Check Point
SOFTWARE TECHNOLOGIES LTD

IS YOUR CLOUD SECURE?

Why advanced threat prevention security needs to be part of your cloud strategy

Greg Thomas| Security Engineer

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

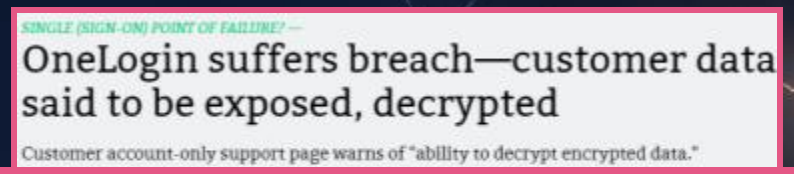
CLOUD • MOBILE • THREAT PREVENTION

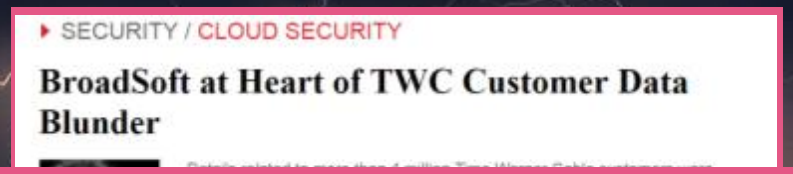
"I think that you will all agree that ***we are living in most interesting times.*** *I never remember myself a time in which our history was so full, in which day by day brought us new objects of interest, and, let me say also,* ***new objects for anxiety****."*

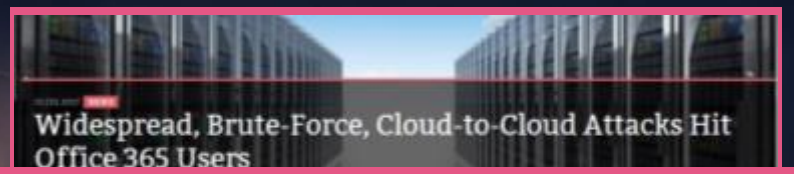
Joseph Chamberlain, Bristol, England, 1898

CURRENT STATE OF CLOUD SECURITY

NOT EVERY CLOUD HAS A SILVER LINING







And the hits just keep on coming . . .

Help Net Security
September 20, 2017

Number of lost, stolen or compromised records increased by 164%

Compared to the last six months of 2016, the number of lost, stolen or compromised records increased by 164%. A large portion came from the 22 largest data breaches, each involving more than one million compromised records. Of the 918 data breaches more than 500 (59% of all breaches) had an unknown or unaccounted number of compromised data records.

Most of the industries the Breach Level Index tracks had more than a 100% increase in the number of compromised, stolen or lost records. Education witnessed one of the largest increases in breaches up by 103% with an increase of over 4,000% in the number of records. This is the result of a malicious insider attack compromising millions of records from one of China's largest comprehensive private educational companies.

Healthcare had a relatively similar amount of breaches compared to the last six months of 2016, but stolen, lost or compromised records increased 423%. The

HOW EXPOSED ARE WE *REALLY* IN THE CLOUD?

Check Point
SOFTWARE TECHNOLOGIES LTD

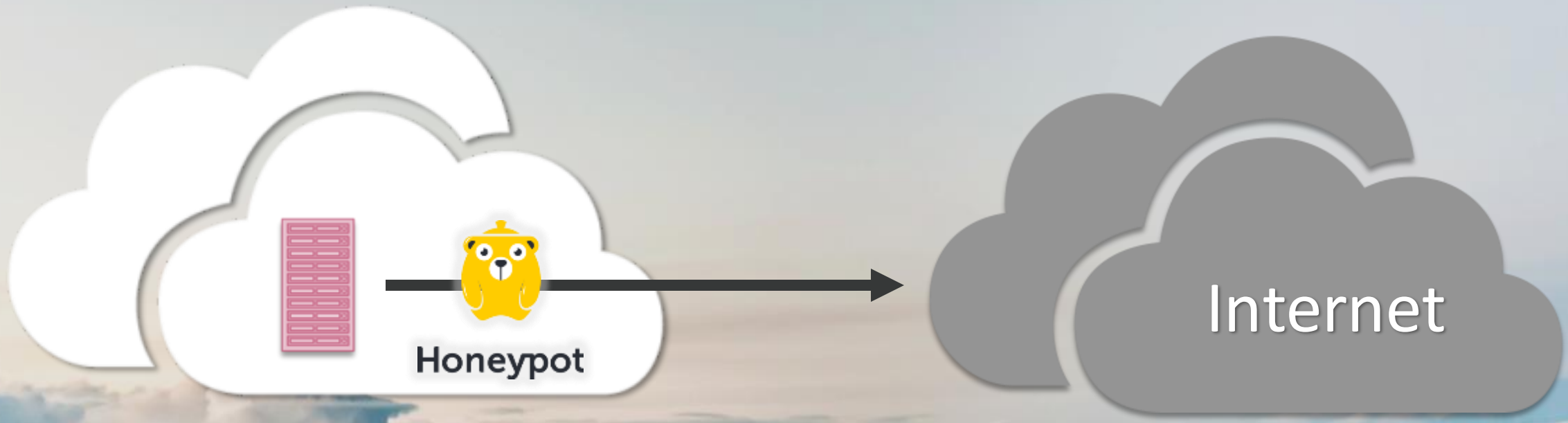
HOW LONG IS A MALWARE SIGNATURE VALID?

