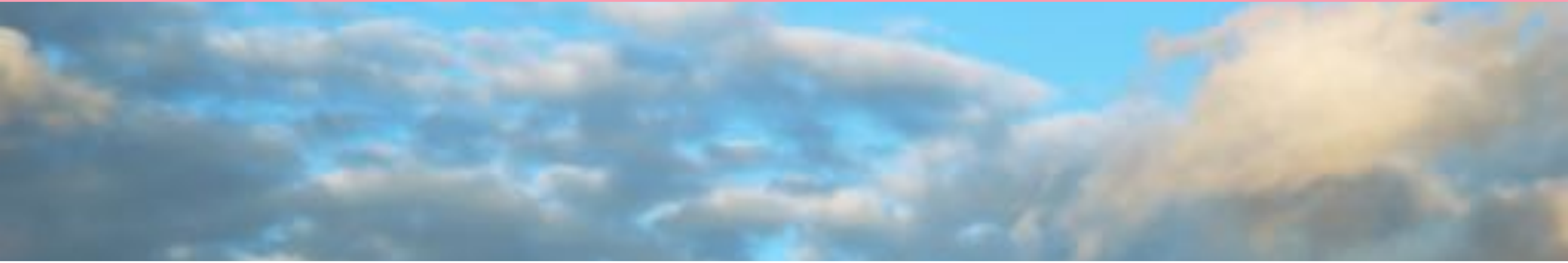
“Protecting You From You!”

The #1 Challenge In The Age of Software Defined Everything



Check Point®
SOFTWARE TECHNOLOGIES LTD.

-0.20%
+0.60%
+0.12%
-0.20%
+0.60%
+0.60%
+0.12%
+0.12%
+0.12%

Some Important Perspective

“Enterprises sper 2018, with public
cloud services clair of that, according to
IDC. That's right. **Pub** **tal IT spending globally.”**

“In other words, rat rket share within public
cloud, a far more us to help enterprises
break free of ineffic shackles.”

TechRepublic
- By Matt Asay
- August 6, 2019

Check Point®
SOFTWARE TECHNOLOGIES LTD.

The Choice Is Obvious…

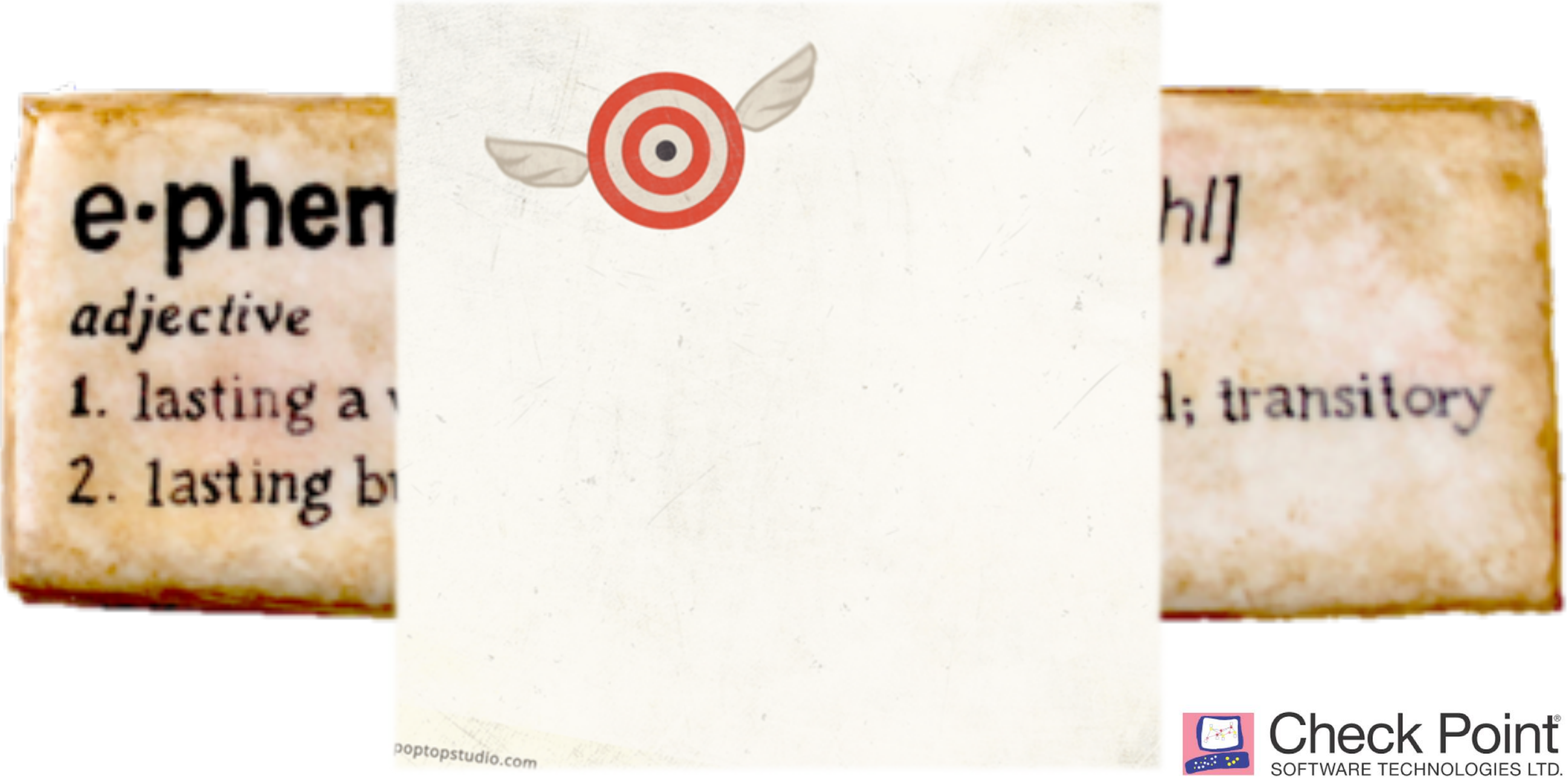
Now, You're Renting A Slightly Larger Boat

You've Been The Captain of Your Own Ship

Things You Won't See In Your Datacenter…

Check Point
SOFTWARE TECHNOLOGIES LTD.

Things You Won't See In Your Datacenter…



Check Point
SOFTWARE TECHNOLOGIES LTD.

Things You Won't See In Your Datacenter…

What Is Your Primary Cloud Deployment Strategy?

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Biggest Operational Headaches

Check Point
SOFTWARE TECHNOLOGIES LTD.

