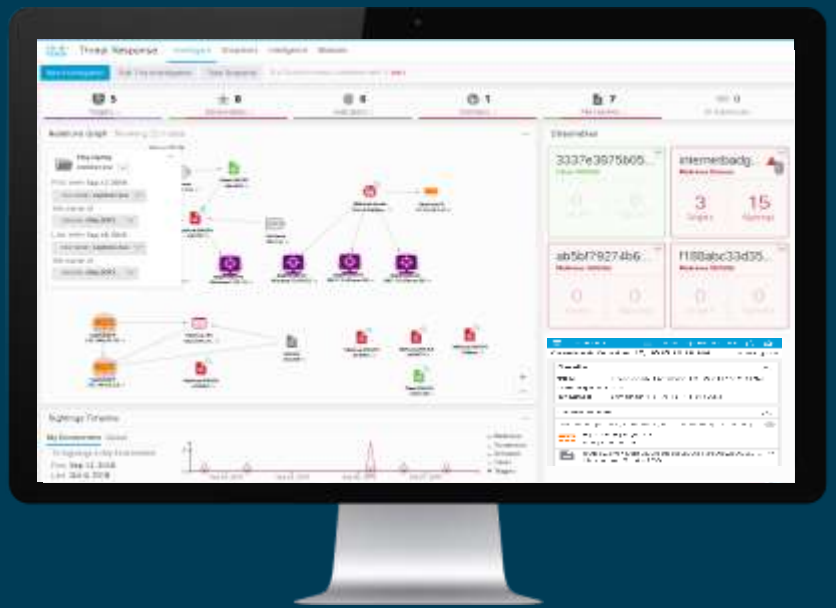
Stufen der Integration

Integration nicht einmalig, sondern andauernd!

Integrated Security Architecture



Integration am *Front-End*: Cisco Threat Response (CTR)



- Effektives SOC-Werkzeug für
  - *Detection*
  - *Investigation*
  - *Remediation*
- Kontext aus allen Cisco Security-Lösungen
- Keine zusätzlichen Kosten

Zusammenfassung

Besuchen Sie uns: Halle 10.0 – Stand 420


CISCO