Check Point
SOFTWARE TECHNOLOGIES LTD

CPX 360°

YOU CAN GET BURNED WHEN IT'S CLOUDY

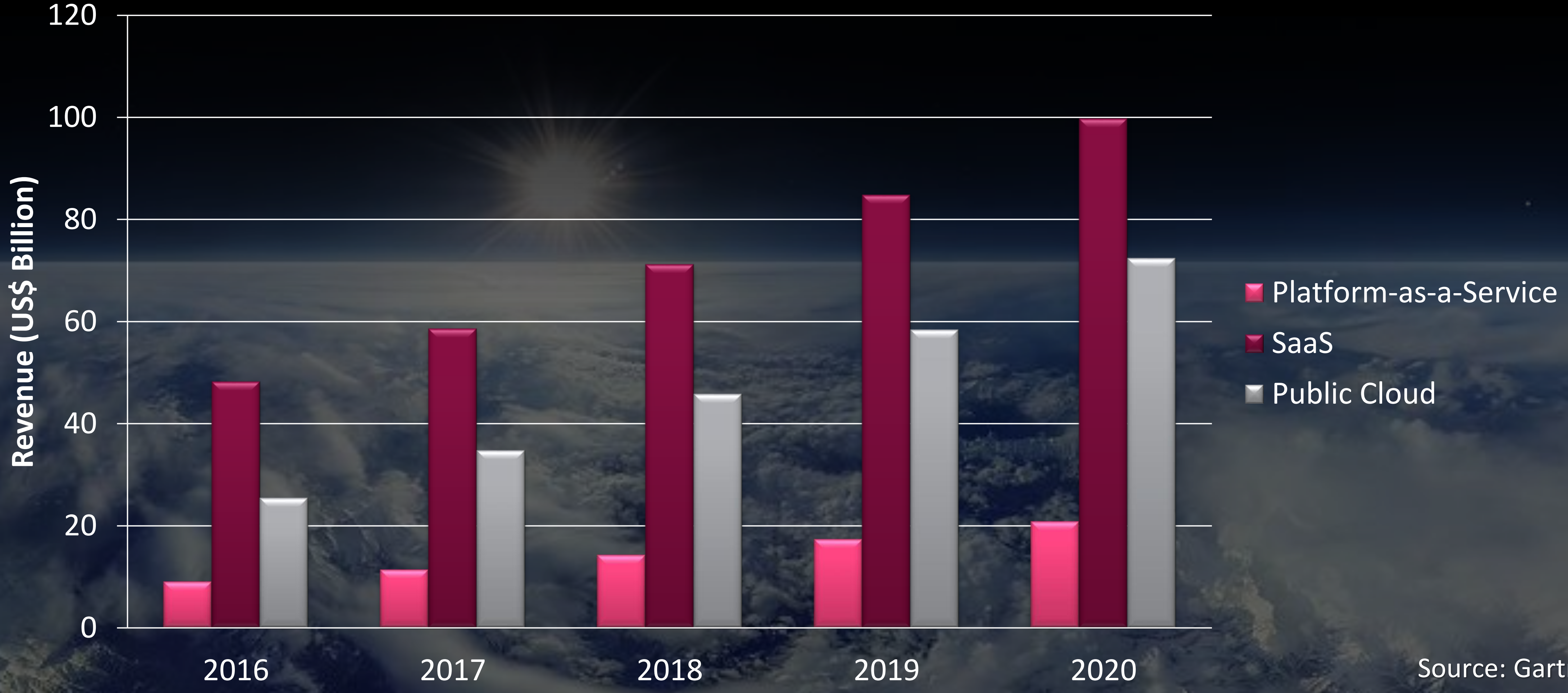
Peter Sandkuijl| Head of Security Solutions, Engineering, Europe

WELCOME TO THE FUTURE OF CYBER SECURITY

“I think that you will all agree that ***we are living in most interesting times.*** *I never remember myself a time in which our history was so full, in which day by day brought us new objects of interest, and, let me say also,* ***new objects for anxiety.****”*

Joseph Chamberlain, Bristol, England, 1898

NEW OBJECTS OF INTEREST



Worldwide Cloud Services Revenue Forecast

Source: Gartner

NEW OBJECTS OF ANXIETY

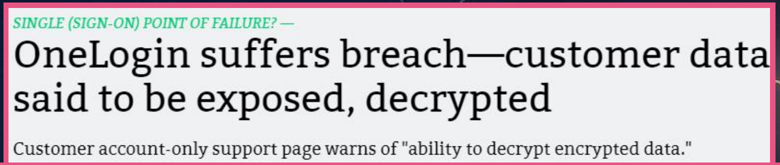
Networks are more Inter-Connected

&

Threats are more Sophisticated and Automated

CURRENT STATE OF CLOUD SECURITY

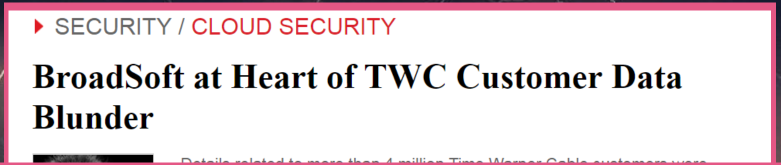
NOT EVERY CLOUD HAS A SILVER LINING



SINGLE (SIGN-ON) POINT OF FAILURE? —

OneLogin suffers breach—customer data said to be exposed, decrypted

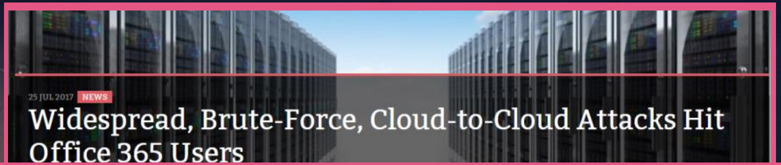
Customer account-only support page warns of "ability to decrypt encrypted data."