Compliance & Visibility…

On-Premise Datacenter

Public Cloud Datacenter

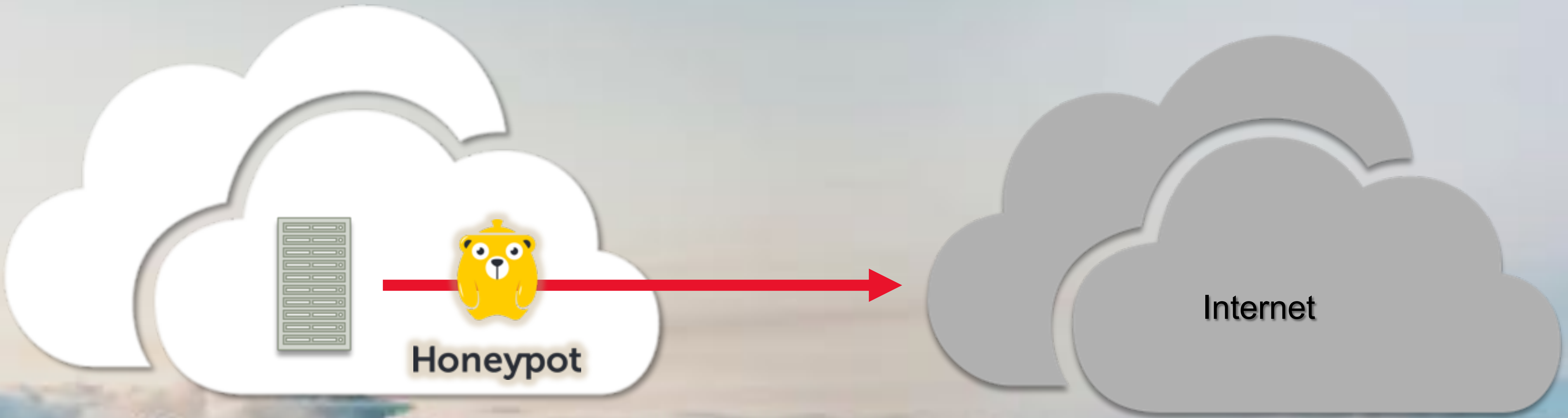
Check Point
SOFTWARE TECHNOLOGIES LTD.

How Well Do Traditional Network Security Tools/Appliances Work In Cloud Environments?

Check Point®
SOFTWARE TECHNOLOGIES LTD.

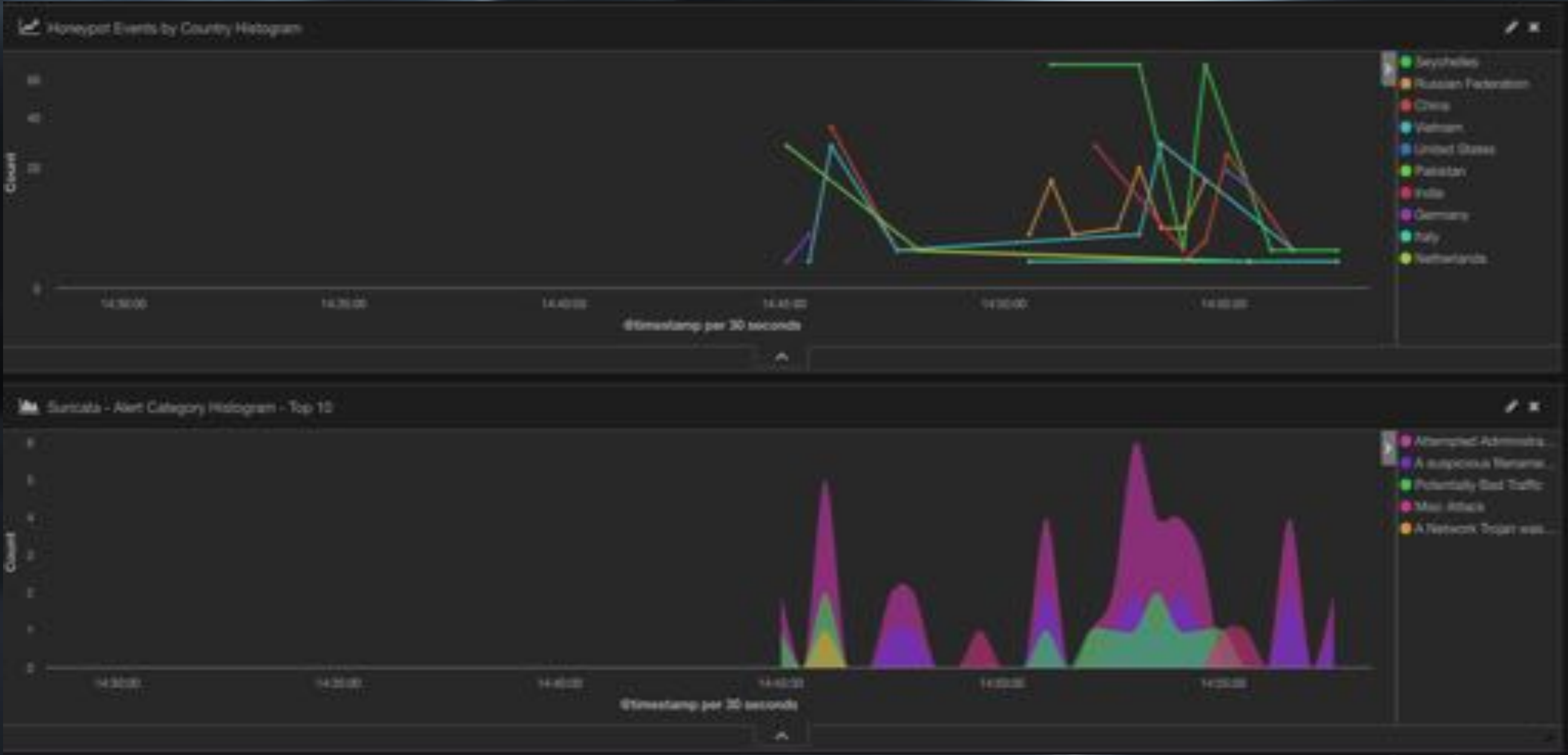
HOW EXPOSED ARE WE *REALLY* IN THE CLOUD?

OUR CLOUD ENVIRONMENT



WITHIN THE FIRST 15 MINUTES

Houston we have a problem . . .