99% of malware hashes are seen for **58 seconds** or less

Public Cloud - IAAS

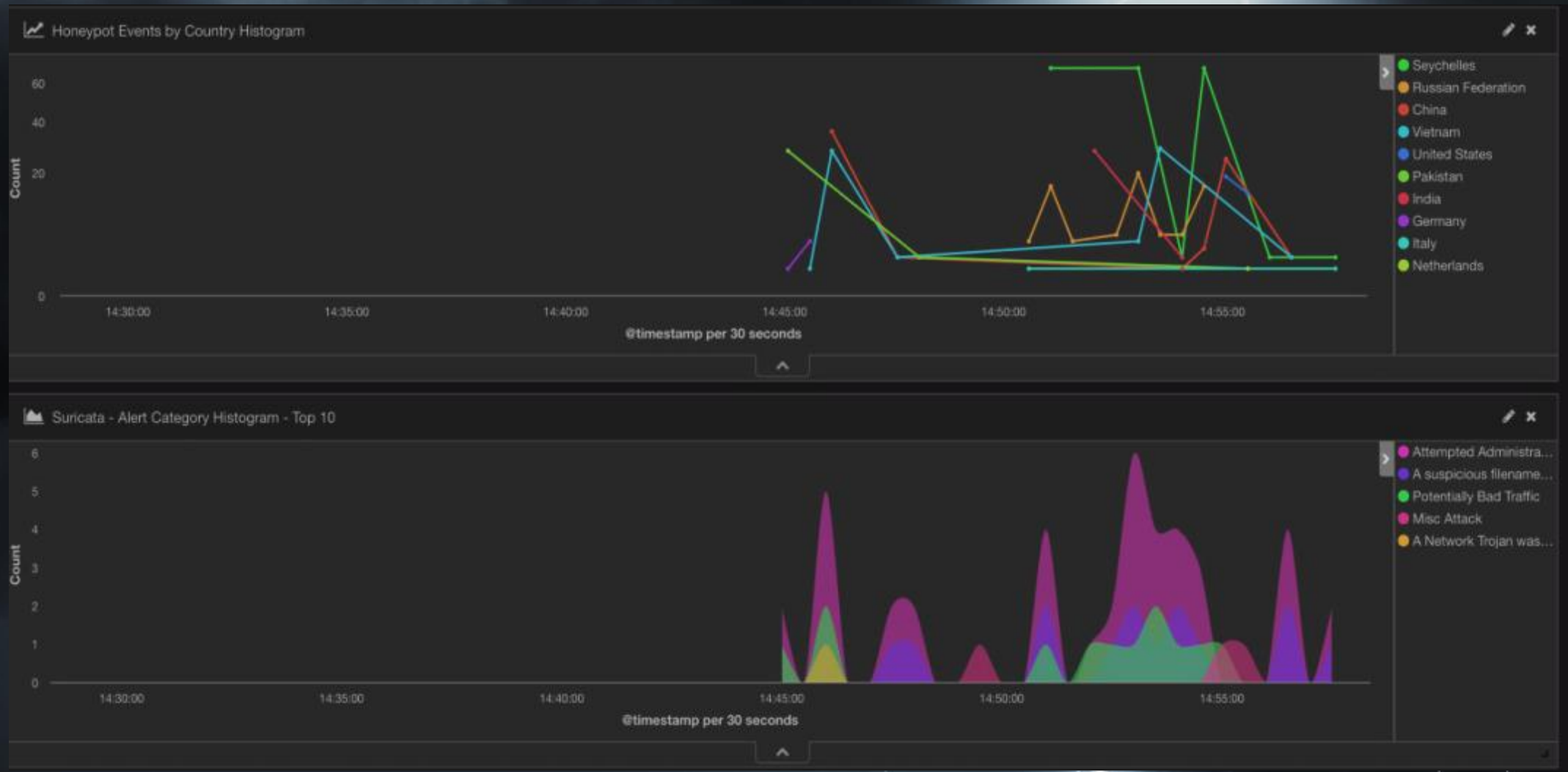
Public IAAS

OUR CLOUD ENVIRONMENT



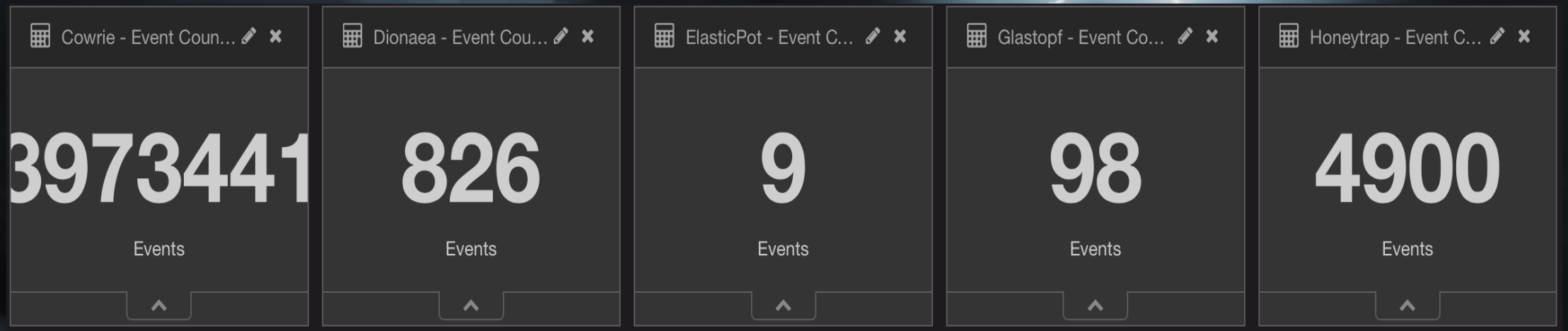
WITHIN THE FIRST 15 MINUTES

Houston we have a problem . . .



AFTER 7 DAYS . . .

Oh won't you please be my neighbor . . .



~4 million attacks recorded!

WHAT ABOUT

REAL CUSTOMER

ENVIRONMENTS?

CASE STUDY 1: GLOBAL TELCO