SECURITY / CLOUD SECURITY

BroadSoft at Heart of TWC Customer Data Blunder

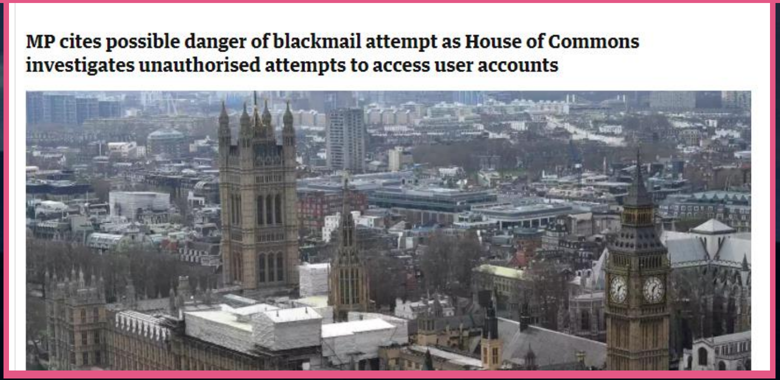
Details related to more than 4 million Time Warner Cable customers were



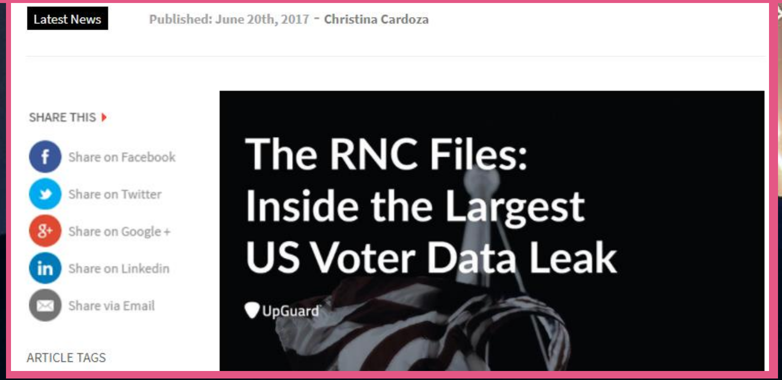
25 JUL 2017 NEWS

Widespread, Brute-Force, Cloud-to-Cloud Attacks Hit Office 365 Users

And the hits just keep on coming . . .

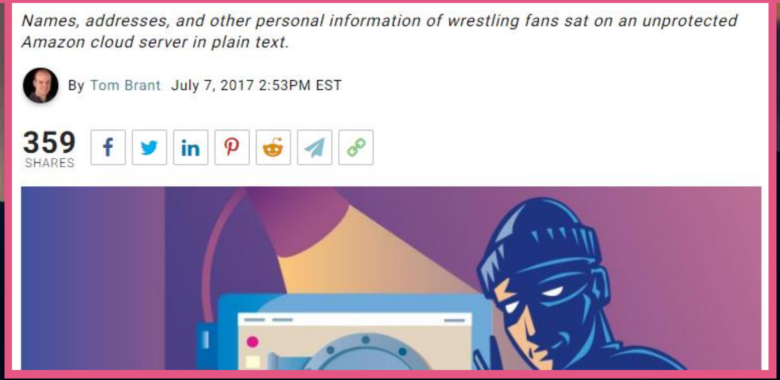


MP cites possible danger of blackmail attempt as House of Commons investigates unauthorised attempts to access user accounts