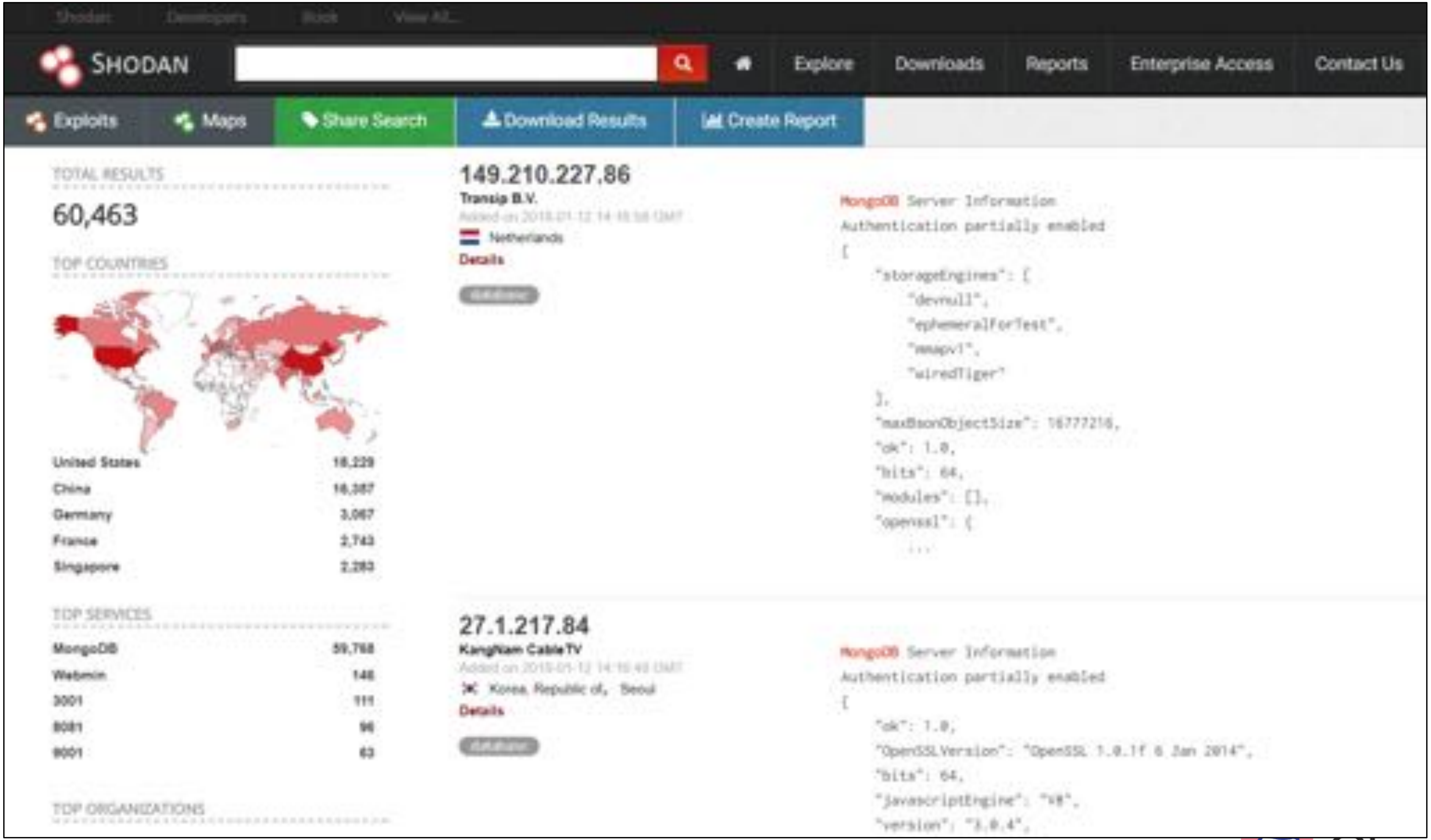


OK, WHAT ABOUT AFTER 7 DAYS

- 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/UDP ports

Everyone Uses Mongo!

ebay
intuit.
OTTO
Google
mongoDB®
CISCO™
Expedia
f
Check Point®
SOFTWARE TECHNOLOGIES LTD.



TOTAL RESULTS

60,463

TOP COUNTRIES

United States	18,229
China	16,387
Germany	3,067
France	2,743
Singapore	2,283

TOP SERVICES

MongoDB	59,768
Webmin	148
3001	111
8081	96
8001	63

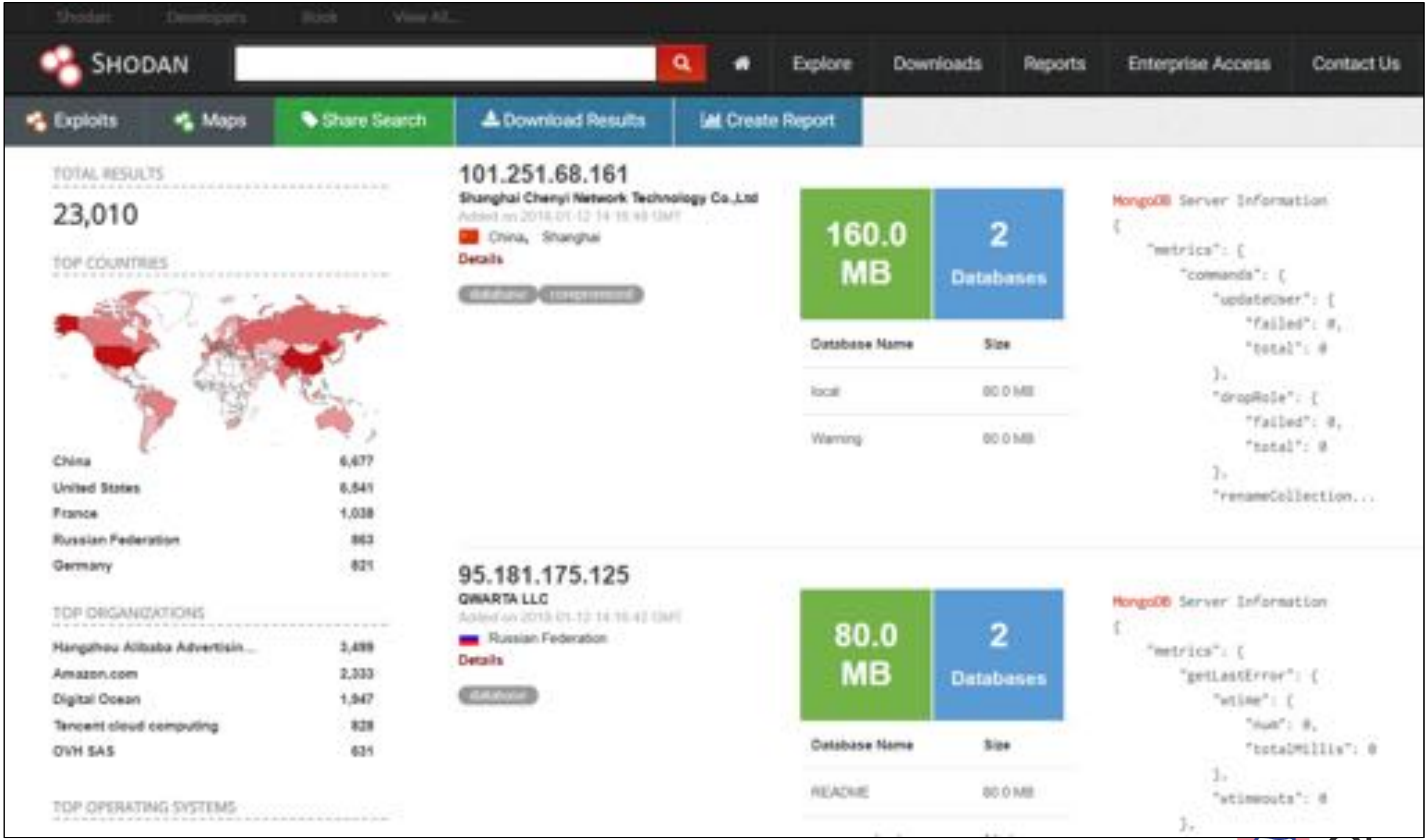
TOP ORGANIZATIONS

149.210.227.86
Transip B.V.
Added on 2016-01-12 14:18:58 GMT
Netherlands
Details

```
MongoDB Server Information
Authentication partially enabled
{
    "storageEngines": [
        "devnull",
        "ephemeralForTest",
        "mmapv1",
        "wiredTiger"
    ],
    "maxBsonObjectSize": 16777216,
    "ok": 1.0,
    "bits": 64,
    "modules": [],
    "openssl": {
        ...
```