THE WRONG WAY TO PROMOTE A NEW SMART PHONE

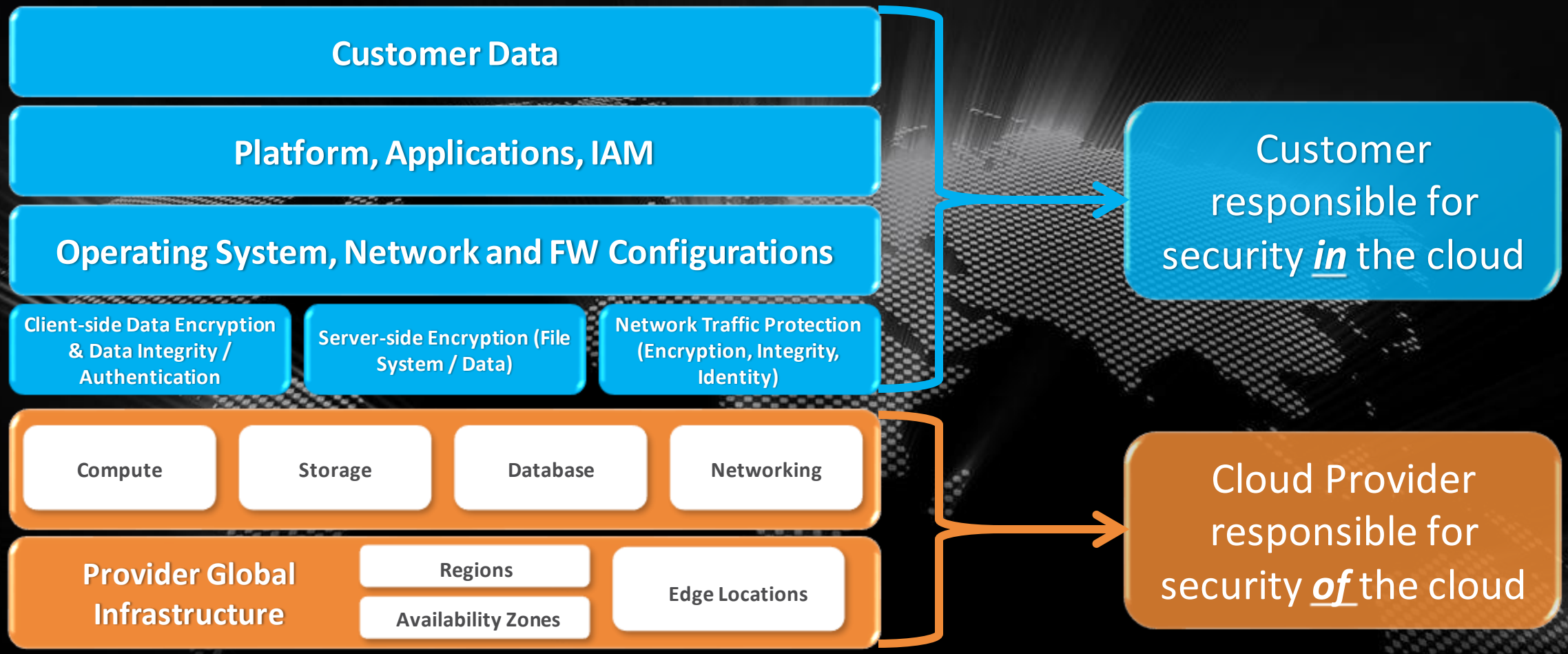
- Copy their premises-based network in the cloud with auto-scaling
- Campaign success! Infrastructure doubles every day since it was launched
- After 5 days – something's not quite right . . .
- Unknown process ID'd and running . . .
- Welcome to the wonderful world of Bitcoin Mining!
- Admin console exposure on web server led to attack