Latest News

Published: June 20th, 2017 - Christina Cardoza

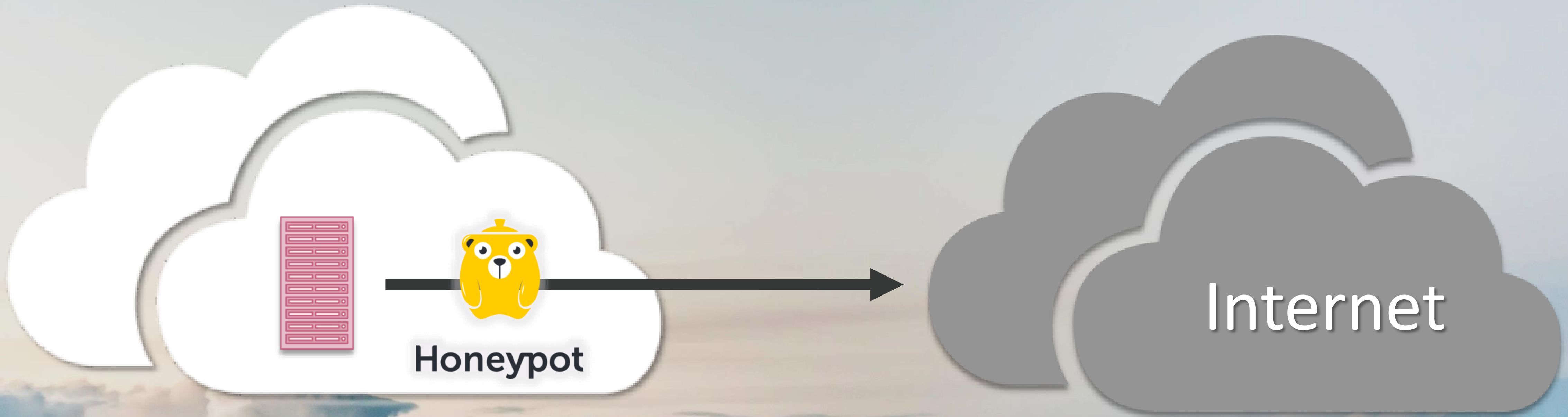


Names, addresses, and other personal information of wrestling fans sat on an unprotected Amazon cloud server in plain text.

By Tom Brant July 7, 2017 2:53PM EST

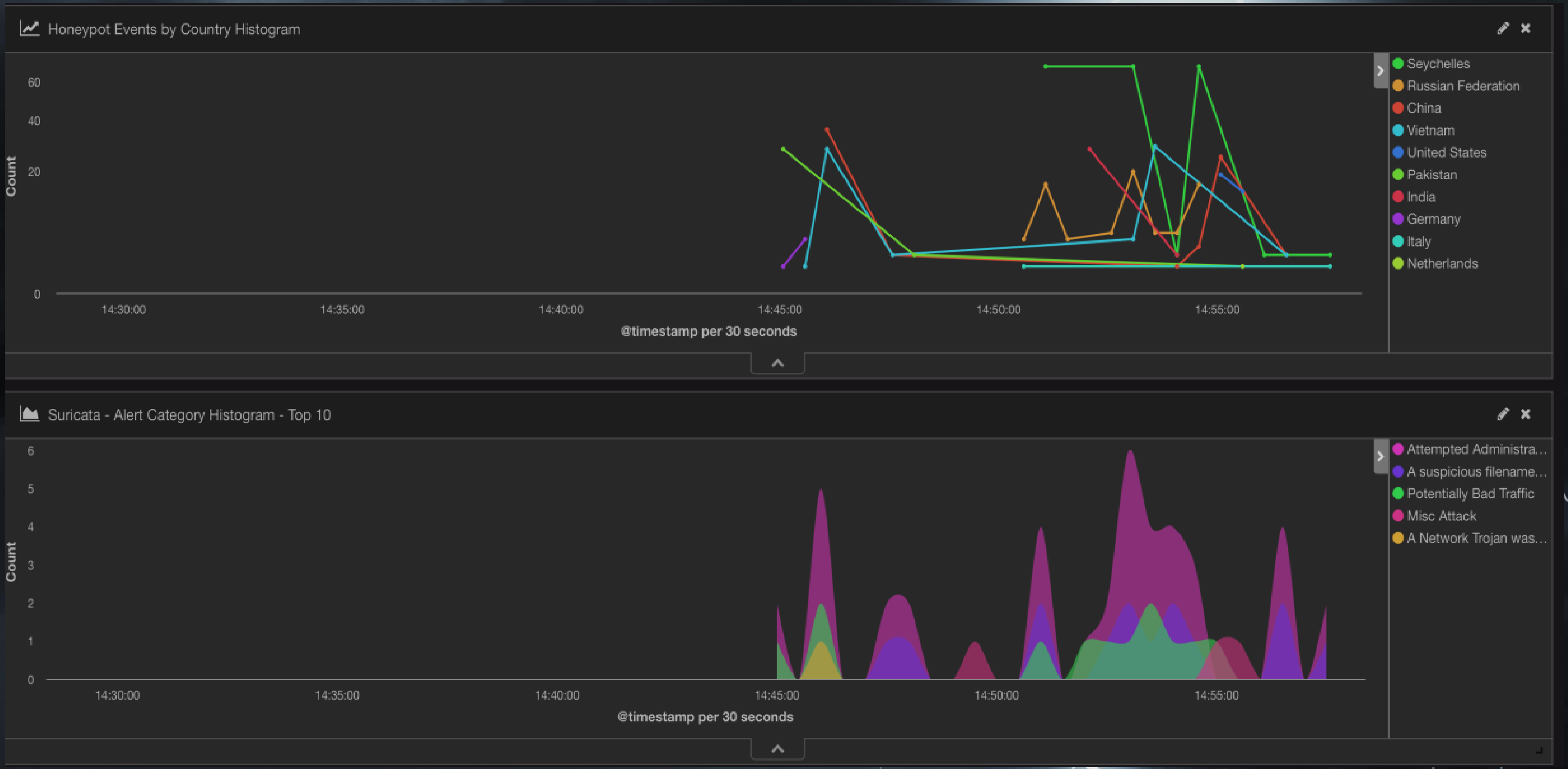
HOW EXPOSED ARE WE *REALLY* IN THE CLOUD?