27.1.217.84
KangNam Cable TV
Added on 2016-01-12 14:18:49 GMT
Korea, Republic of, Seoul
Details

```
MongoDB Server Information
Authentication partially enabled
{
    "ok": 1.0,
    "OpenSSLVersion": "OpenSSL 1.0.1f 6 Jan 2014",
    "bits": 64,
    "javascriptEngine": "V8",
    "version": "3.0.4",
```



TOTAL RESULTS

23,010

TOP COUNTRIES

China	6,477
United States	6,841
France	1,038
Russian Federation	863
Germany	821

TOP ORGANIZATIONS

Hangzhou Alibaba Advertisin...	3,499
Amazon.com	2,333
Digital Ocean	1,947
Tencent cloud computing	828
OVH SAS	631

TOP OPERATING SYSTEMS

101.251.68.161

Shanghai Chenyi Network Technology Co.,Ltd

Added on 2018-01-12 14:15:48 GMT

China, Shanghai

Details

database compromised

160.0 MB — 2 Databases

Database Name	Size
local	80.0 MB
Warning	80.0 MB

```
MongoDB Server Information
{
    "metrics": {
        "commands": {
            "updateUser": {
                "failed": 0,
                "total": 0
            },
            "dropRole": {
                "failed": 0,
                "total": 0
            },
            "renameCollection...
```

95.181.175.125

QWARTA LLC

Added on 2018-01-12 14:16:42 GMT

Russian Federation

Details

database

80.0 MB — 2 Databases

Database Name	Size
README	80.0 MB

```
MongoDB Server Information
{
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis": 0
            },
            "wtimeouts": 0
        },
```

Has Your Organization Been Hacked In The Cloud?

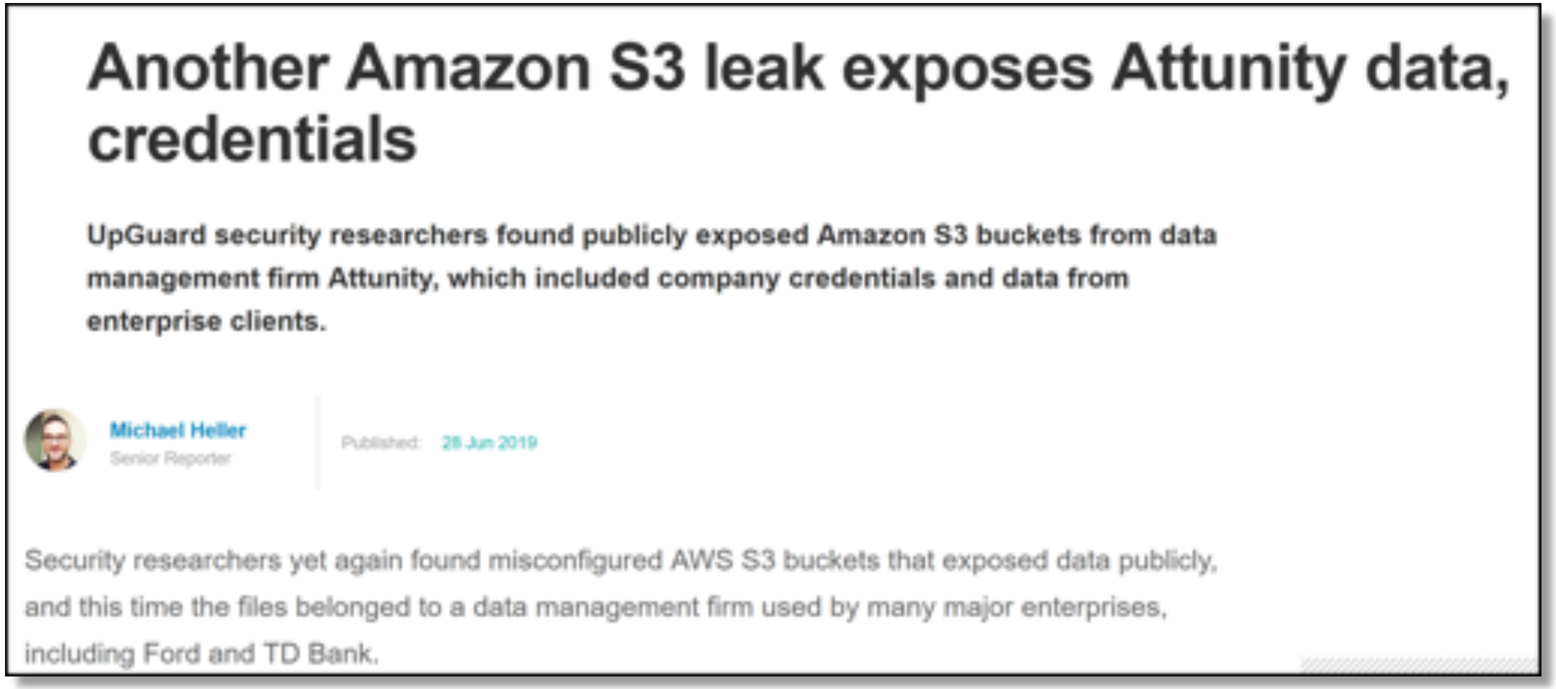
Yi

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Issue: Most Cloud Breaches Exploit Poor or Non-Existent Access Controls

7% of S3 buckets lacked access control,
35% unencrypted
[2017 study]



Another Amazon S3 leak exposes Attunity data, credentials

UpGuard security researchers found publicly exposed Amazon S3 buckets from data management firm Attunity, which included company credentials and data from enterprise clients.

Michael Heller
Senior Reporter

Published: 28 Jun 2019

Security researchers yet again found misconfigured AWS S3 buckets that exposed data publicly, and this time the files belonged to a data management firm used by many major enterprises, including Ford and TD Bank.