Check Point
SOFTWARE TECHNOLOGIES LTD

WHO'S RESPONSIBLE FOR PUBLIC CLOUD SECURITY?

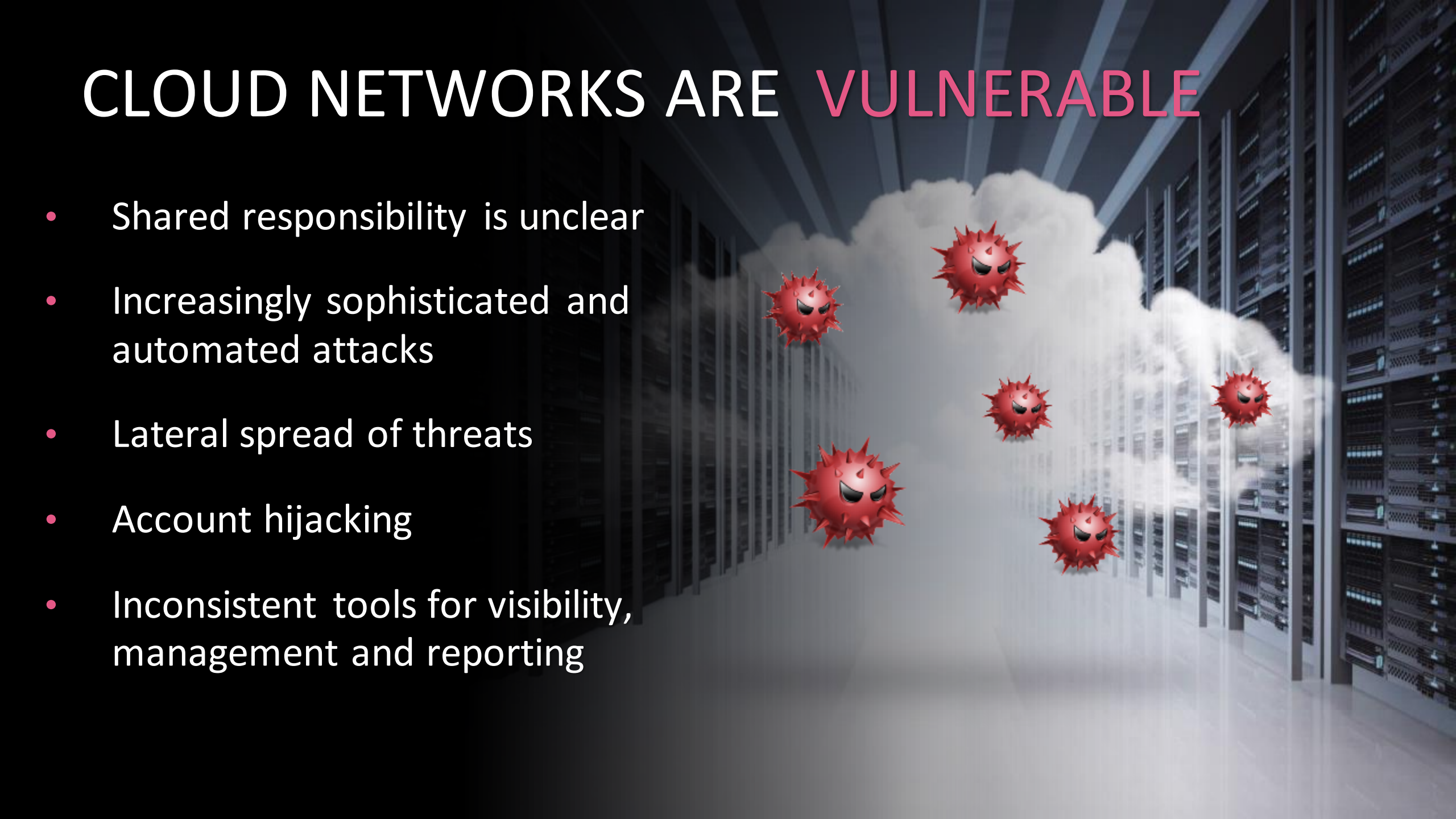
IT'S A SHARED RESPONSIBILITY

CLOUD = SHARED RESPONSIBILITY



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



