The Importance of Human-Centric Security in the age of Digital Transformation

Christian Patrascu

Sr. Director, Sales
CEU – Central Eastern Europe

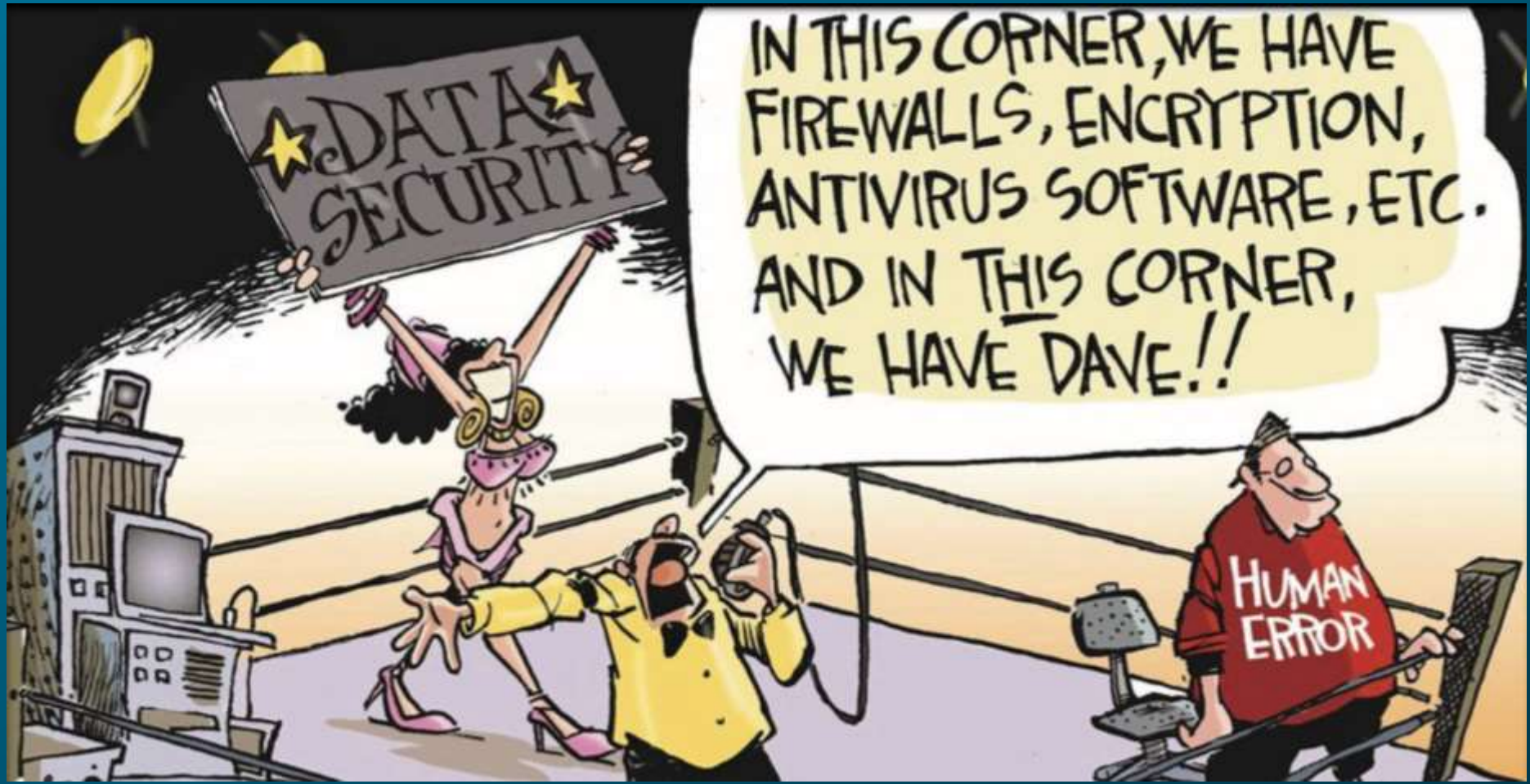
FORCEPOINT

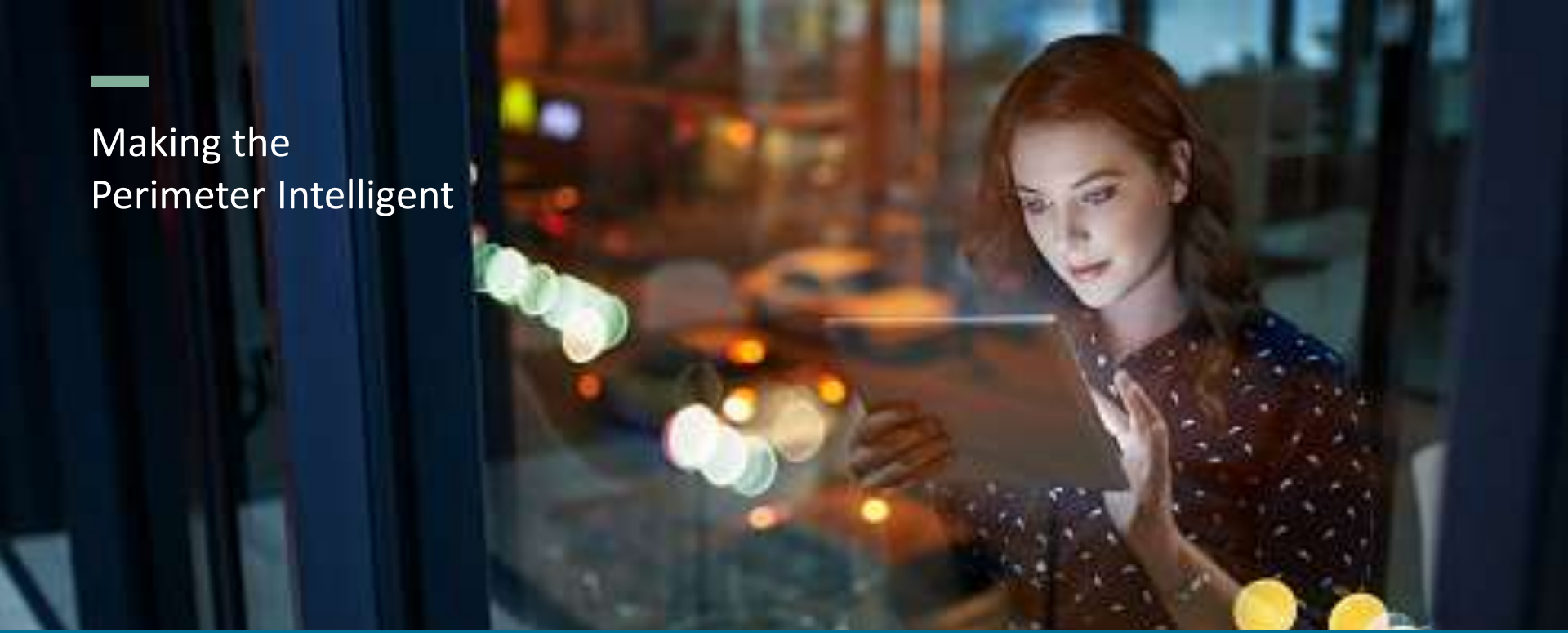
Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

Forcepoint: the Company

- Wir als Forcepoint revolutionieren die Sicherheitsbranche
  - Durch die Bereitstellung eines einzigartigen, auf den Menschen ausgerichteten Cybersicherheitsansatzes (HCS)
  - Mit dem Ziel, Benutzer und Daten zu schützen
  - Reibungslos und skalierbar für Cloud, On-Premises und Hybrid

Warum revolutioneren wir die Sicherheitsbranche durch den menschenzentrien Ansatz (HCS) ?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR



Making the Perimeter Intelligent

Wie machen wir ‘menschenzentrierte Sicherheit’?

Machen wir einen Schritt zurück: Was ist die Idee der Perimetersicherheit?