Limited encryption at rest is a contributing problem

Just One Example

S3 Buckets Publicly Accessible

Customer AND Internal Data Exposed

Data Included

OneDrive Accounts

Email

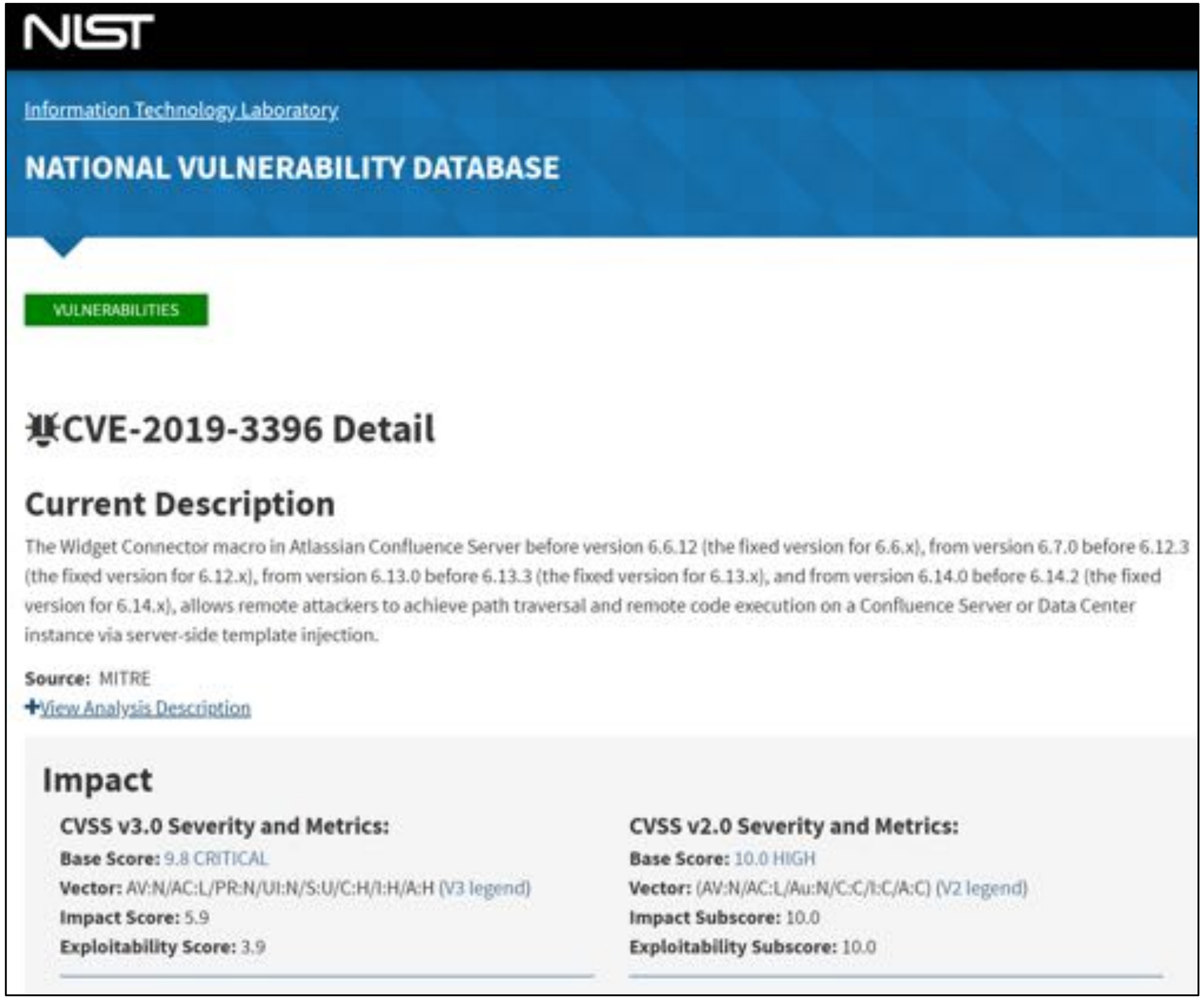
System passwords

Network architecture

Product specs

Check Point
SOFTWARE TECHNOLOGIES LTD.

Issue: Application or Stack Vulnerabilities Require Patching



NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2019-3396 Detail

Current Description

The Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Impact Score: 5.9

Exploitability Score: 3.9

CVSS v2.0 Severity and Metrics:

Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CheckPoint IR Team Case

Unpatched Confluence Server In Large AWS Estate

Exploited by Rocke Group Threat Actor

Customer Detected Unusual CPU Spikes

CheckPoint Investigation Found

Cryptocurrency Mining In Progress

MONERO

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Issue: Compounded ‘Cloud Native’ Attack

Large FinSec: ~100 million records compromised

Customer deployed vulnerable/ misconfigured open source WAF w/SSRF vulnerability

Attacker used SSRF to attack the instance’s Metadata Service and gained the instance’s role session tokens.

Customer’s misconfiguration of the WAF’s IAM role was critical and enabled unlimited access to S3

Lack of proper security monitoring prevented mitigation at early phases of the attack

Breach: March 2019
Detected: July 2019

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

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Cloud Providers Are Getting Better

The Cloud Platforms Know-Security Is Inhibiting Adoption

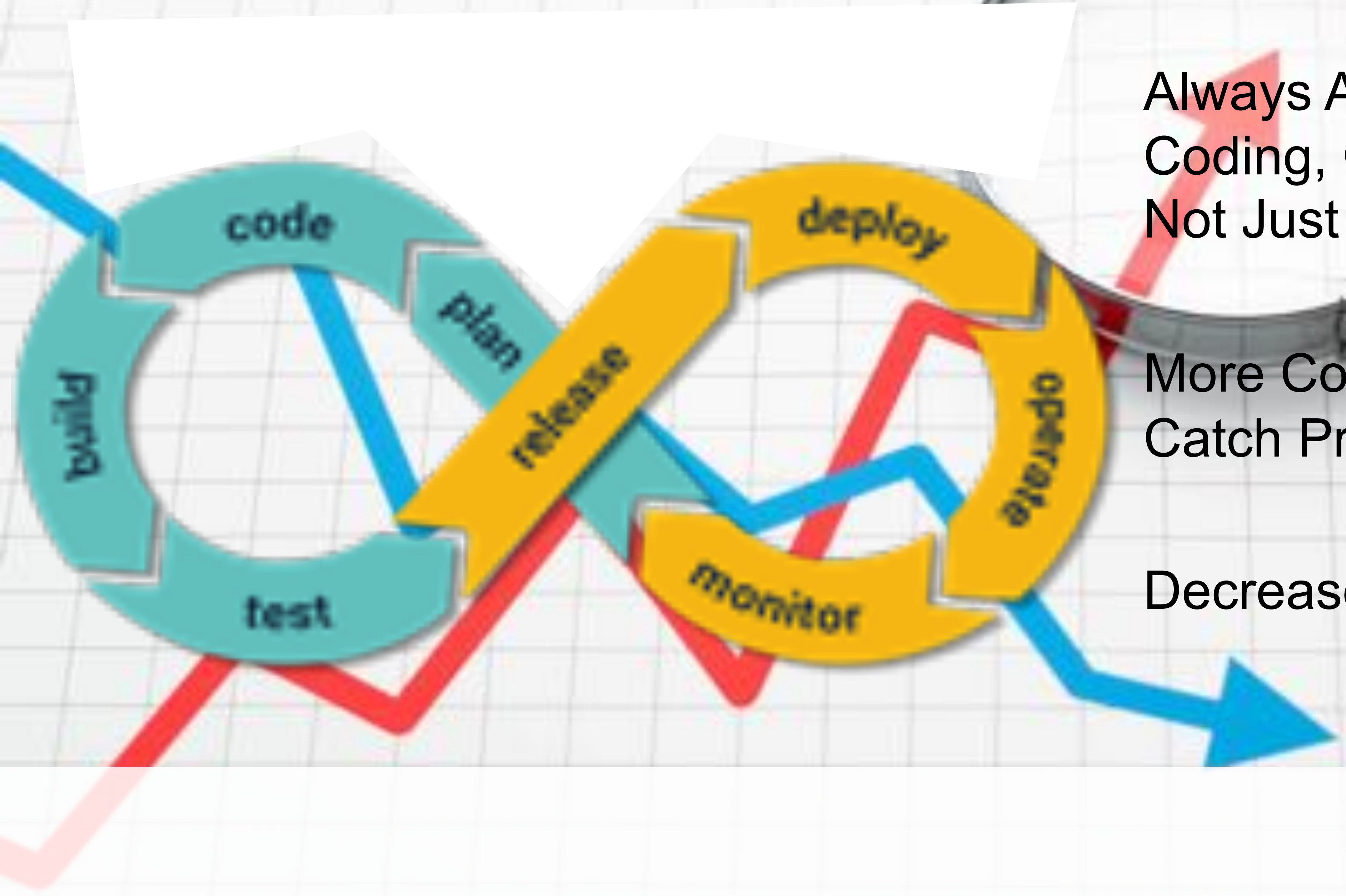
Security Services Offered To Reduce Risk