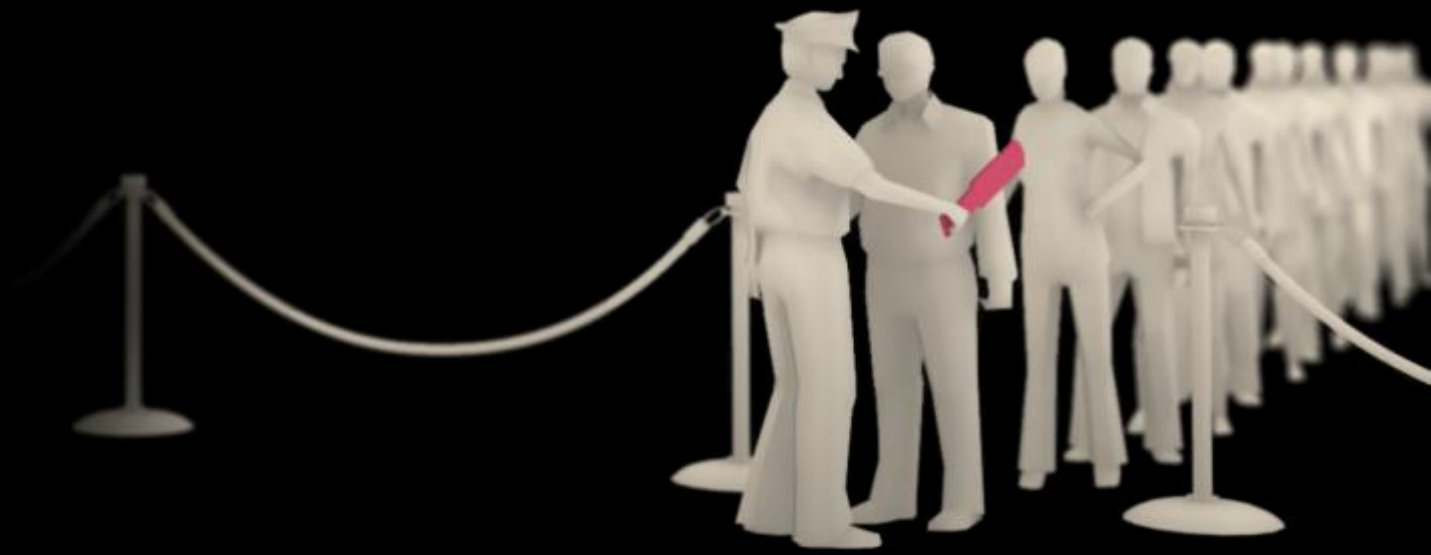
LEGACY SECURITY ARCHITECTURE IS NOT DESIGNED FOR CLOUD

Check Point
SOFTWARE TECHNOLOGIES LTD

- Cloud applications are everywhere
  Perimeter security is not enough – we need security inside the cloud