OUR CLOUD ENVIRONMENT



WITHIN THE FIRST 15 MINUTES

Houston we have a problem . . .



CLOUD = SHARED RESPONSIBILITY

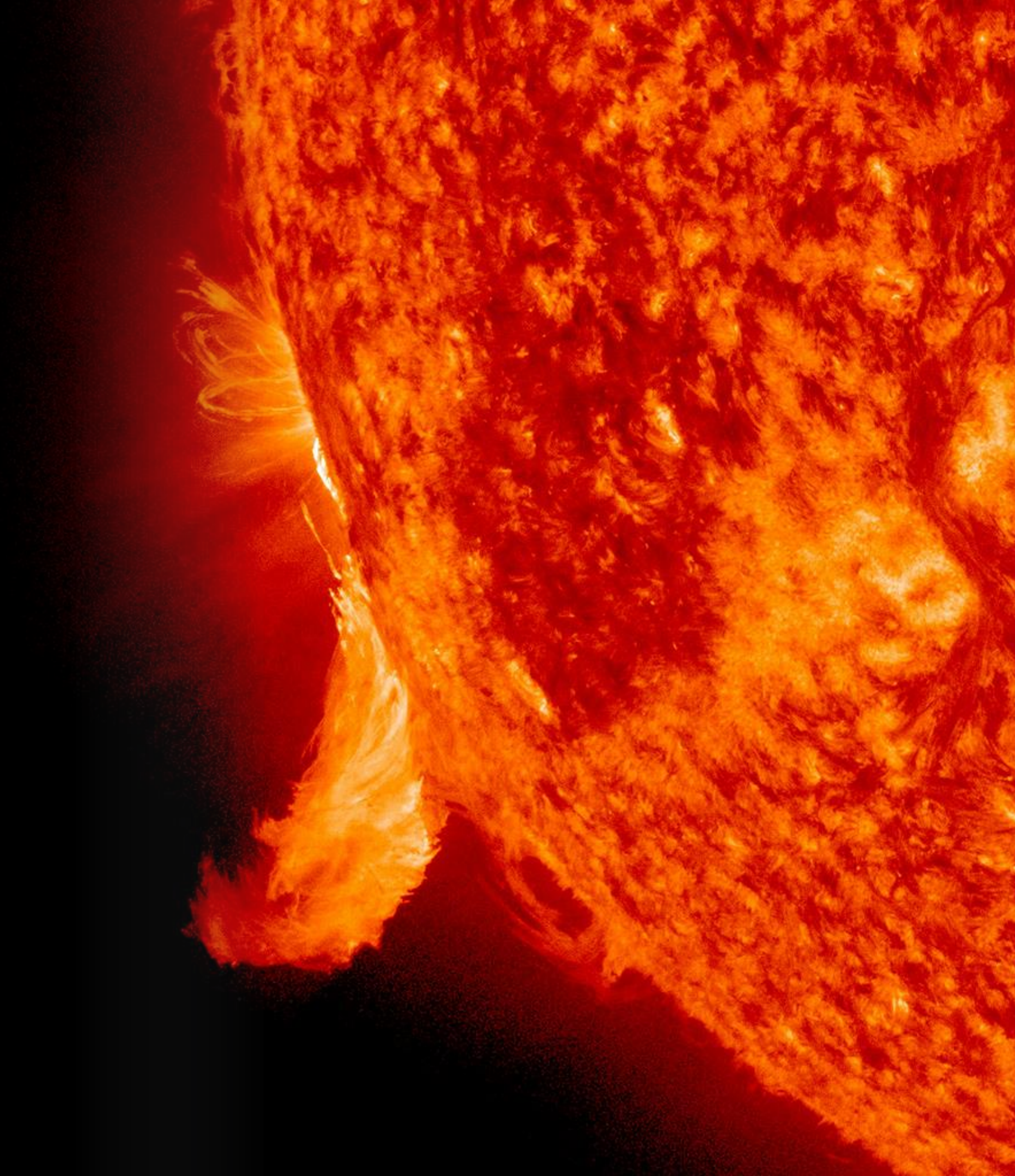
Cloud Provider responsible for security ***of*** the cloud

Customer responsible for security ***in*** the cloud

CLOUD NETWORKS ARE VULNERABLE

- Shared responsibility is unclear
- Increasingly sophisticated and automated attacks
- Lateral spread of threats
- Account hijacking
- Inconsistent tools for visibility, management and reporting

IT’S TIME FOR SOME SUN BLOCK



CLOUD SECURITY RECOMMENDATIONS

1. COMPREHENSIVE PROTECTIONS

Prevent attacks against cloud applications, data and workloads

2. EASE OF OPERATIONS

One-click deployment, auto-provisioning templates

3. CONSUME & CONTRIBUTE CONTEXT

Adjust to dynamic nature of cloud

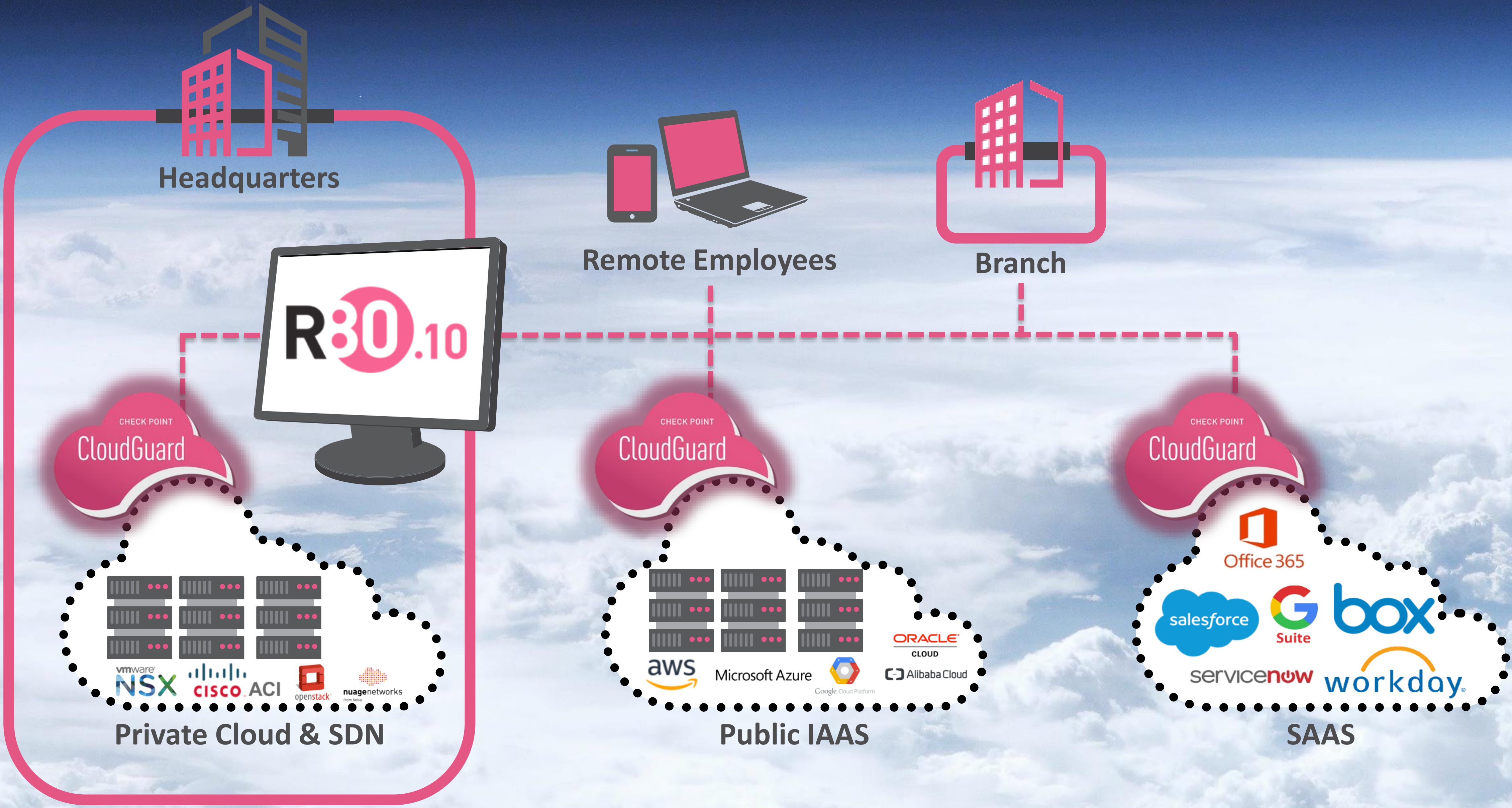
4. CENTRALIZED MANAGEMENT

Single pane-of-glass experience across all clouds

INTRODUCING CHECK POINT CLOUDGUARD

PROTECTING ANY CLOUD, ANY SERVICE, ANYWHERE

COMPREHENSIVE SECURITY ARCHITECTURE



THANK YOU

WELCOME TO THE FUTURE OF CYBER SECURITY

CPX360°

SUMMARY

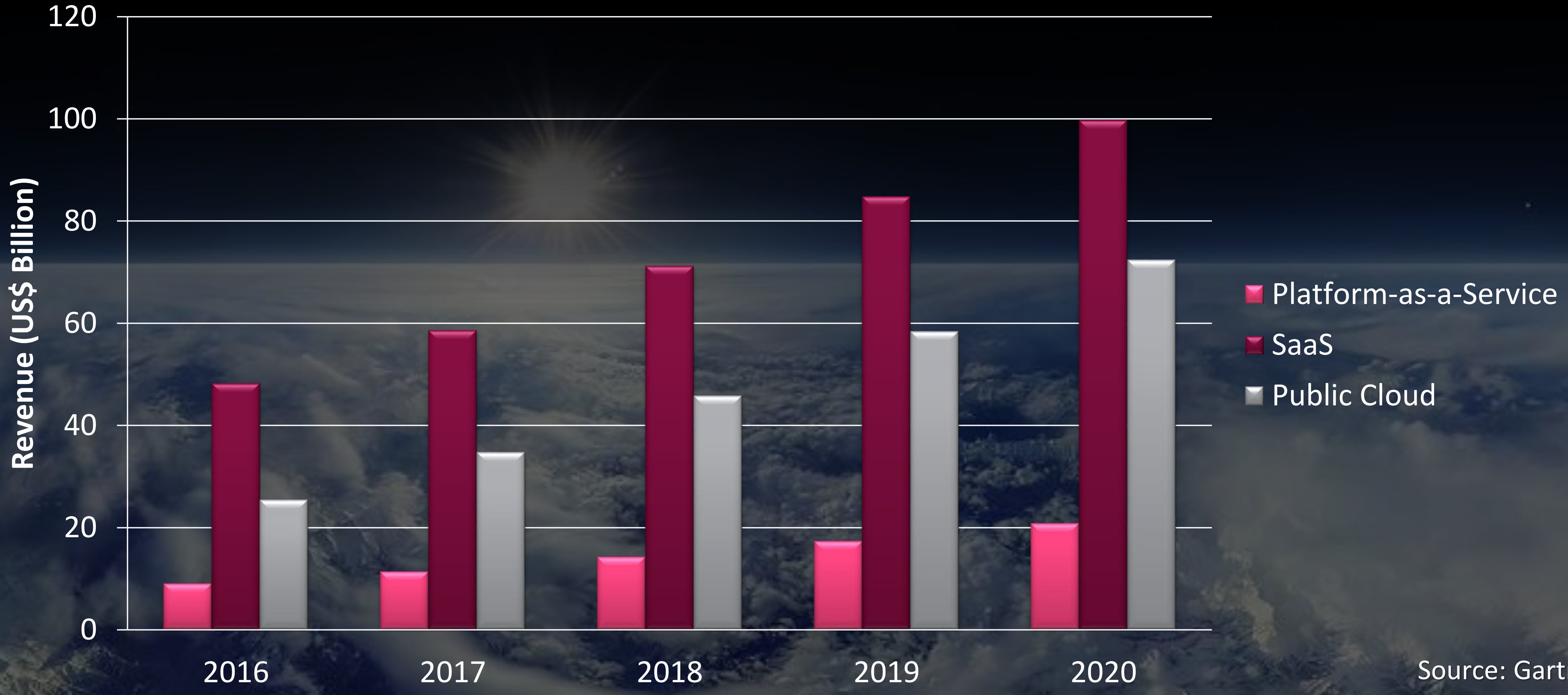
- Back-up Slides

“We are in a cloud security transition period in which focus is shifting from the provider to the customer. Enterprises are learning that huge amounts of time spent trying to figure out if any particular cloud service provider is ‘secure’ or not has virtually no payback.”

Jay Heiser, VP and Cloud Security Lead, Gartner, Inc. JAN 5, 2018

https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html - 5 January, 2018

RISING TIDE OF CLOUD INTEREST



Worldwide Cloud Services Revenue Forecast

Source: Gartner

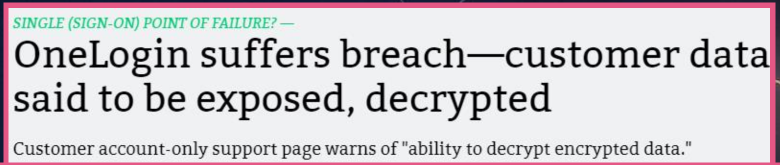
NEW SOURCES OF ANXIETY

Networks are more Cloud-based and Inter-Connected

Threats are more Sophisticated and Automated

CURRENT STATE OF CLOUD SECURITY

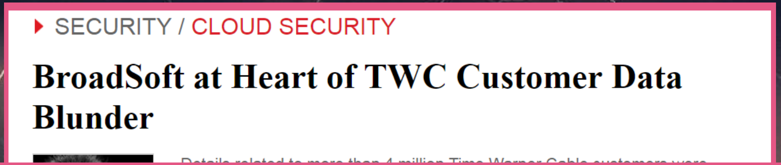
NOT EVERY CLOUD HAS A SILVER LINING



SINGLE (SIGN-ON) POINT OF FAILURE? —

OneLogin suffers breach—customer data said to be exposed, decrypted

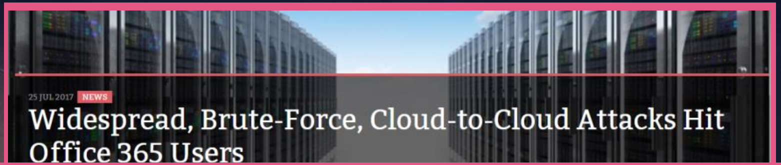
Customer account-only support page warns of "ability to decrypt encrypted data."



SECURITY / CLOUD SECURITY

BroadSoft at Heart of TWC Customer Data Blunder

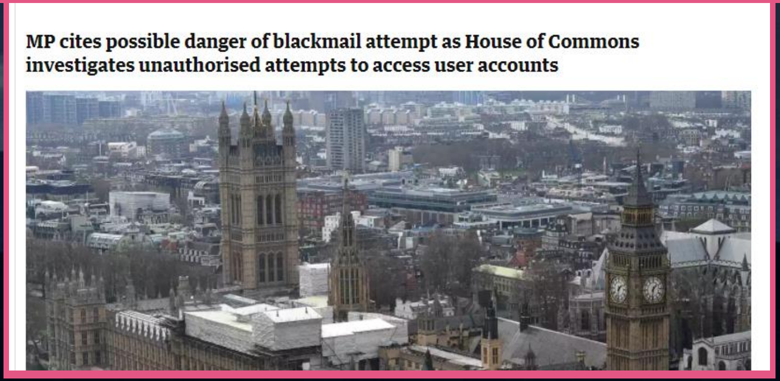
Details related to more than 4 million Time Warner Cable customers were



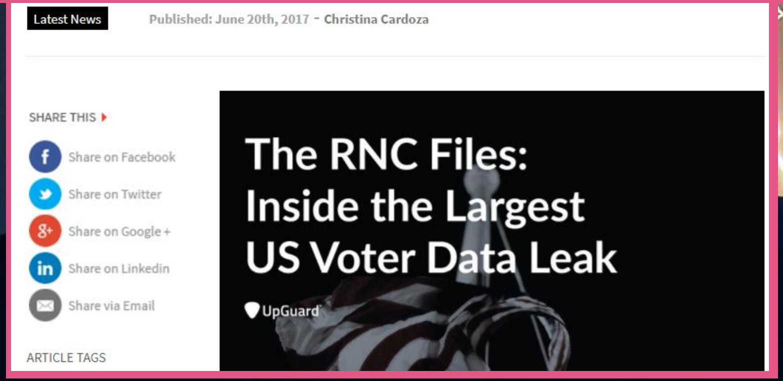
25 JUL 2017 NEWS

Widespread, Brute-Force, Cloud-to-Cloud Attacks Hit Office 365 Users

And the hits just keep on coming . . .



MP cites possible danger of blackmail attempt as House of Commons investigates unauthorised attempts to access user accounts



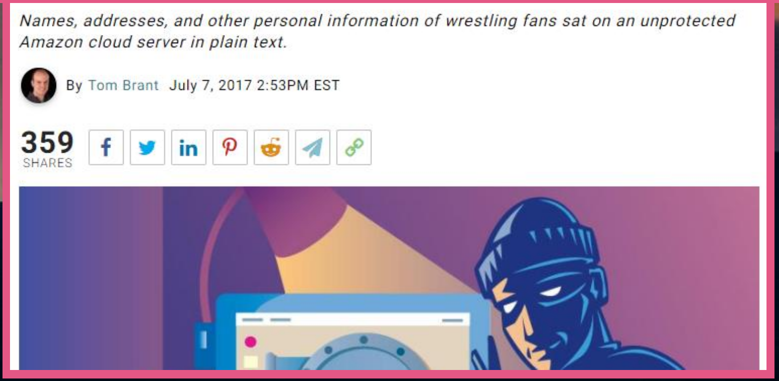
Latest News

Published: June 20th, 2017 - Christina Cardoza

SHARE THIS

- Share on Facebook
- Share on Twitter
- Share on Google+
- Share on Linkedin
- Share via Email

ARTICLE TAGS



Names, addresses, and other personal information of wrestling fans sat on an unprotected Amazon cloud server in plain text.

By Tom Brant July 7, 2017 2:53PM EST

359 SHARES

Cloud Security Case 1

- Power Co – Ransomeware attack
  - Reverse engineering: Big hurry to allow 3rd party vendor access
    - RDP server direct connected to Internet – portscan against 3389 (Open RDP): Brute Force
      - Logging into RDP – matter of days, guess credentials: Letmein123
    - Attacker gains access – RDP on an open ESXi server; no segmentation
      - Minicats – dump memory and hashes of credentials; stage ransomware on all servers
  - Back-ups would take 3-5 days to restore, so paid the bad guys; assumed they would be in the clear, came back 4 days later and got hit again . . . Doubled ransome, so customer decided to rebuild infrastructure = segmentation, rebuild servers, VPN with authentication in RDP
  - Issue – flat network with NO segmentation / micro-segmentation so now way to stop lateral spread of an attack; no way of knowing is malware was even on the malware or how the servers were communicating
  - Security controls need to be logically inserted into the network; segementation, visibility and control

Cloud Security - Case 2

- Issues – hurry to adopt cloud but not doing due diligence
- Retailer –small private instances of infrastructure in public cloud but still needed mySQL server access / database back to on-prem
  - Didn't want site-to-site VPN so opened firewall rules for direct access from cloud to corp prem
    - Attacker found vulnerability –SQL injection attack in app– on cloud, broke into server and profiled all connections, found mySQL connection back to HQ; used credentials in web server and dumped entire database back on customer environment
    - Also saw SSH exposed, got credentials and were able to log into database server with SSH, moved laterally from server to server since everything was the same user name and password – attacker had data and ability to move laterally
    - Easily avoidable – site-to-site VPN, IPS in cloud and unified view into all environments

CASE STUDY 1: POWER COMPANY

CASE STUDY 2: RETAILER

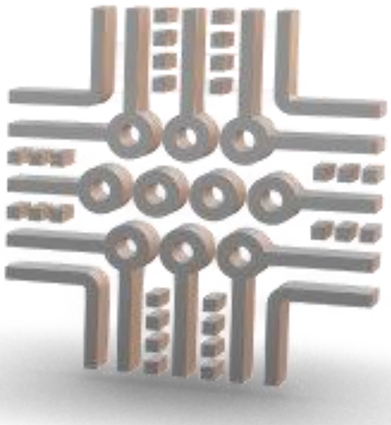
OK, WHAT ABOUT AFTER 7 DAYS

- **3.97 Million** ssh/telnet attacks + attempts to upload malware our cloud
- **826** scripting attacks
- 9 attacks detected by the ElasticPot search engine
- 98 exploit attempts against known vulnerabilities
- ~4900 attacks against TCP/UPD ports

CLOUDGUARD IN CPX360

CHECK POINT
CloudGuard

Check Point
SOFTWARE TECHNOLOGIES LTD.

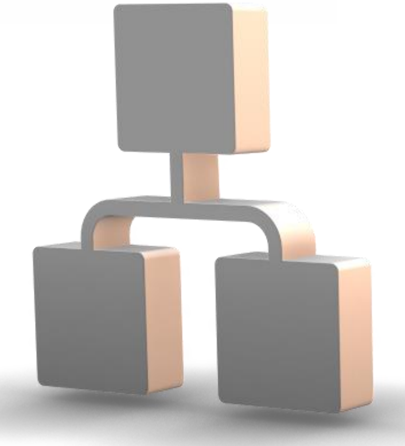


Cloud Cyber Attacks

Session: “Who’s responsible for your cloud security?”

Cloud Security Operation

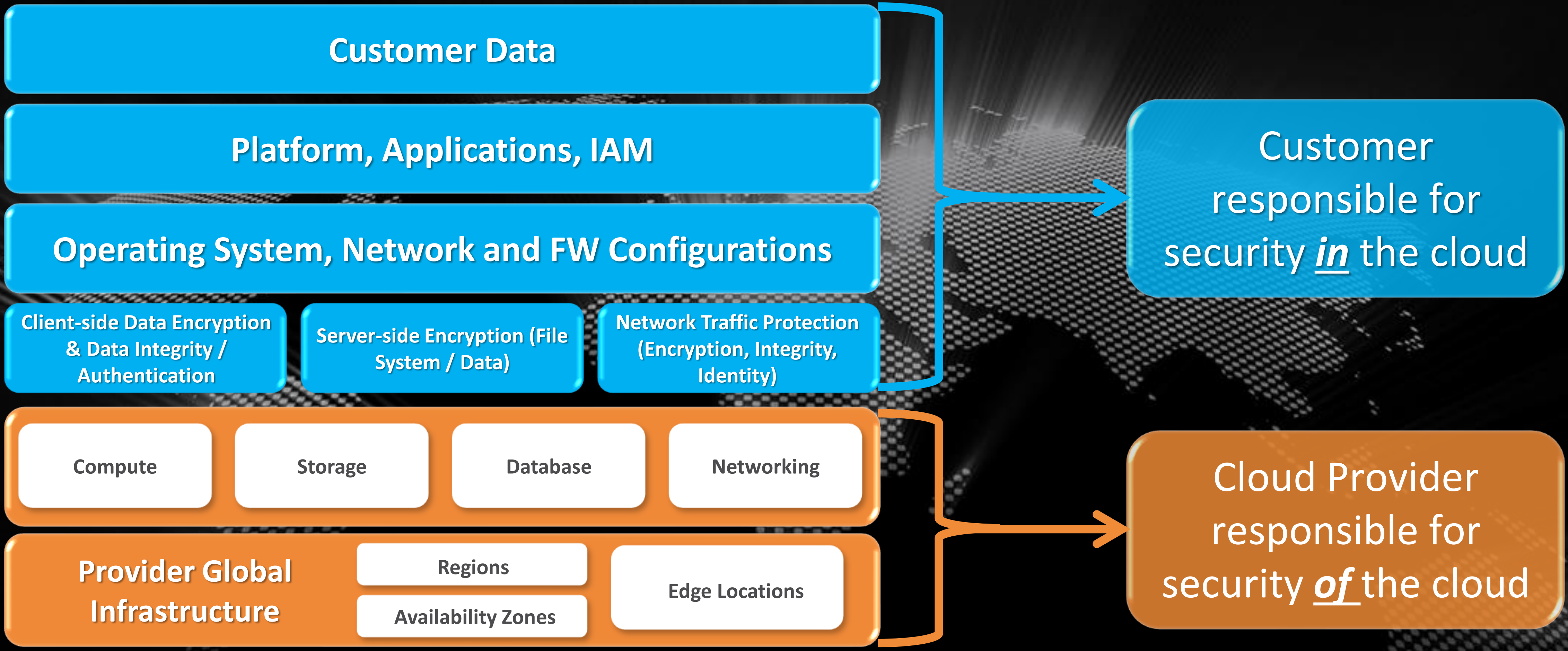
Session: “Adaptive Security that drives innovation in the cloud ”



Cloud Security BluePrint

Session: “Cloud Security Architecture & Blueprint”

CLOUD = SHARED RESPONSIBILITY



Customer Data

Platform, Applications, IAM

Operating System, Network and FW Configurations

Client-side Data Encryption & Data Integrity / Authentication

Server-side Encryption (File System / Data)

Network Traffic Protection (Encryption, Integrity, Identity)

Compute

Storage

Database

Networking

Provider Global Infrastructure

Regions

Availability Zones

Edge Locations

Customer responsible for security ***in*** the cloud

Cloud Provider responsible for security ***of*** the cloud