Sie bauen eine Mauer um das, was Sie schützen möchten

Outcome

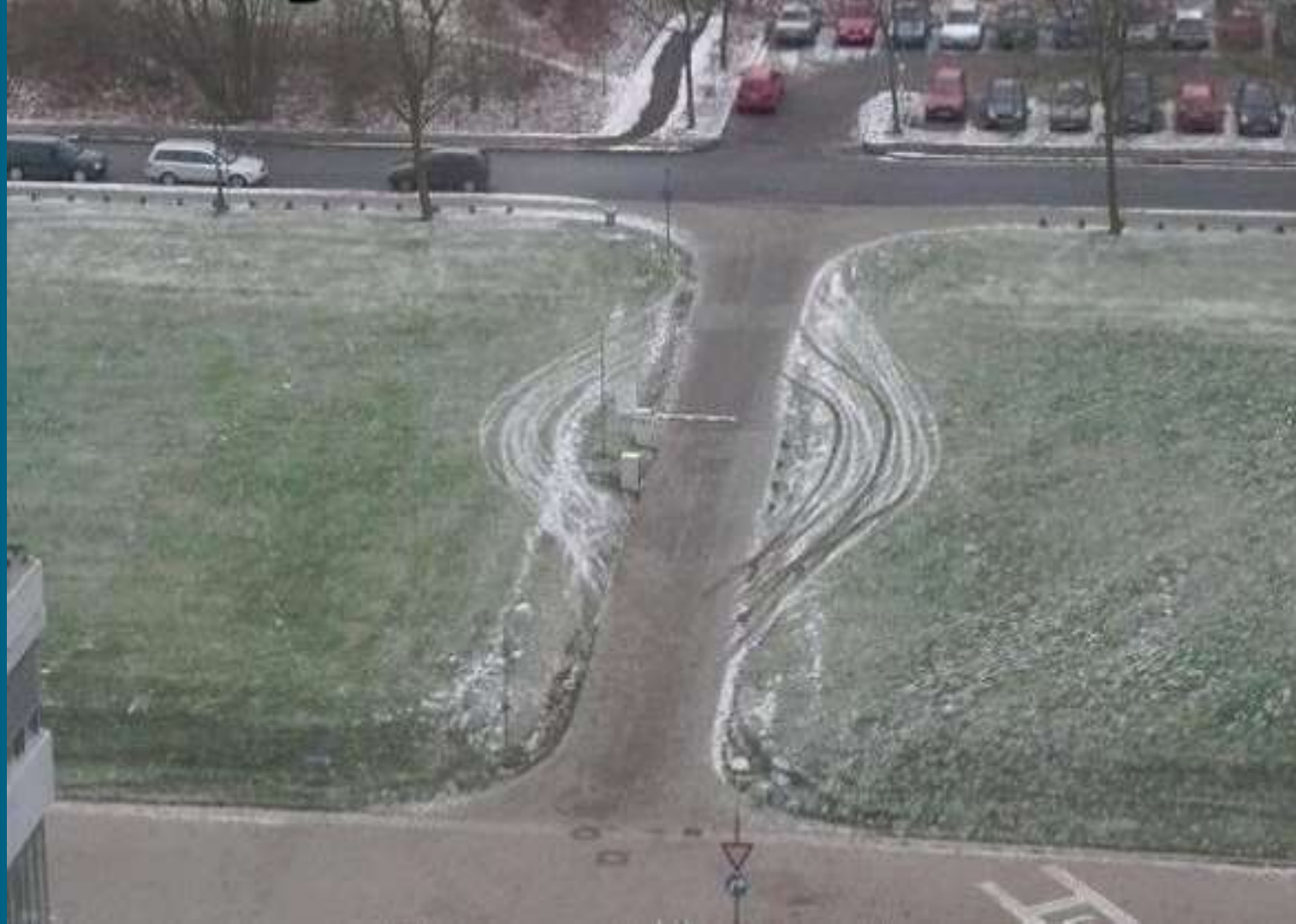
Building a Wall Around What You Want to Protect

Case 1

Welche Möglichkeiten gibt es, diese Mauer zu bauen?

- Die Mauer ist nicht hoch genug

Outcome



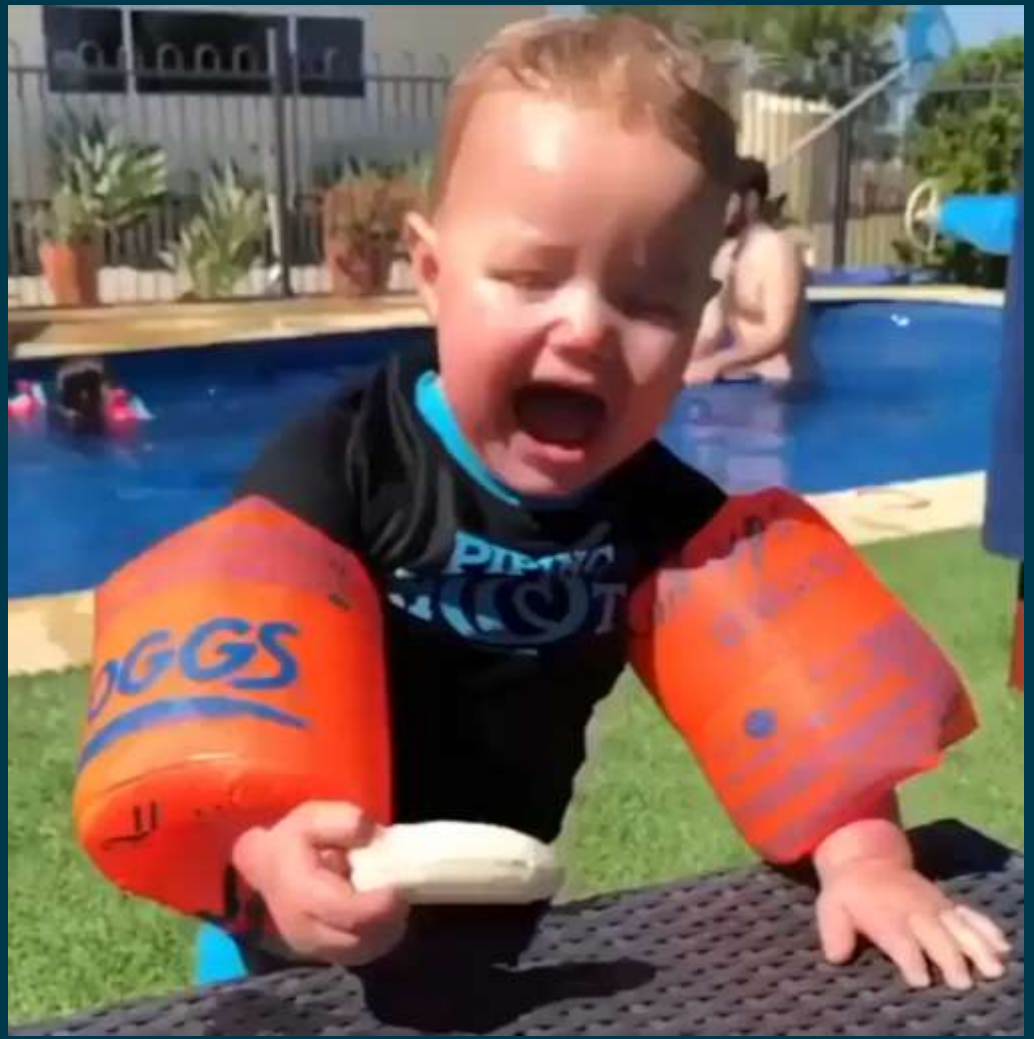
Building a Wall Around What You Want to Protect

Case 2

Welche Möglichkeiten gibt es, diese Mauer zu bauen?

- Die Mauer ist zu hoch

Outcome



Building a Wall Around What You Want to Protect

Case 3

Welche Möglichkeiten gibt es, diese Mauer zu bauen?

- Die Mauer ist genau richtig!

Outcome

Die Mauer ist genau richtig!
Warum reicht der Perimeter immer noch nicht ?

- Single Point of Failure: Verzögerung, Skalierbarkeit usw.
- Perimeter braucht eine Vorlage, nach der gesucht werden muss.
- Was vor und nach dem Perimeter passiert: Es wird nicht analysiert!
- Volles Vertrauen hinter dem Perimeter. Nicht jeder ist ein Engel!
  - Böswillige Insider und versehentliche Bedrohung
- Daten fließen wie schlängelnde Flüsse von on Prem in die Cloud
  - Neues Paradigma – Gibt es den Perimter noch ?

Case 3

Was ist die Lösung jetzt?

Ein anderer Ansatz zur Cybersicherheit

Bereichern des Perimeters durch zwei Dimensionen: Daten und Benutzer

Ziel ist es, den Perimeter intelligent zu machen! Verstehen was vor und hinter dem Perimeter passiert

Wie? Verhaltensanalysen auf Benutzerebene - nicht am Perimeter

Warte ! Ist das nicht Big Brother ?

Compromising Privacy?

Nein - Wir müssen die Wahrnehmung und Sichtweise ändern :

Nein - Wir müssen die Wahrnehmung und Sichtweise ändern :

- Compliance (Ziel: Vertrauen der Aktionäre) baut auf Kontrollframeworks auf
  - Es geht nicht darum, den Benutzer zu kontrollieren
  - Hier geht es darum, das Risiko zu kontrollieren

- Dies ist Ihre Haftung basierend auf den Compliance-Rahmenframeworks

Putting this all together

Wir haben bereits die Idee von ZERO Trust. Dies ist die erste Inkarnation in 3 Schritten :

Step 1

Verhalten vor und nach dem Perimeter analysieren. Zero Trust

Step 2

Dynamische Rückkopplung des Risikos in die Policies. Keine statischen Regeln!

Step 3

Treffen einer Entscheidung auf der Grundlage des Kontexts, nicht nur der allgemeinen ‘Black or White Policy’

Mithilfe von Verhaltensanalysen; Den Perimeter intelligent machen

Use Case 1: Risikoadaptive dynamische Nutzung

Einkaufsleiter (Sepp)
Nürnberg, Deutschland

Monday
January 21 @ 10am

Arbeit waehrend Urlaub

+ Additional Context

Risk Score: 30

Risk-Adaptive Protection

No enforcement action

Thursday
January 22 @ 1pm

Remote login und Anlegen eines neuen Benutzers

+ Additional Context

Risk Score: 50

Risk-Adaptive Protection

Video capture activated

Evidence available for investigation later

Wednesday
January 23 @ 9pm

Copy file to staging area: Lieferanteninformationen

+ Additional Context

Risk Score: 80

Risk-Adaptive Protection

Copy allowed but file encrypted

No corporate data at risk

Saturday
January 24 @ 9pm

Bulk copy to USB drive Einkaufskonditionen & Vertraege

+ Additional Context

Risk Score: 95

Risk-Adaptive Protection

Action is blocked & account is locked

Avoided $10M breach and proof that Henry is the attacker is available

In den letzten 7 Jahren wurden 1 Billion US-Dollar für Cybersicherheit ausgegeben, mit 95% Erfolg: für die Angreifer

46% geben an, dass sie Angreifer nicht hindern können, in interne Netzwerke einzudringen.

100% der CIOs glauben, dass ein erfolgreicher Phishing-Angriff in den nächsten 12 Monaten eintreten wird.

Die Zahl der Sicherheitsvorfälle in Unternehmen hat sich trotz einer Erhöhung der Budgets um 9% gegenüber dem Vorjahr um 26% erhöht.

Source: CyberArk Global Advanced Threat Landscape Report 2018

Sources: Verizon 2018 Data Breach Investigations Report.

Follow us!

Forcepoint

Forcepoint

@Forcepointsec

@Forcepointlabs

Forcepoint