- Cloud applications are elastic
  Legacy security is static

- DevOps wants agile environment
  Security is a showstopper



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

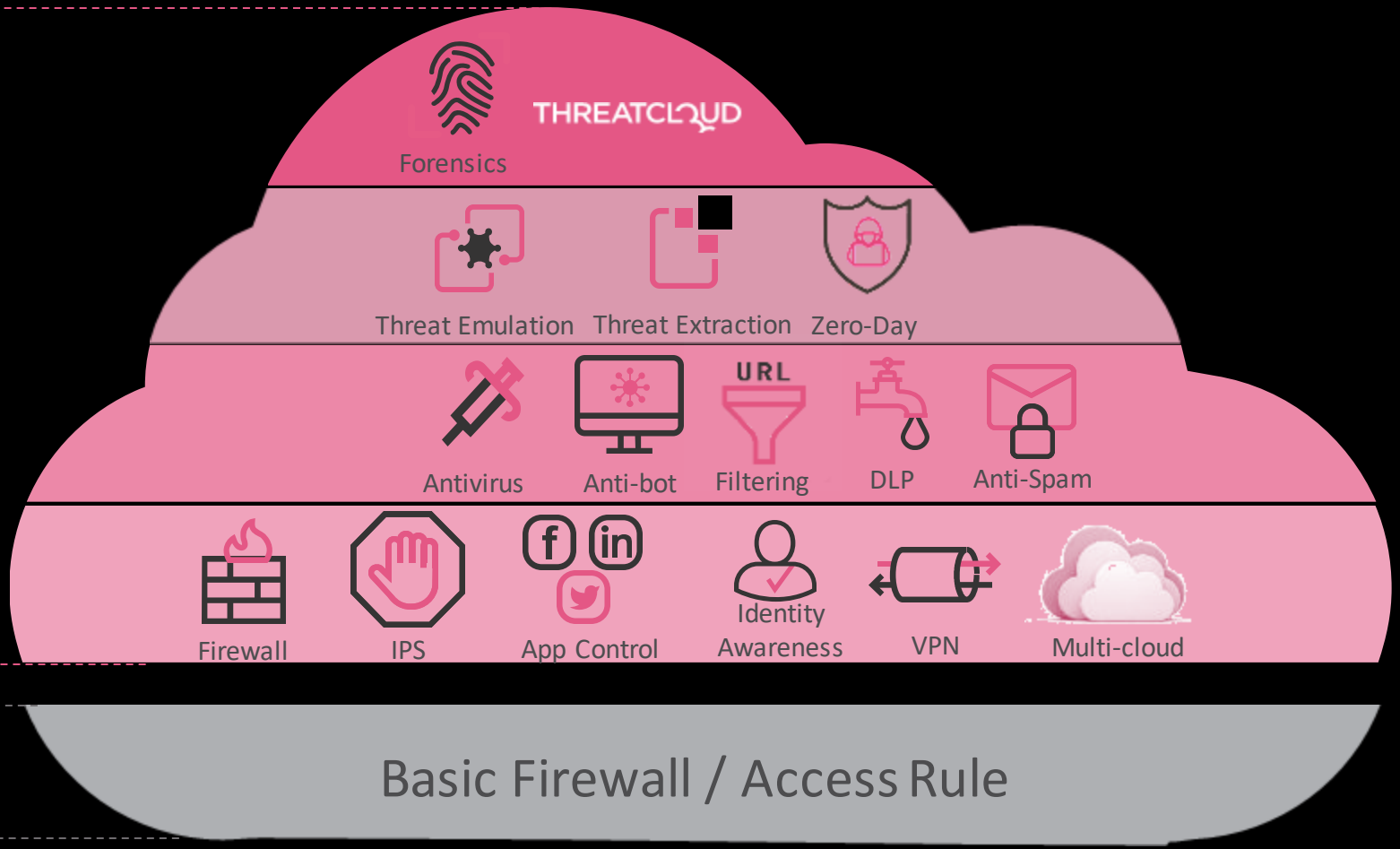
4. CENTRALIZED MANAGEMENT

Single pane-of-glass experience across all clouds

CLOUDGUARD IAAS ADVANCED PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT CloudGuard IaaS



Google Cloud · ORACLE CLOUD · aws · Azure · Alibaba Cloud

70% OF ENTERPRISES ADOPTED CLOUD APPLICATIONS*

ARE WE SECURED?

*Gartner

THE CASE OF A FINANCIAL INSTITUTION

Moved its email to the cloud

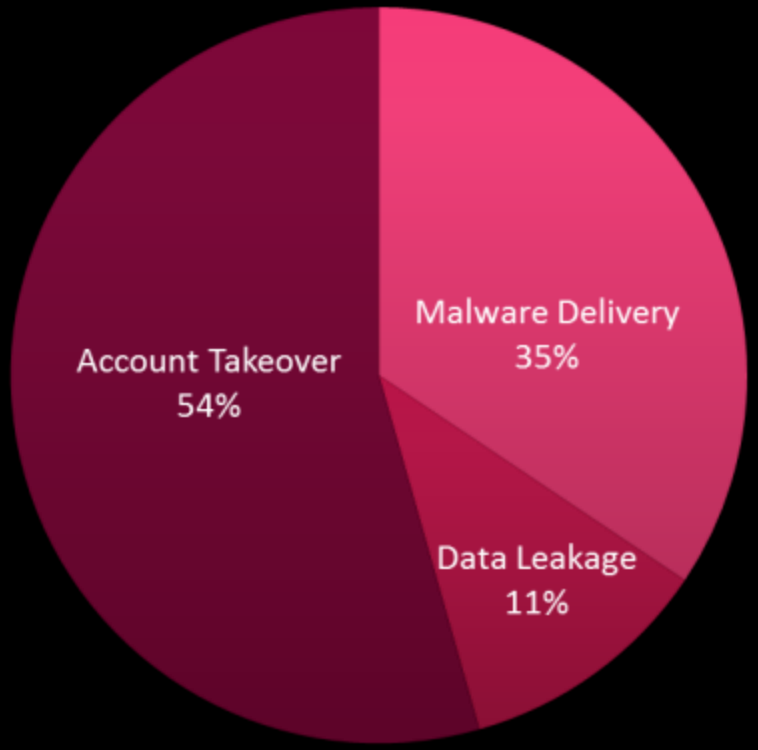
Office 365

Customers received email invoices with fake bank accounts

Emails were sent by hackers who took over an email account

$2M Stolen

90% of SaaS breaches are caused by hacking.
50% of the breaches are through account takeover.