Providers Continue Evolving and Expand Security Services

Cloud Security Services Are Innovating…

- Security Is Dynamic – Constantly Evolving Threats
- Consistency is Key – But Challenging Across Multiple Clouds
- Rich APIs Create Opportunities
- Seek Vendors With Commitment To Cloud

KeyTrend: *Shift Left* from Production to DevSecOps

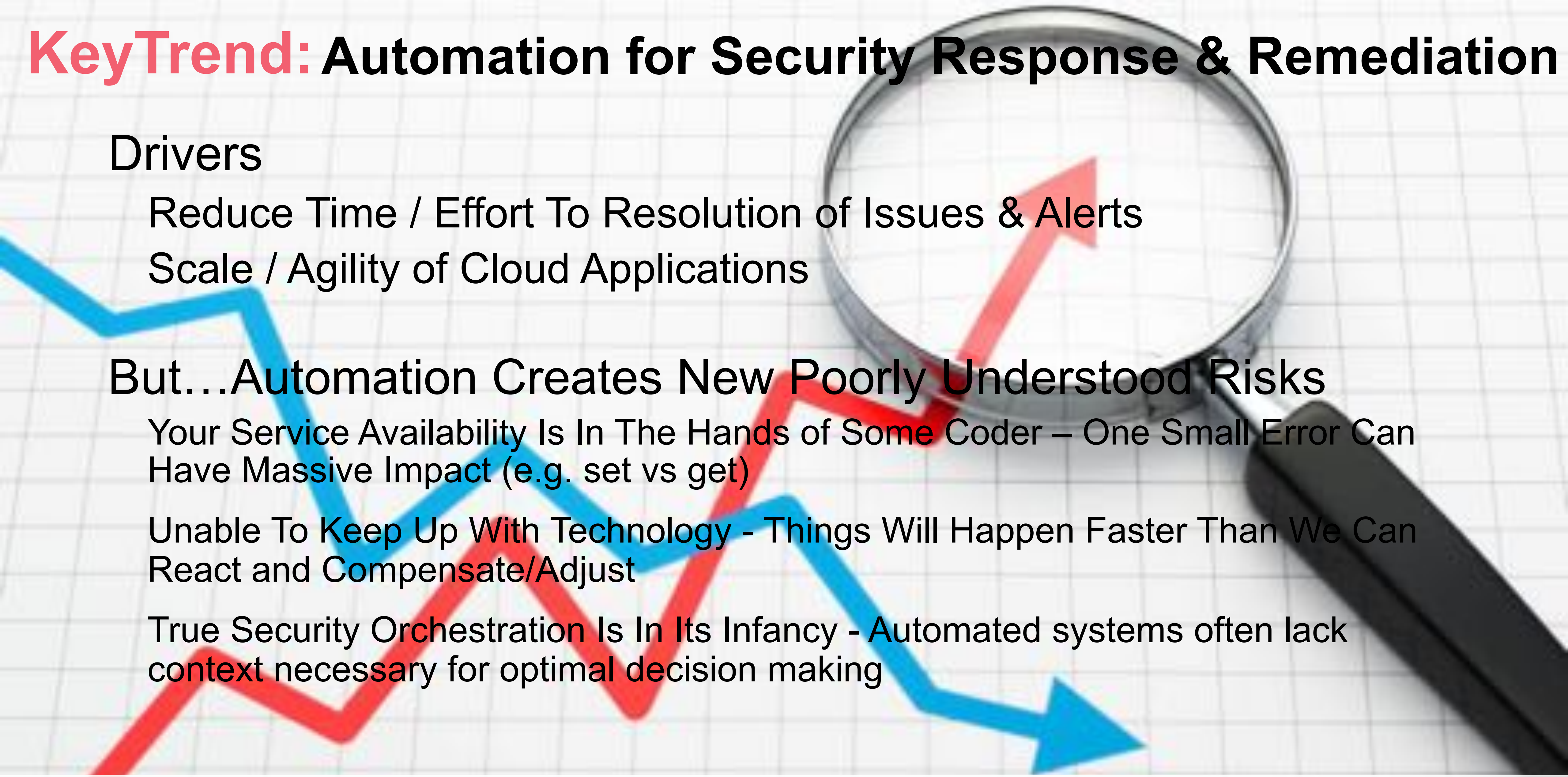


Always Apply Security - Coding, Commit, & Test - Not Just In Production

More Cost Effective - Catch Problems Early

Decreases Friction & Delay

KeyTrend: Automation for Security Response & Remediation



Drivers

- Reduce Time / Effort To Resolution of Issues & Alerts
- Scale / Agility of Cloud Applications

But…Automation Creates New Poorly Understood Risks

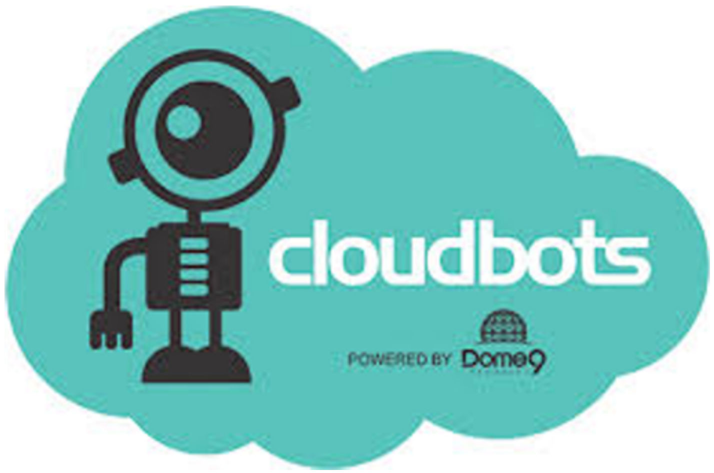
- Your Service Availability Is In The Hands of Some Coder – One Small Error Can Have Massive Impact (e.g. set vs get)
- Unable To Keep Up With Technology - Things Will Happen Faster Than We Can React and Compensate/Adjust
- True Security Orchestration Is In Its Infancy - Automated systems often lack context necessary for optimal decision making

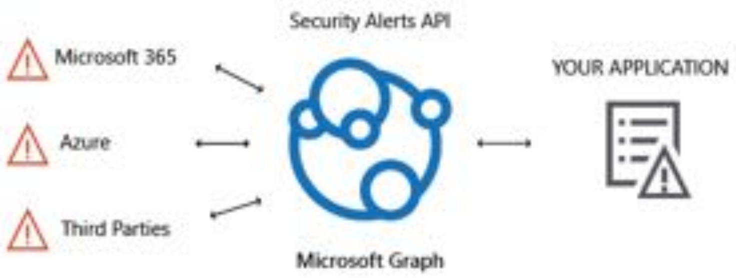
KeyTrend: Containers Are Growing in Popularity

"By 2023, more than 70% of global organizations will be running more than two containerized applications in production, up from less than 20% in 2019."

Gartner: 3 Critical Mistakes That I&O Leaders Must Avoid With Containers. (Available by subscription-only)

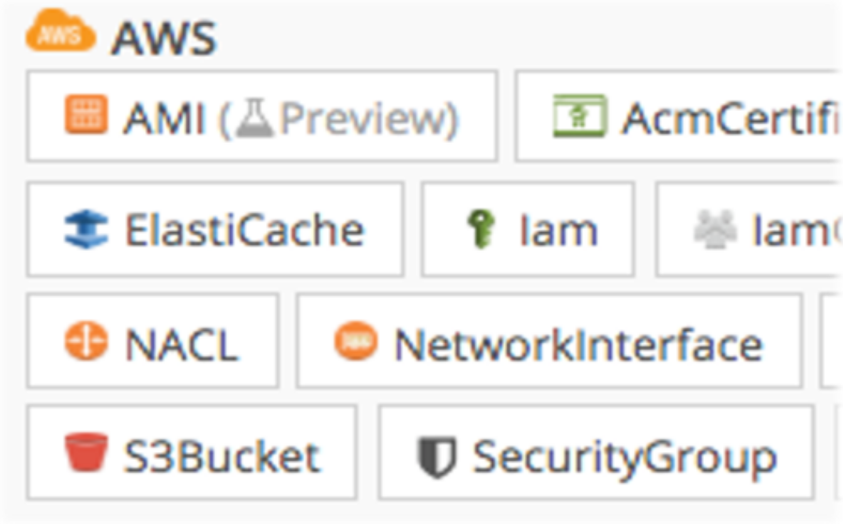
Which Security Control Would Most Increase Confidence In Adopting Public Clouds?





Check Point®
SOFTWARE TECHNOLOGIES LTD.

What Do You Consider Most Important When Evaluating A Cloud Security Solution?



pd

Jira

servicenow

slack

Check Point
SOFTWARE TECHNOLOGIES LTD.

Top 5 Cloud Security Design Guidelines

1. Protecting all assets
VM, Container, Serverless, PaaS ,
Apps, Network, Repositories

2. All Disciplines
Hardening, Compliance, Access,
Threats, DLP

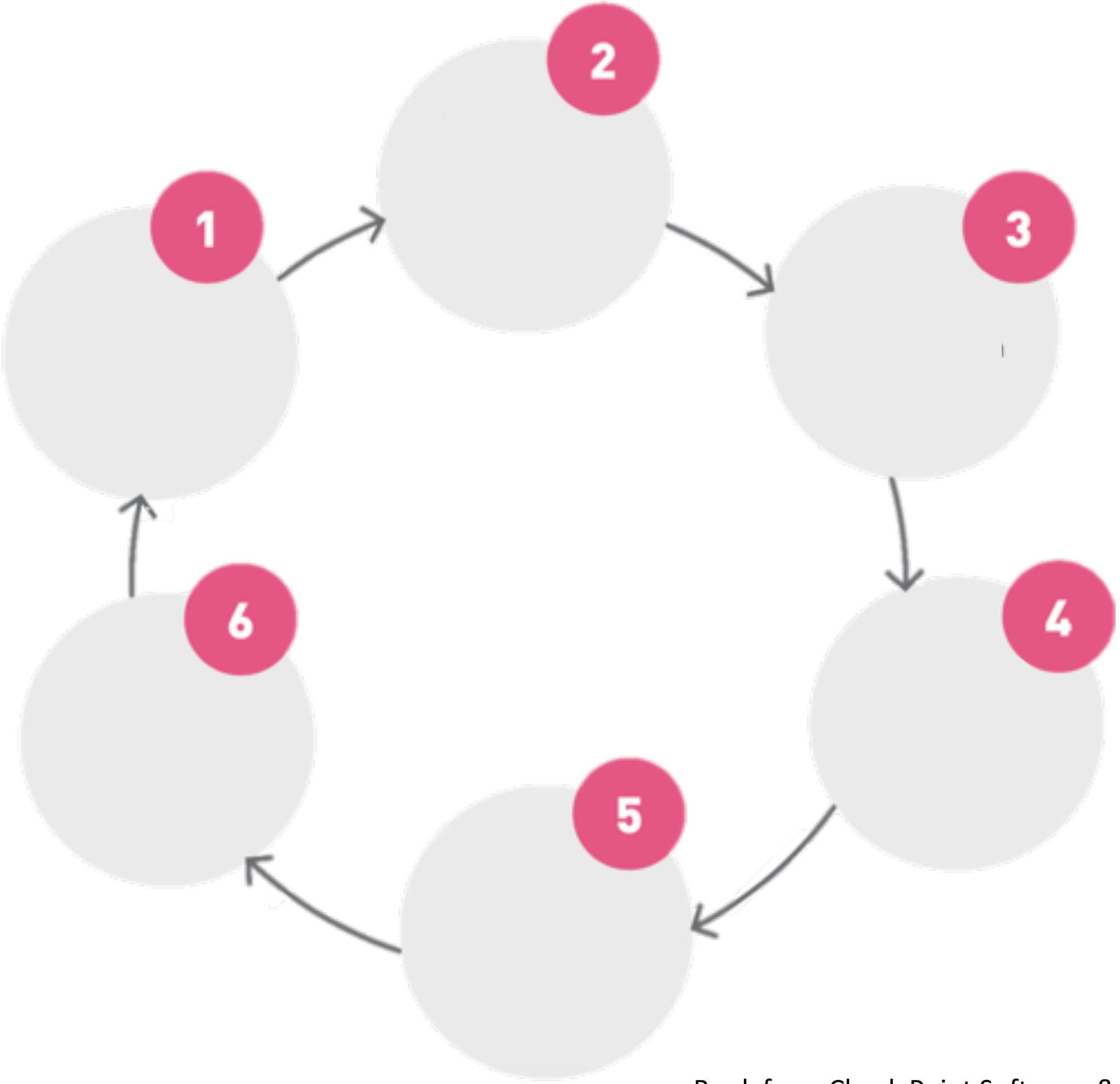
3. Enabling DevOps & IT
Automated Deployment , Adaptive
Policy, API deployment

4. Secure all Clouds
AWS, Azure, Google, Ali,
OCI, Private NSX, ACI

5. Leveraging Native controls
Logs, Controls,
Remediation,
Orchestration

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Six Steps to Compliance Automation



eBook from Check Point Software & AWS
AUTOMATE YOUR CLOUD COMPLIANCE JOURNEY IN 6 STEPS

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Four Steps to Begin Implementing Containers

Get Started! Begin familiarizing your IT and development teams with deploying a Kubernetes stack in the public cloud

Select Best App Candidates – Standalone apps that don't require other apps to run.

Gartner to Infrastructure & Operations Leaders: "Establish a foundation to measure results achieved with containers by creating a list of container management objectives and outcomes…"*

Stay Up To Date - Container-related industry is fast-moving and constantly changing.

Robert Christiansen CIO Magizine

*Gartner: 3 Critical Mistakes That I&O Leaders Must Avoid With Containers.

Check Point® SOFTWARE TECHNOLOGIES LTD.

You Must Protect You from You!

Security Is YOUR Problem In The Cloud

Cloud Attack Surface is Broad & Complex

Investigate/Consider Cloud Native Security Offerings

Investigate/Consider 3rd Party Services

Don’t Compromise…Your Adversaries Won’t!

Wrap Up and Recommendations

There are several key principles that should underlie any cloud security architecture:

Advanced security for networks, as well as data, compute, messaging, and identity attack vectors.

Systematic separation of all traffic flows (to, from, and within cloud environments).

Segmentation by application or service and micro-segmentation of hosts running within the same segment or remotely.

Cultivating agility for DevOps and lines of business without compromising the corporate security posture.

Automation, efficiency, and elasticity in order to keep up with the velocity of business, while reducing risky human errors and misconfigurations by embedding security into code.

A platform-agnostic, borderless architecture in which security policies can be enforced consistently across all environments.

Source: Check Point Software Cloud Security Blueprint 2.0

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Thank You!

Grant Asplund | Office of the CTO-Global Cloud Evangelist

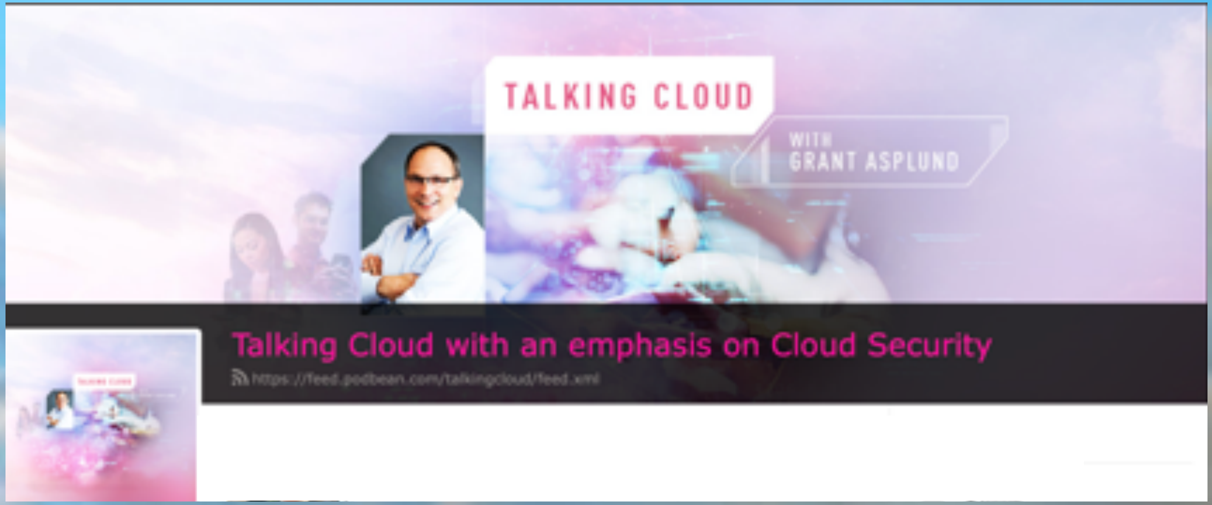
✉ grasplun@checkpoint.com | @gasplund | begranted

Check out my podcast…

TalkingCloud

https://talkingcloud.podbean.com

Listen and Subscribe Today!



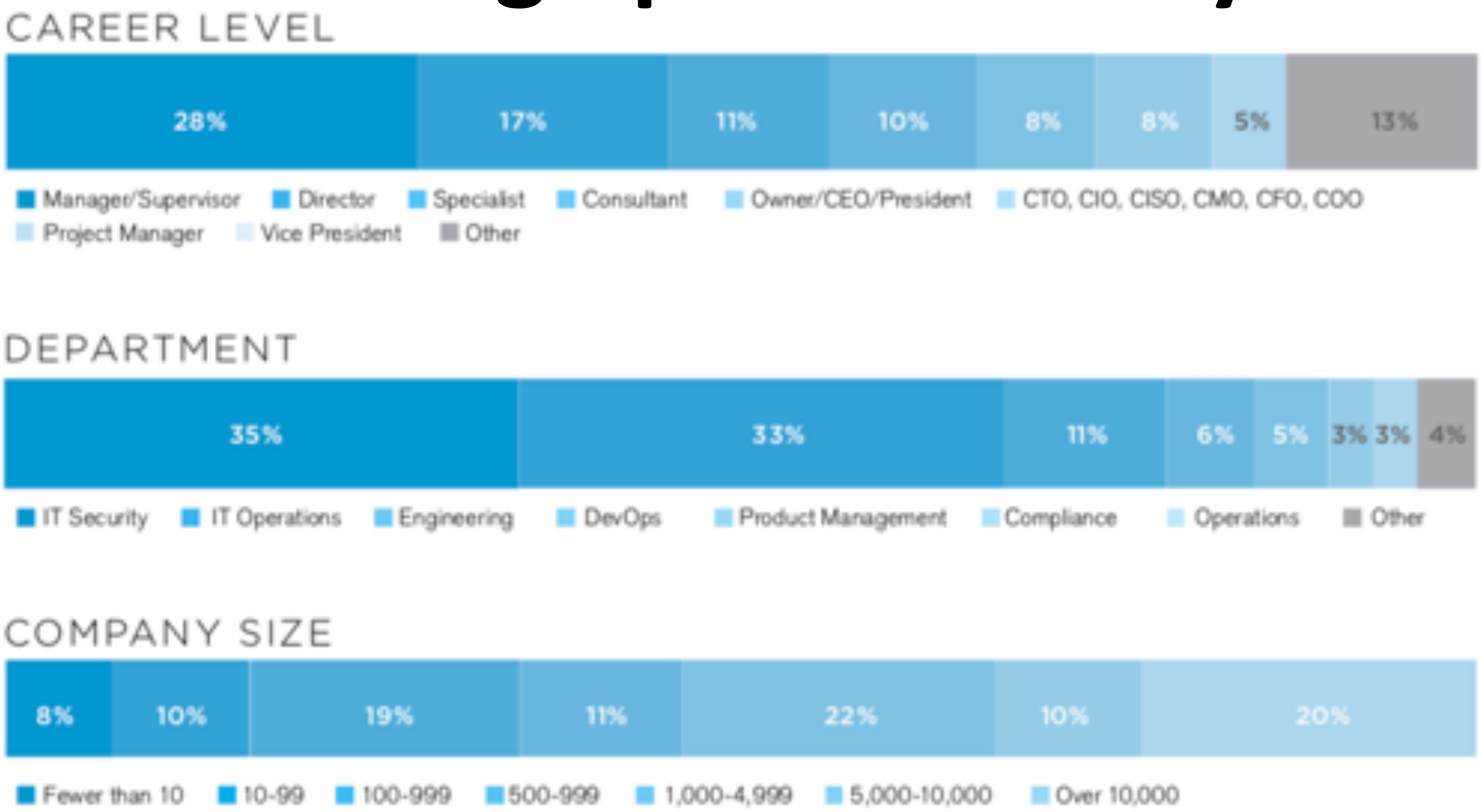
Talking Cloud with an emphasis on Cloud Security

https://feed.podbean.com/talkingcloud/feed.xml

Listen on

Listen on

Demographics Of Study



CAREER LEVEL

DEPARTMENT

COMPANY SIZE

Check Point®
SOFTWARE TECHNOLOGIES LTD.