Source: Check Point Q1-3-2017 Incident response Statistics, n=250, cloud = 55%

Malware Delivery Data Leakage Account Hijacked

INTRODUCING CHECK POINT CLOUDGUARD

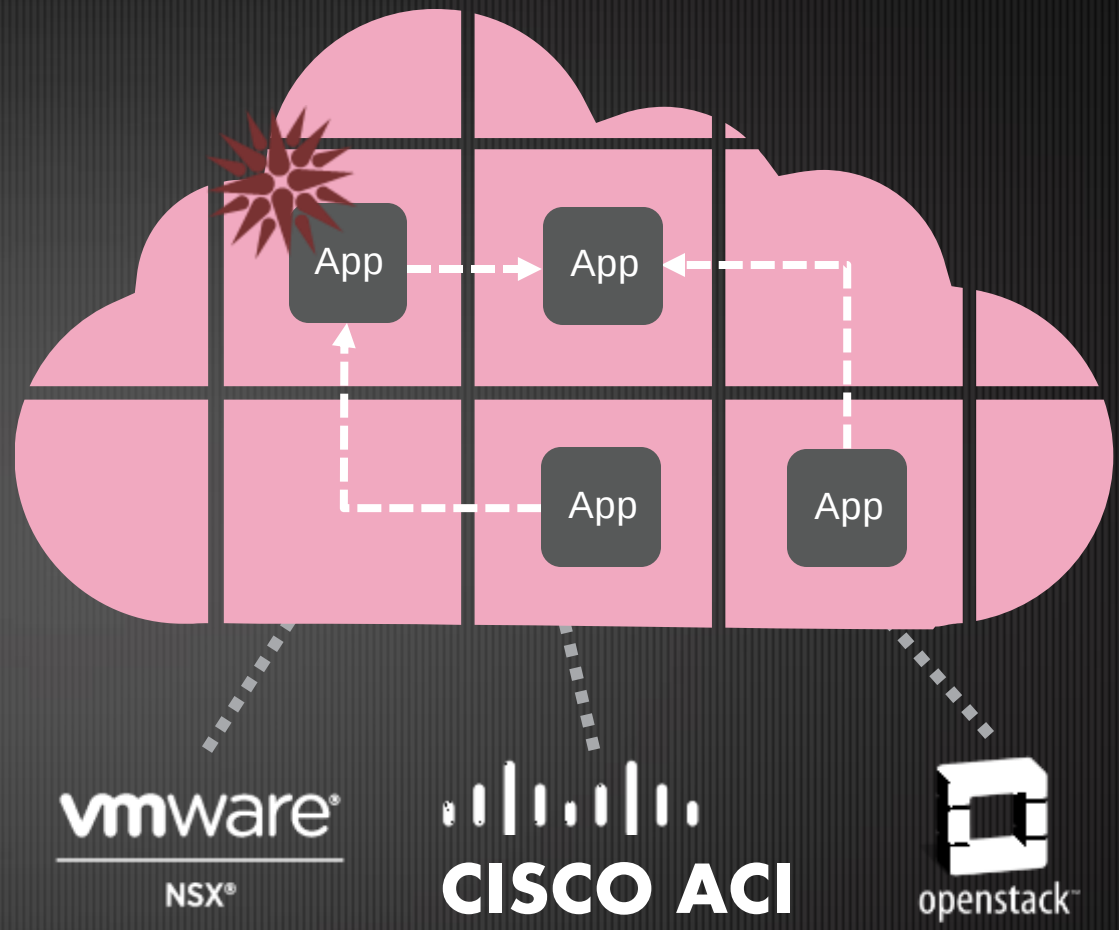
PROTECTING ANY CLOUD, ANY SERVICE, ANYWHERE

COMPREHENSIVE SECURITY ARCHITECTURE

CLOUDGUARD – MICRO SEGMENTATION

Check Point
SOFTWARE TECHNOLOGIES LTD

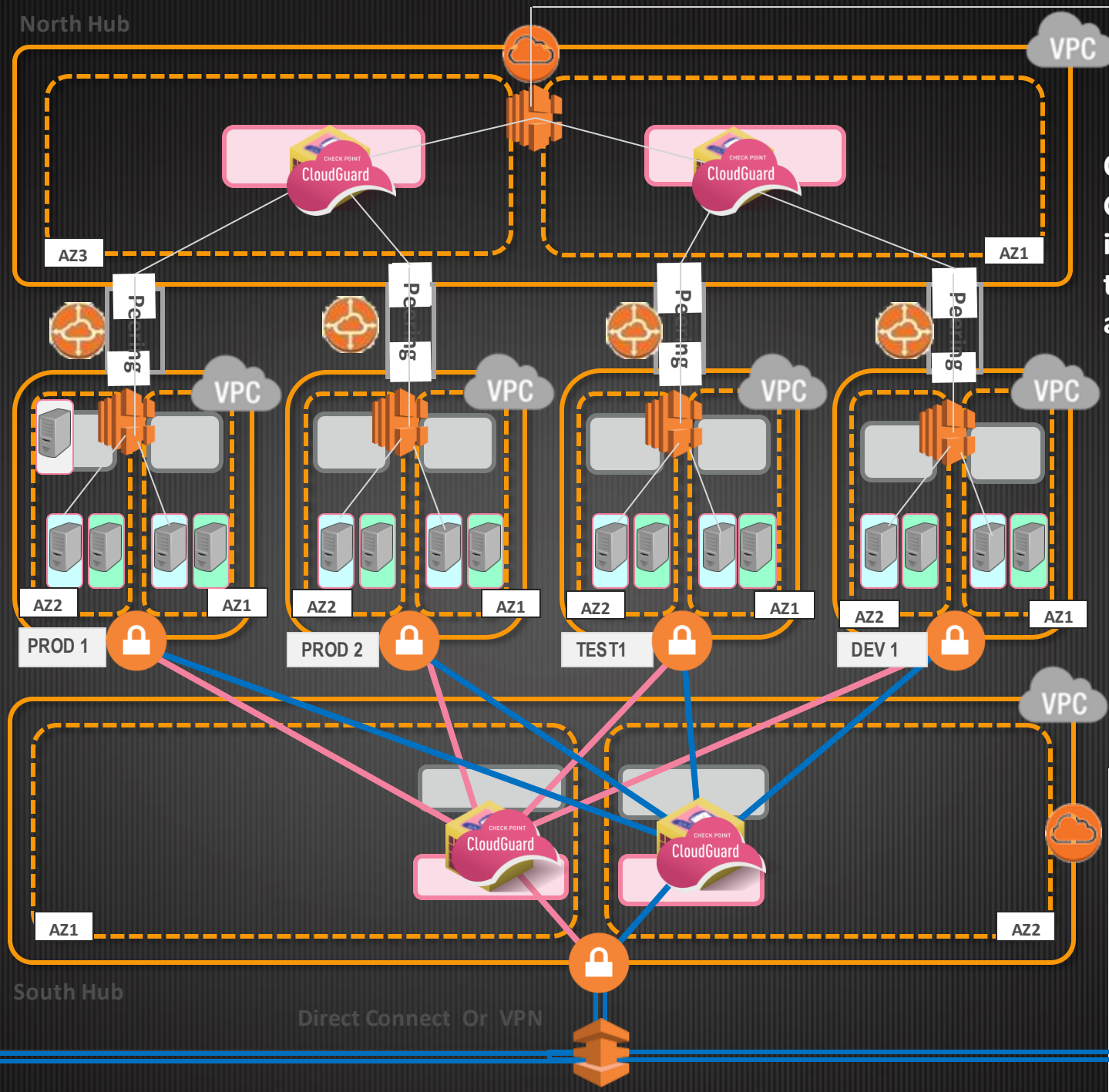
Micro segment the Cloud with advanced protection between applications with tight Integration to SDN



Check Point Security Blueprint

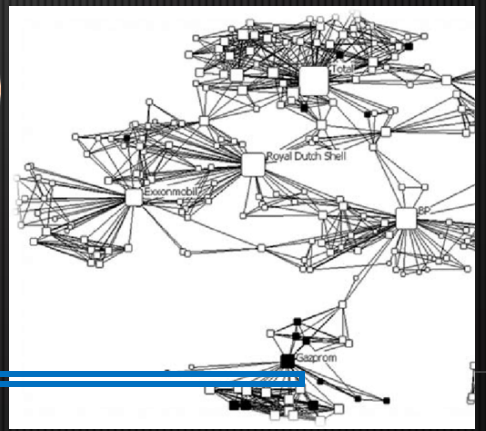
On the South Hub , Cloud Guard Transit Gateways inspect internal traffic moving between VPCs for East-West Threat Prevention, as well as traffic between the Datacenter or MPLS network and the cloud.

Direct Connect or VPN links connect to Transit Gateways



Check Point
SOFTWARE TECHNOLOGIES LTD.

On the North Hub a Cloud Guard auto scale group inspects Internet inbound traffic to Public facing applications/websites.



MOBILE

SandBlast MOBILE

- App Protection
- Network Protection
- Device Protection

Capsule WorkSpace/Docs

- Remote Access
- Secure Business data
- Protect docs everywhere

ENDPOINT

SandBlast AGENT

- Threat Prevention
- Anti-Ransomware
- Forensics

Access/Data Security

- Access Control
- Secure Media
- Secure Documents

Threat Intelligence

THREATCLOUD GEN V

MGMT - R80

CLOUD

servicenow

Infrastructure

CloudGuard IaaS

- Advanced Threat Prevention
- Adaptive Security
- Automation and Orchestration
- Cross Cloud Dynamic Policies
- Multi-Cloud

Microsoft Azure, Azure Stack, VMware NSX, OpenStack, aws

Applications

CloudGuard SaaS

- Zero-Day Threat Protection
- Sensitive Data Protection
- End-to-end SaaS Security
- Identity Protection

Office 365, Salesforce, Dropbox, Google Apps

Hybrid Cloud

HEADQUARTERS

- Multi Layered Security
- Advanced Threat Prevention
- Inbound Outbound Access Control
- Data Protection

- Access Control
- Advanced Threat Prevention
- Segmentation

BRANCH

VPN IDA

LAN

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION