HEY! YOU! GET OFF MY CLOUD!

ATTACKS AGAINST CLOUD HONEYPOTS

Martin Lee
Neil Rankin

ALERT LOGIC

Cloud Adoption

Choose two:

Fast

Cheap

Good

Cloud Models

Public

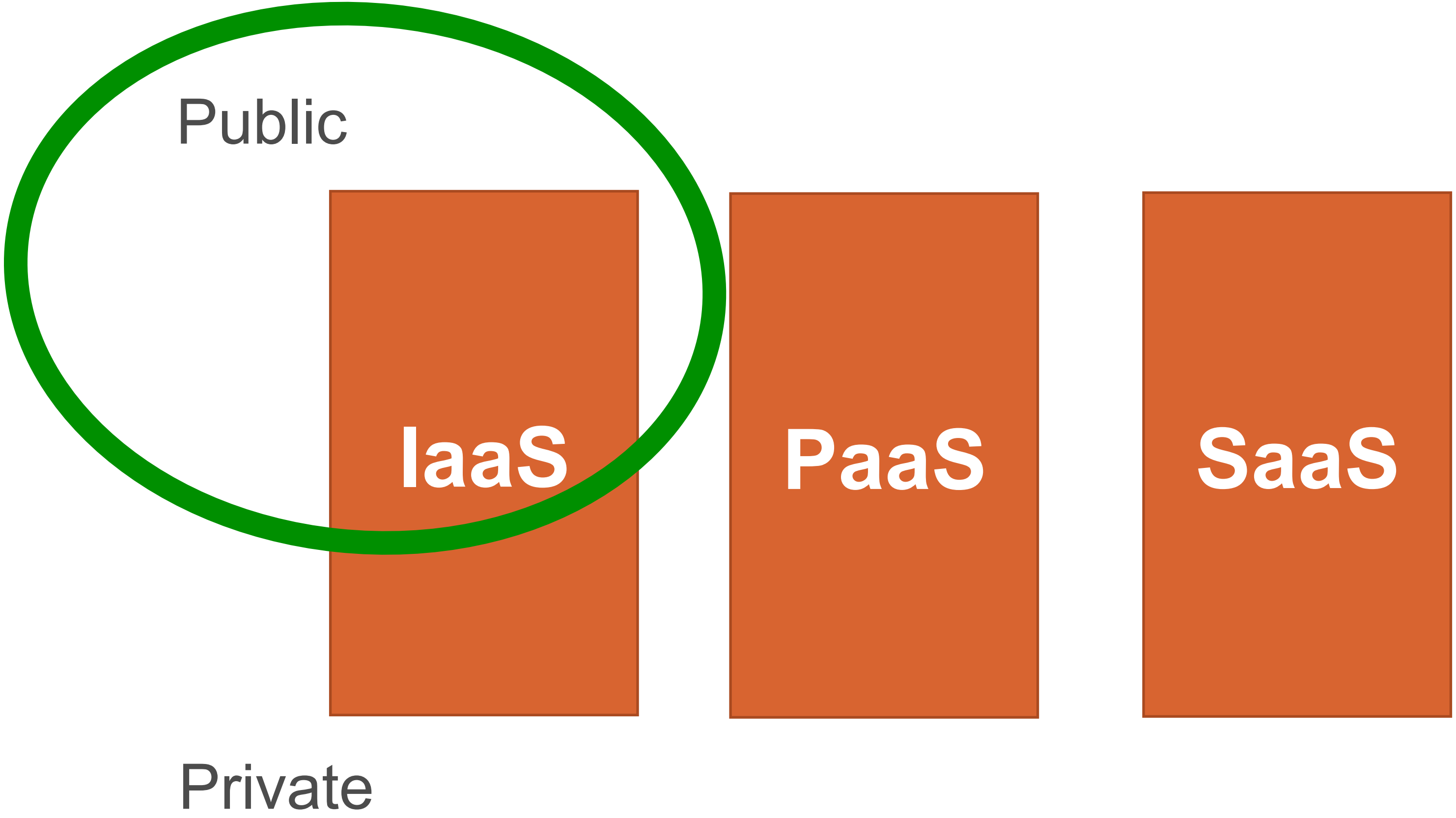
IaaS

PaaS

SaaS

Private

Cloud Models



Public

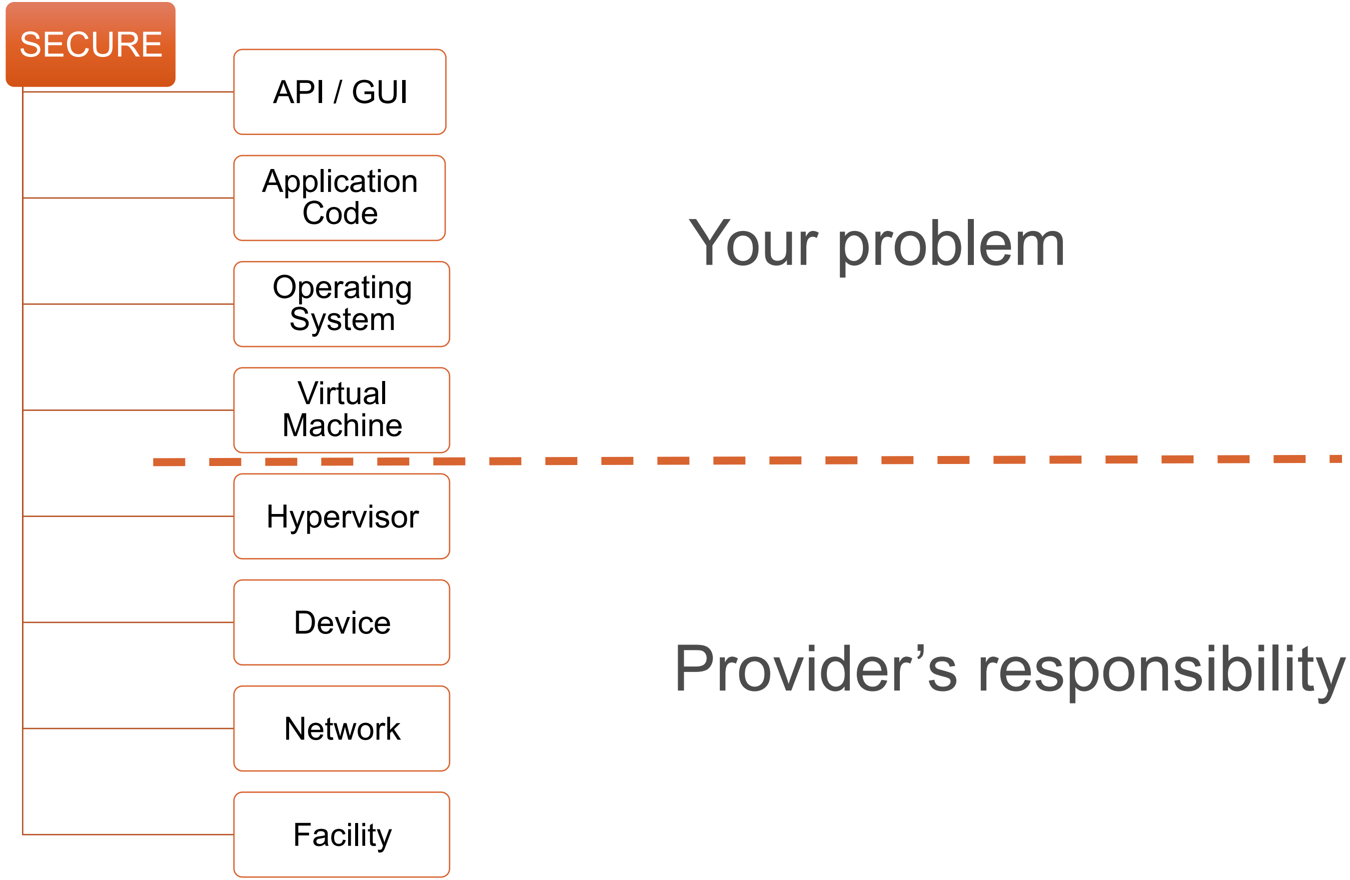
IaaS

PaaS

SaaS

Private

IaaS Cloud Security Layers



SECURE

API / GUI

Application Code

Operating System

Virtual Machine

Hypervisor

Device

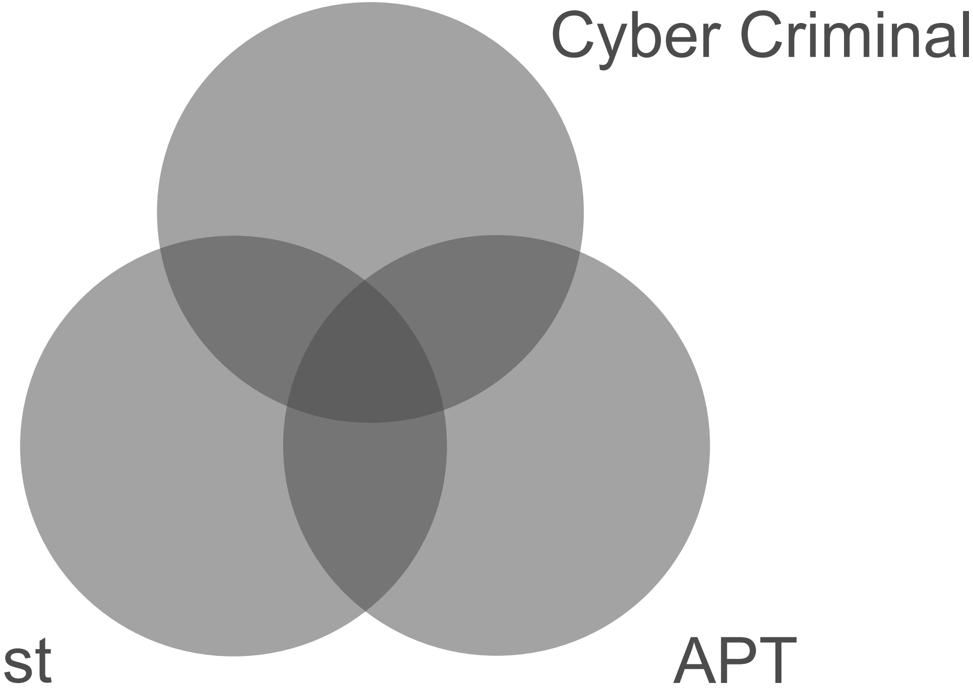
Network

Facility

Your problem

Provider’s responsibility

Threat Model



Cyber Criminal

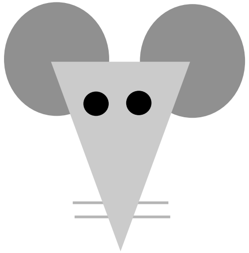
Hacktivist

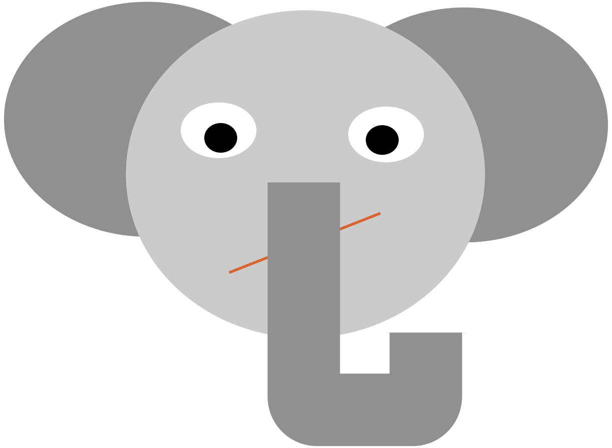
APT

ALERT LOGIC®

Elastic Computing

Development → Deployment

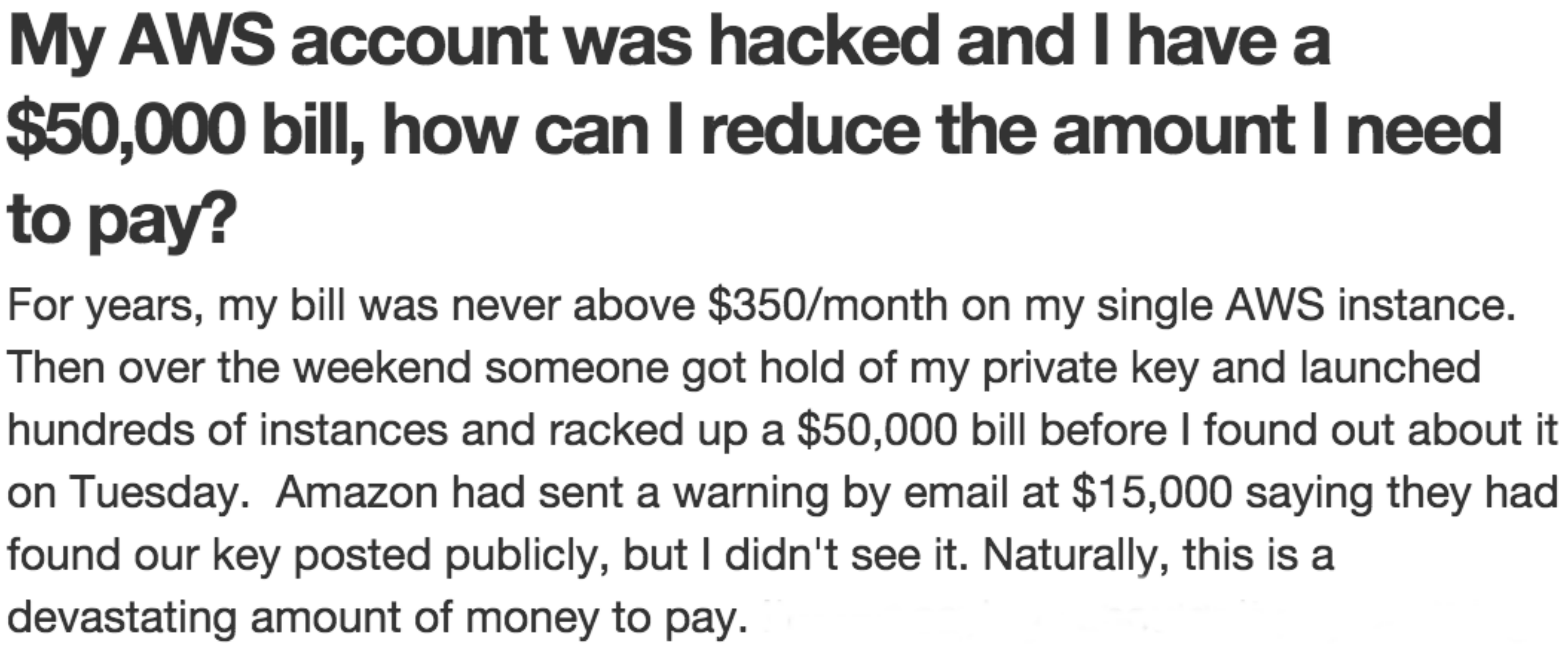




Low utilisation
Low cost

Heavy utilisation
High cost

Elastic Computing



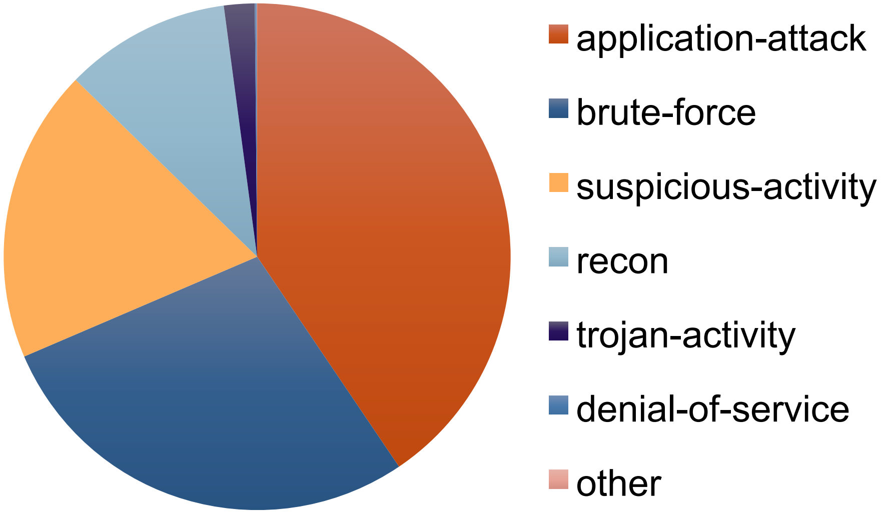
My AWS account was hacked and I have a $50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above $350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a $50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at $15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay.

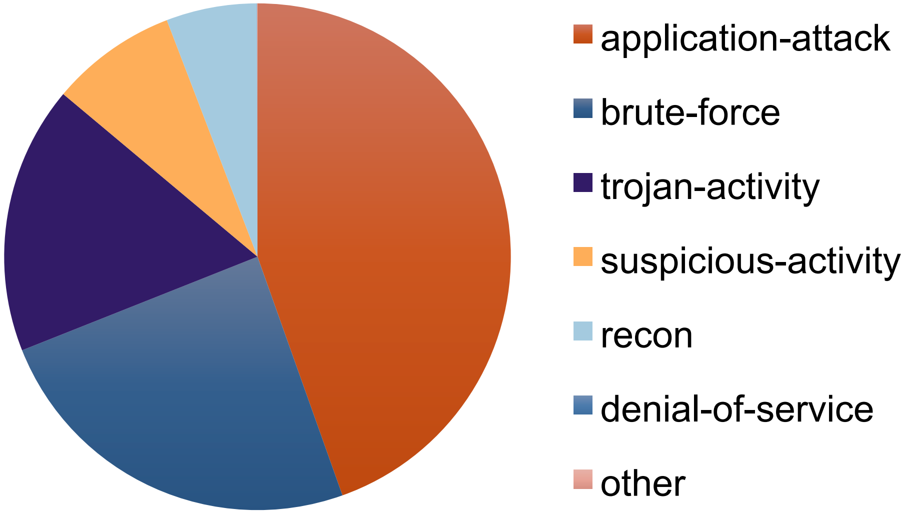
Source: Quora.com

Threat Types - Customers

Cloud Environment



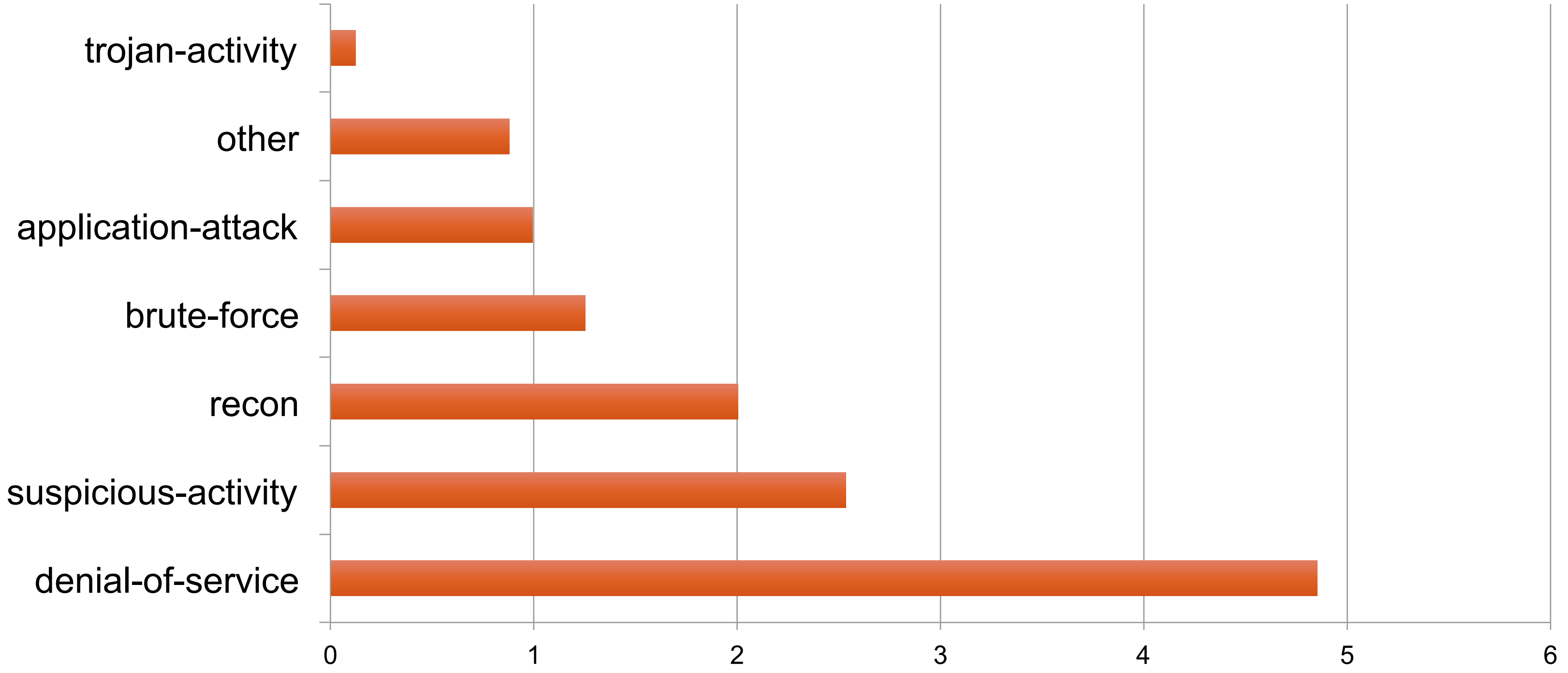
On Premise Environment



Source: Alert Logic ASR 2015

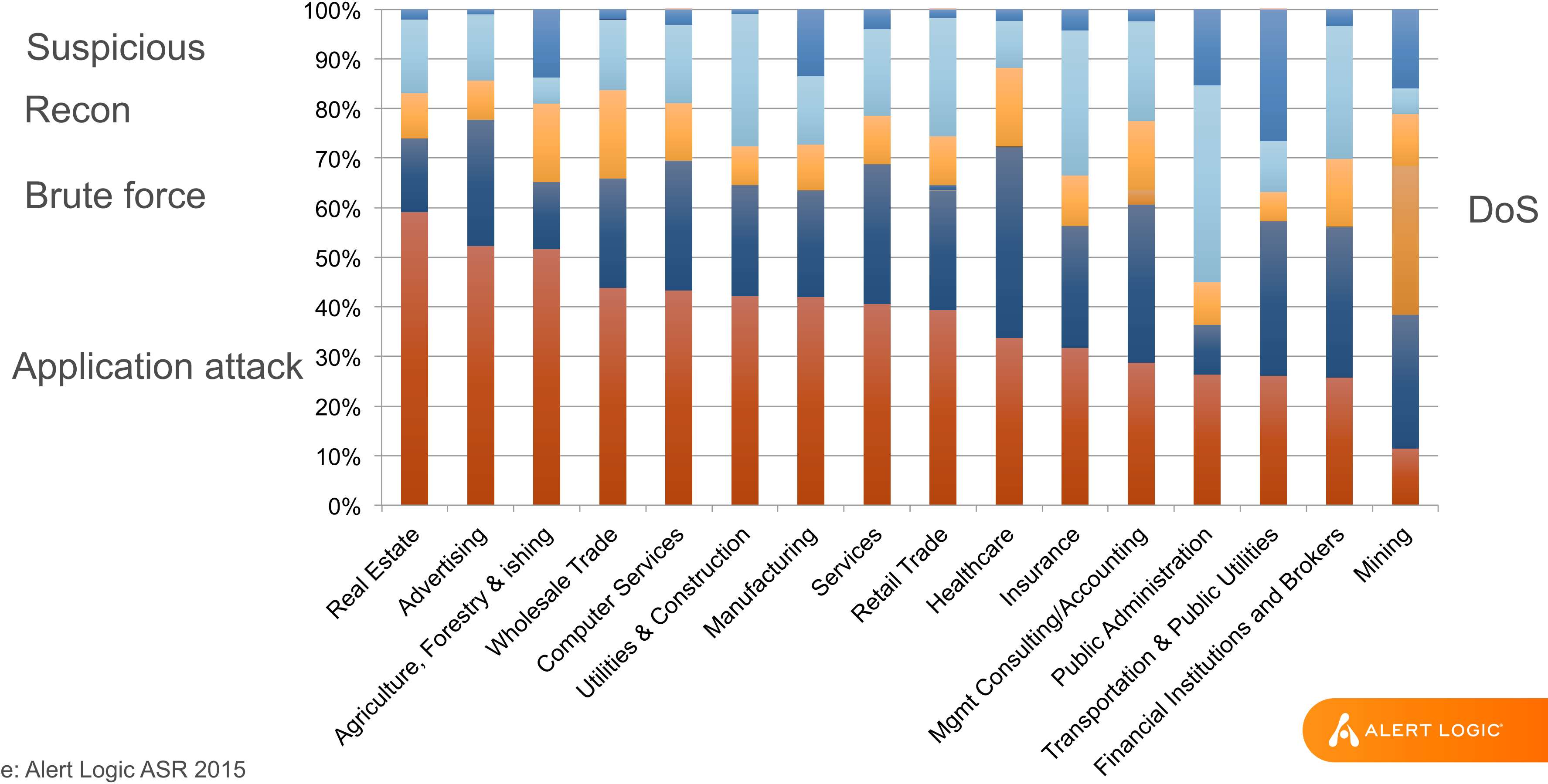
ALERT LOGIC®

Relative Threats - Cloud vs On Premise



Source: Alert Logic ASR 2015

Cloud Threats by Customer Industry Vertical



Source: Alert Logic ASR 2015

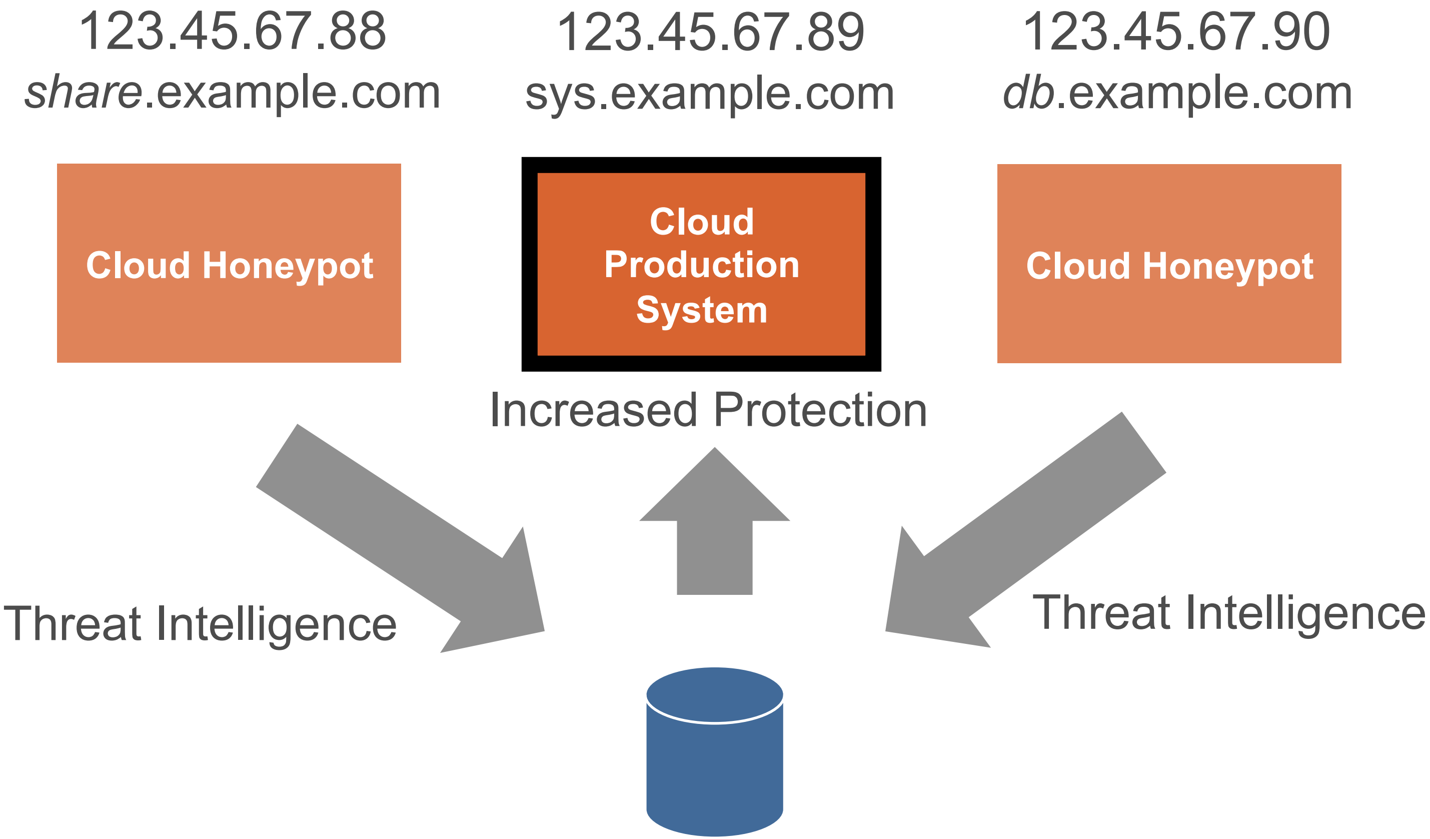
ALERT LOGIC®

Subtle Differences

Cloud threats ≠ On premise threats

Your threats ≠ Your neighbour’s threats

Honeypot Infrastructure



123.45.67.88
share.example.com

Cloud Honeypot

123.45.67.89
sys.example.com

Cloud Production System

Increased Protection

123.45.67.90
db.example.com

Cloud Honeypot

Threat Intelligence

Threat Intelligence

Honeypot Types

Low Interaction

- Simulates high level services
- Collects basic information

Medium Interaction

- Simulates generic functions
- Records interaction

High Interaction

- Simulates specific environment
- Collects details of attack

Medium Interaction

Kippo – medium interaction

https://github.com/desaster/kippo

- Simulates SSH shell
- Fake file system
- Easily detected! – we use heavily modified version
- We used to log brute force attacks & replay session

Medium Interaction

Dionaea – medium interaction

http://dionaea.carnivore.it/

- Simulates network services
- SMB / HTTP / FTP / MySQL / SIP (VOIP)
- Simulates shellcode execution
- We see mostly SMB activity

Low Interaction

Amun – low interaction

http://amunhoney.sourceforge.net/

- Modular Honeypot
- Simulates vulnerable services
- We see mostly SMB activity

Low Interaction

p0f – low interaction

http://amunhoney.sourceforge.net/

- Fingerprint connecting IPs
- Run in tandem

Custom Interaction

Create your own

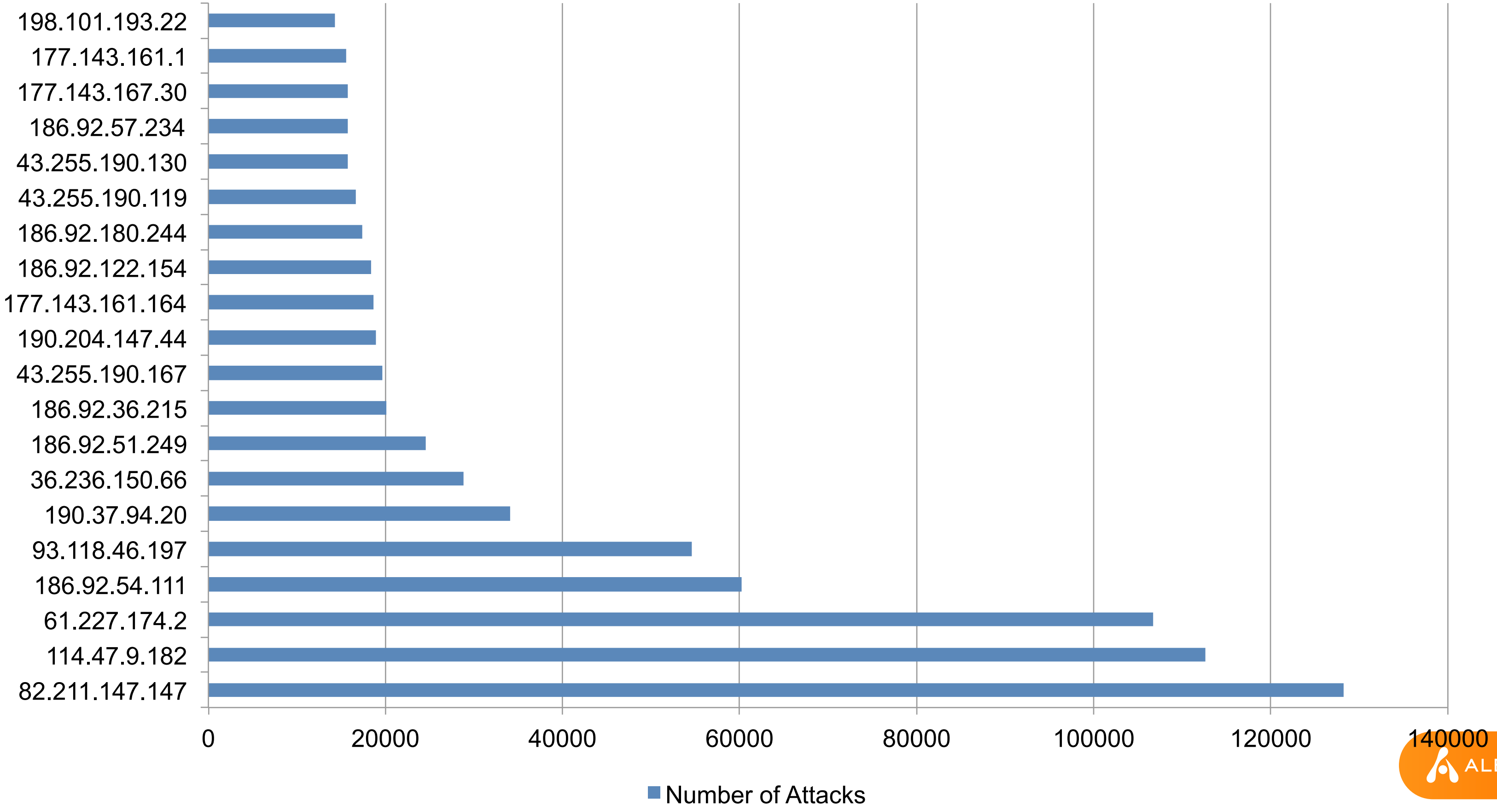
- Modify modular honeypot
- Reflect your environment
- Respond to new threats
- Research attacks against specific vulnerabilities

Results

What do we find?

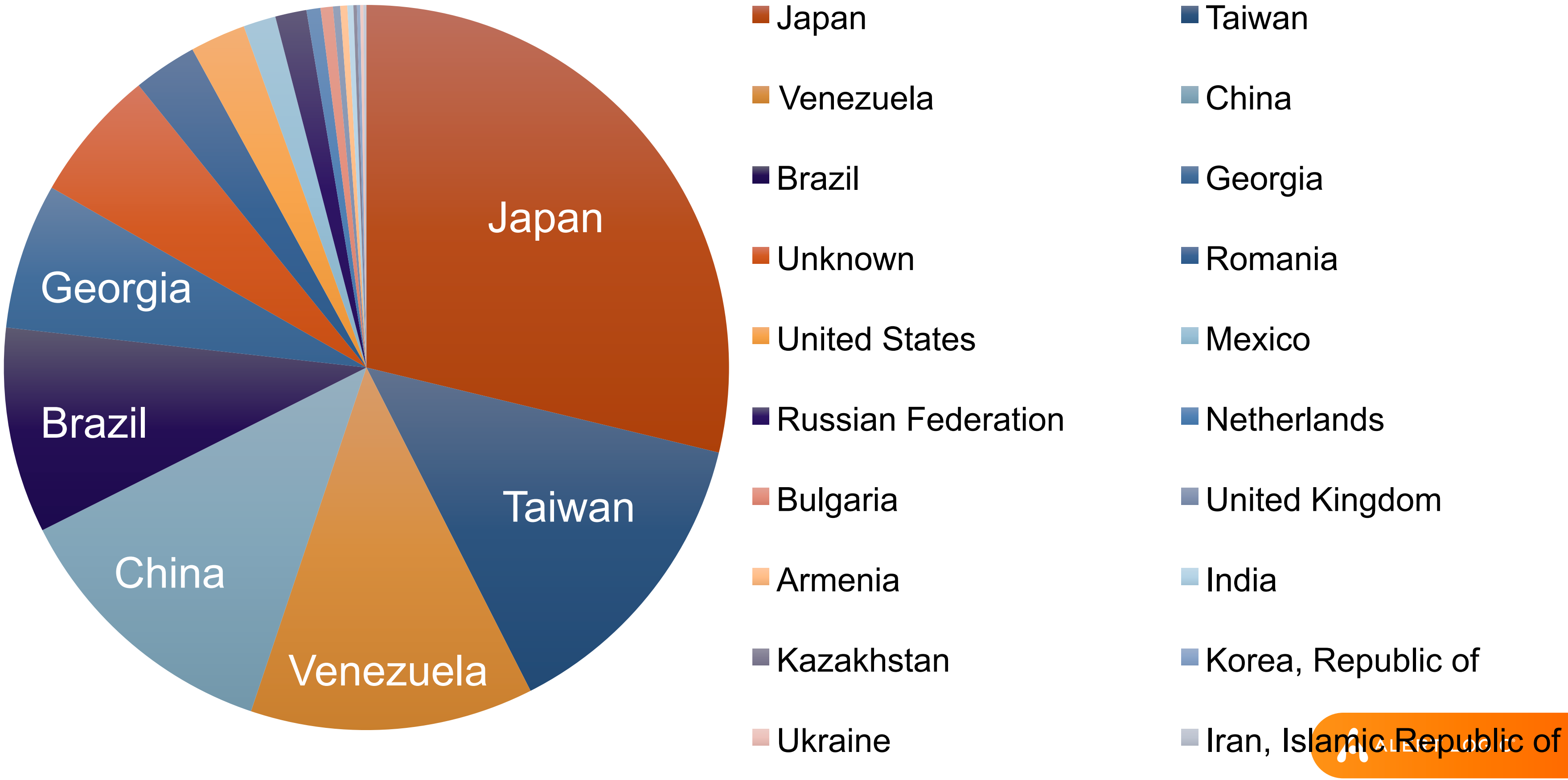
April 2015

Findings – Top 20 IP Addresses

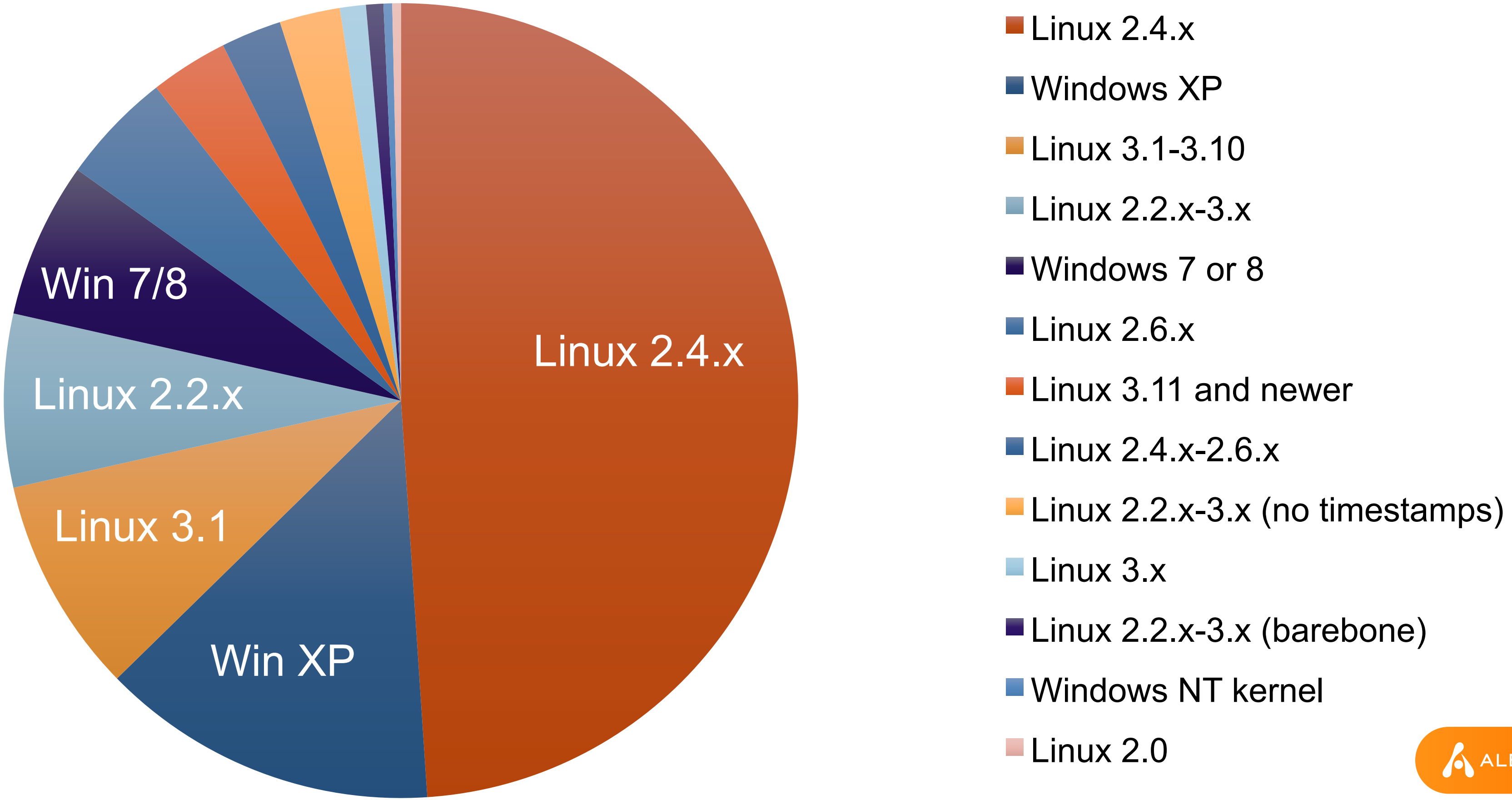


ALERT LOGIC®

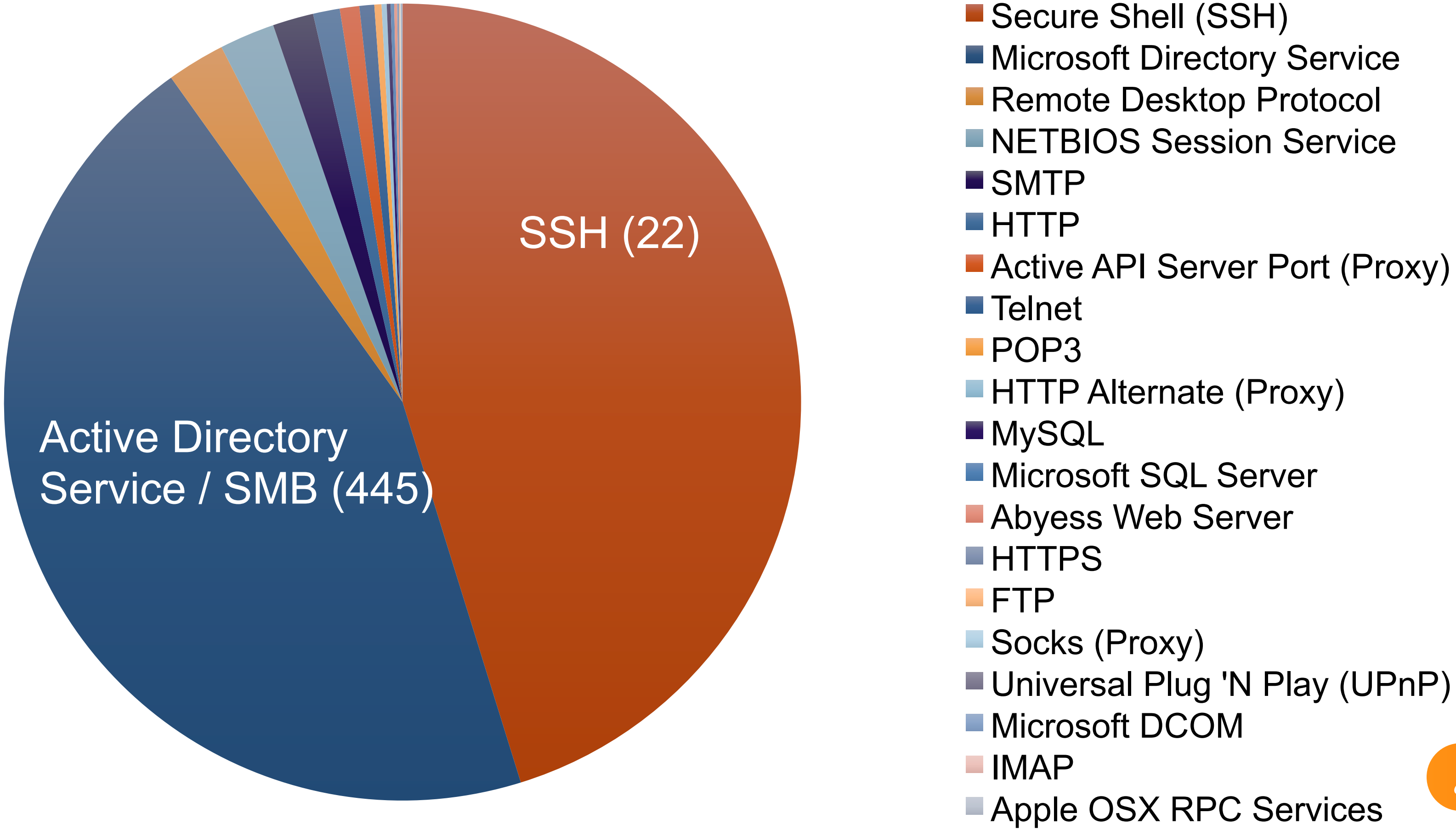
Findings – Top 20 Source Countries



Findings – Attacker OS

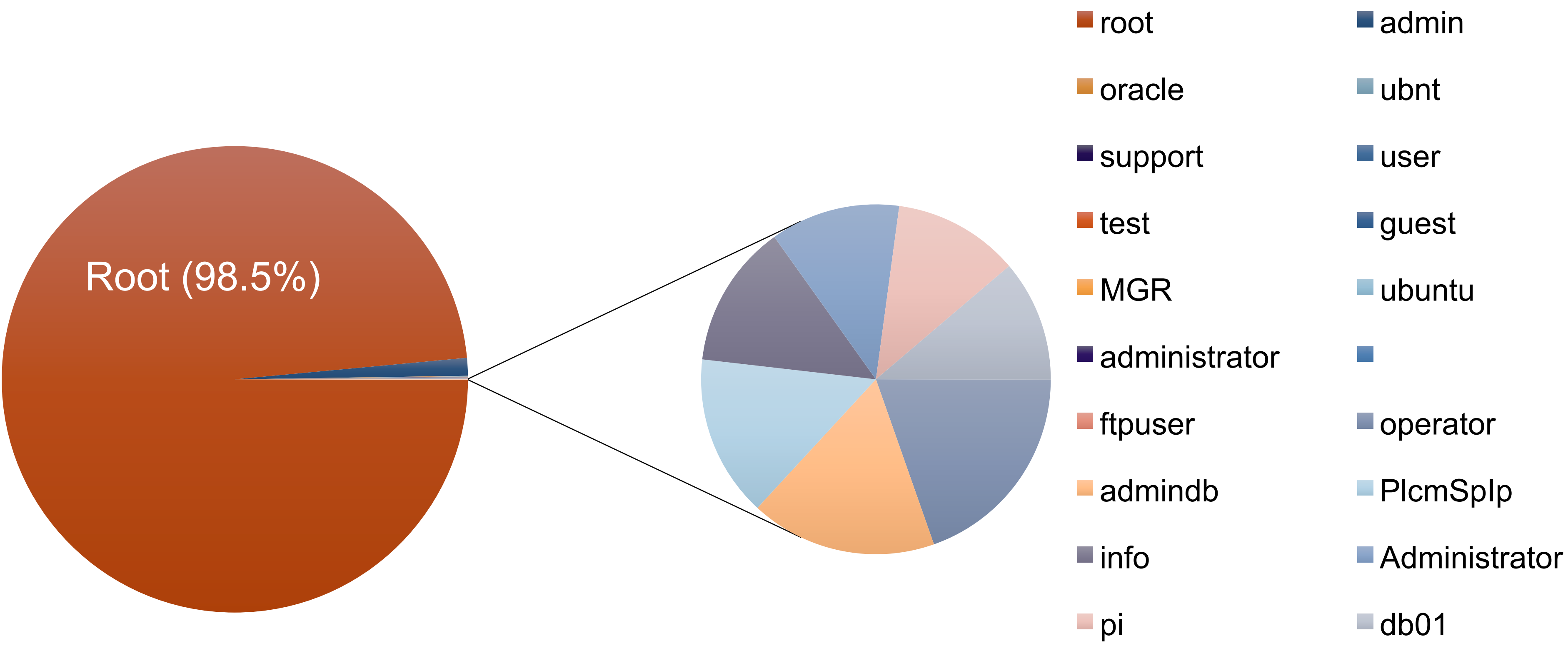


Findings – Top 20 Destination Ports



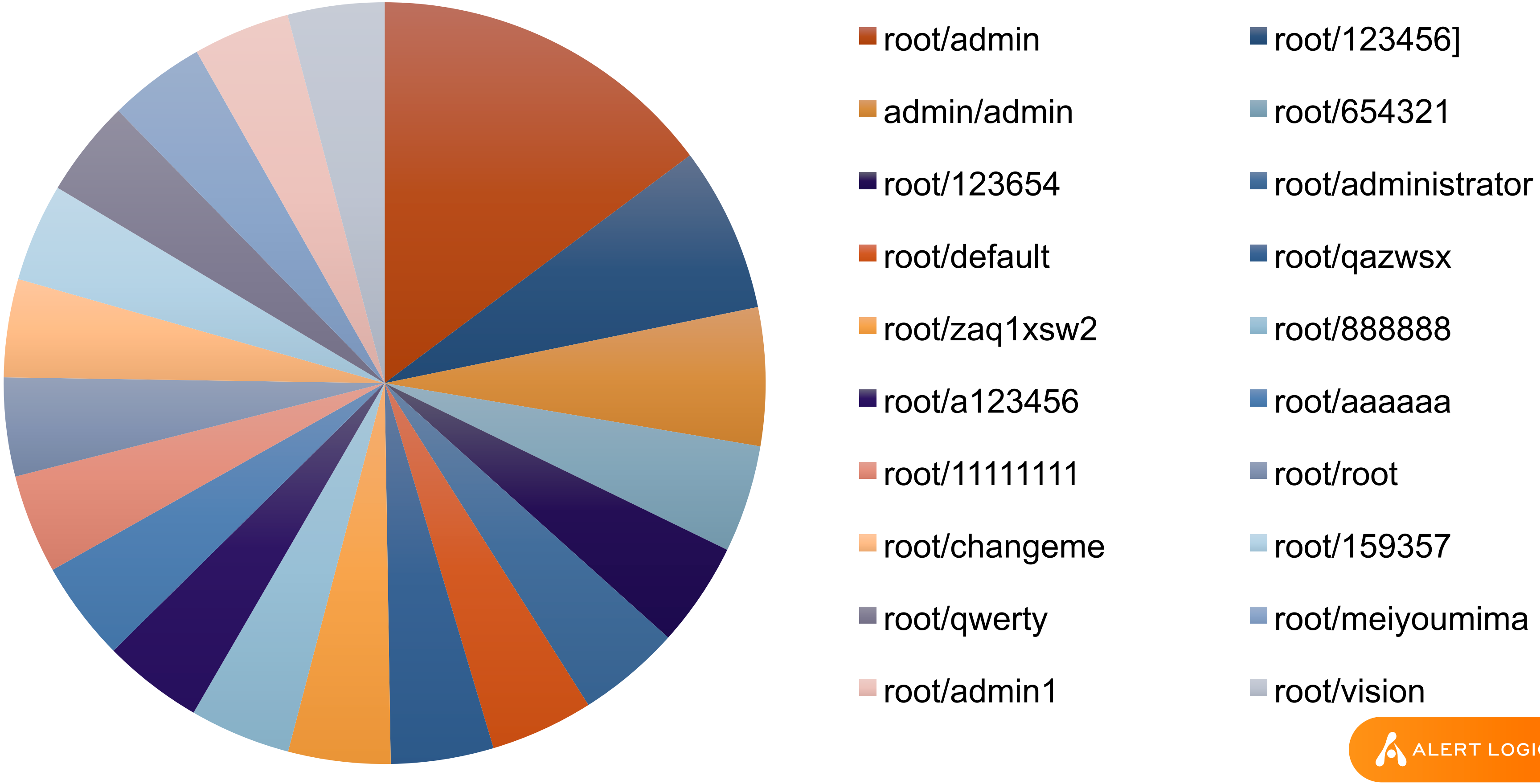
ALERT LOGIC®

Findings – Top 20 Brute Forced Usernames

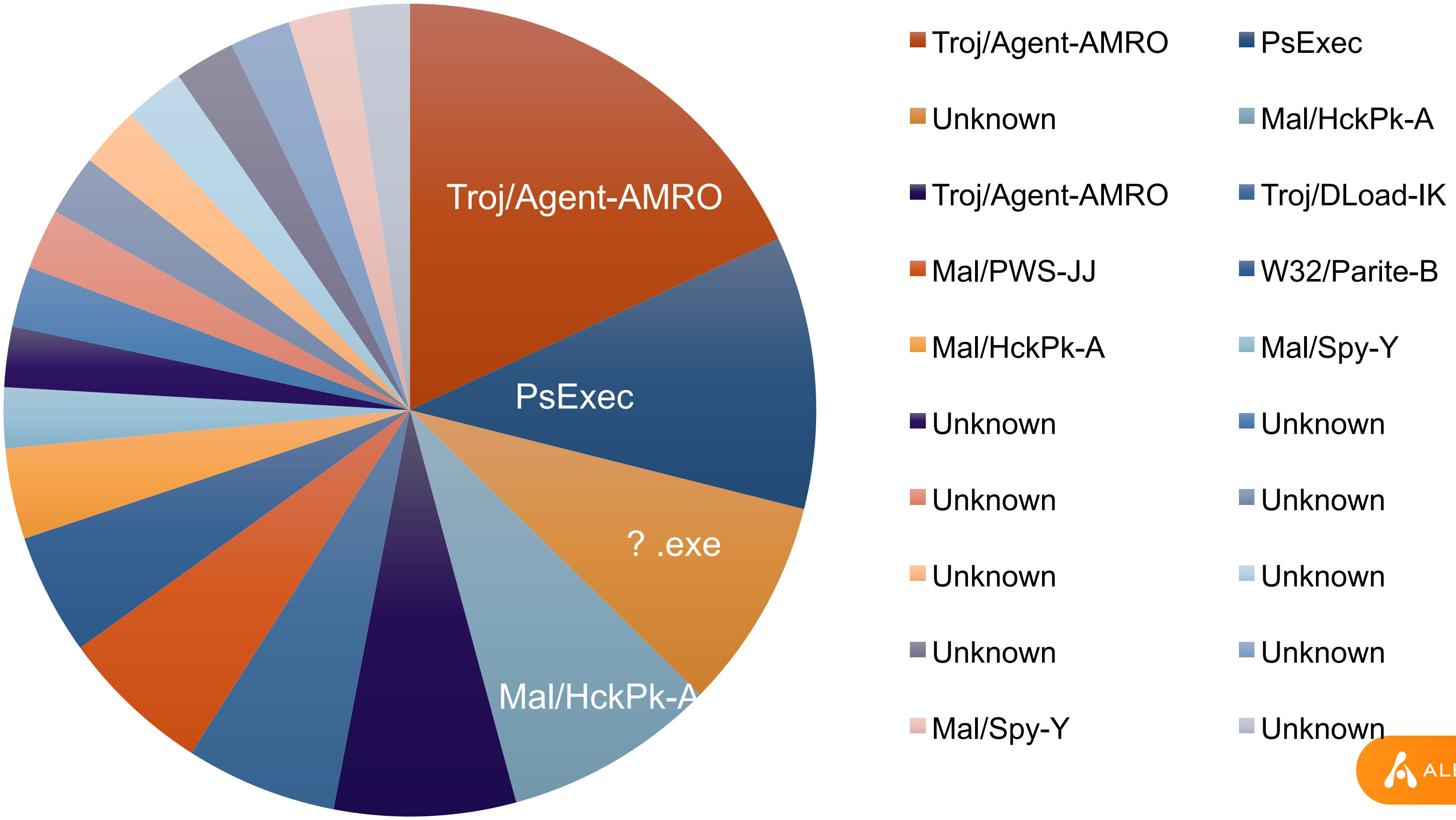


ALERT LOGIC®

Findings – Top 20 Brute Forced Username/Password



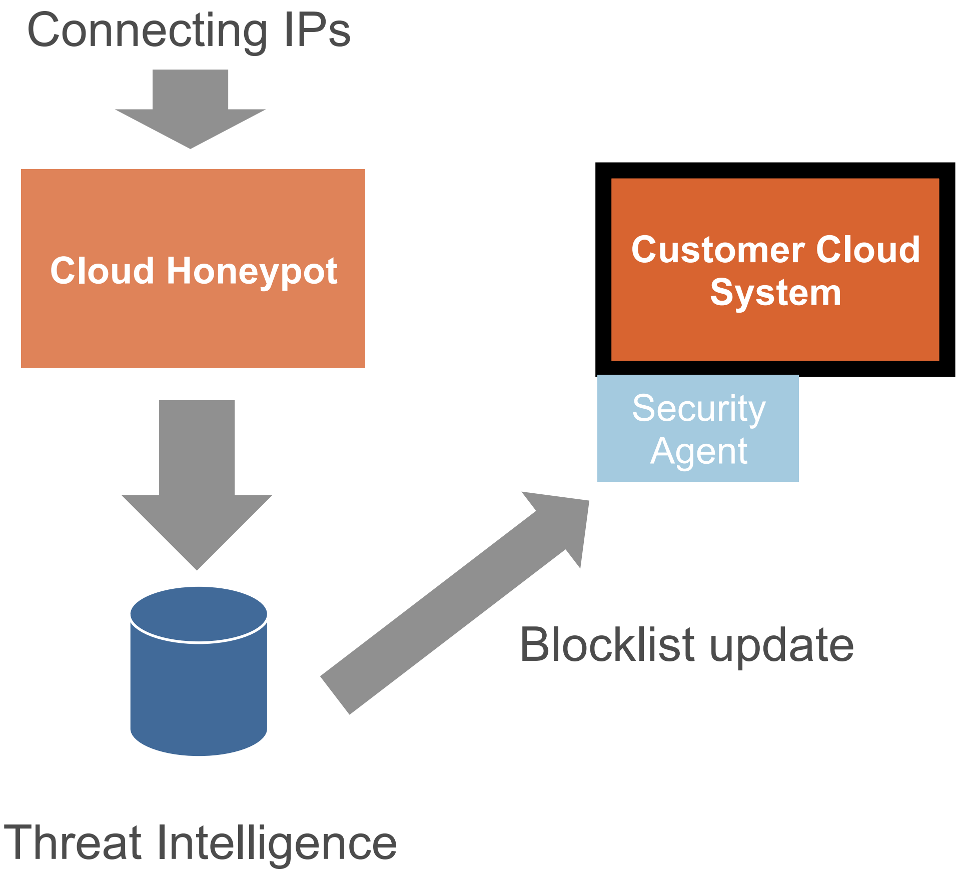
Findings – Top 20 Uploads



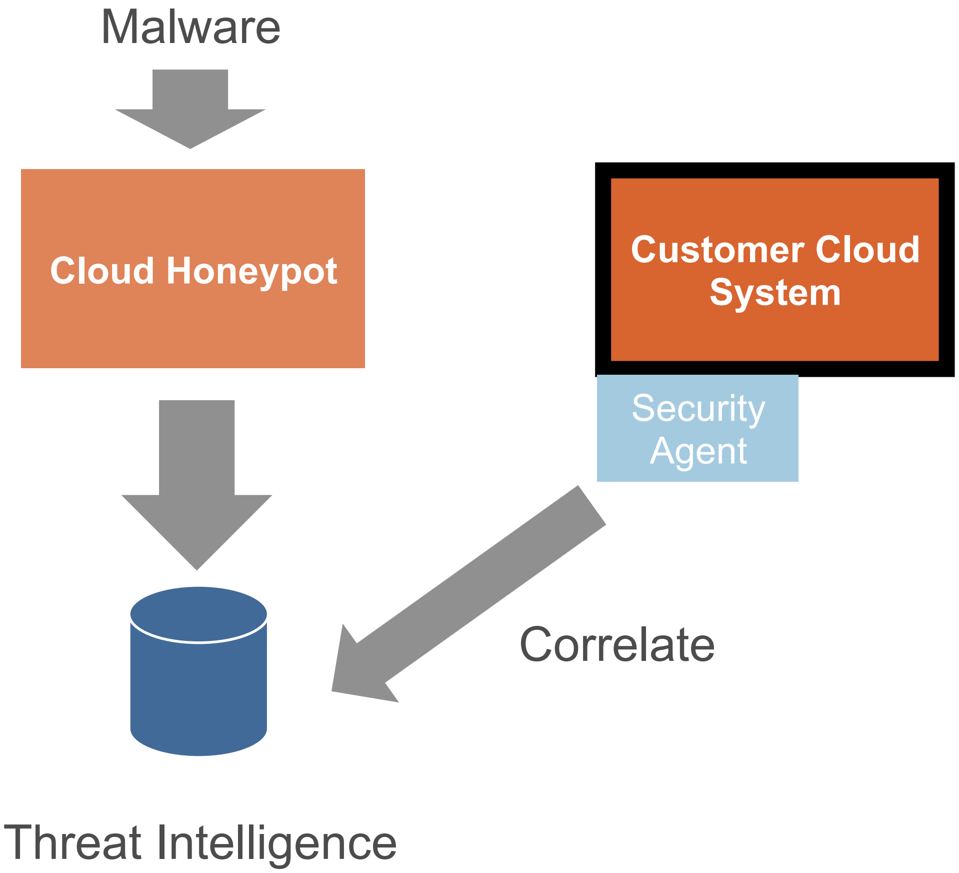
Deployment

Honeypots in Operation

Honeypots for Managed Services



Honeypots for Managed Services



Conclusion

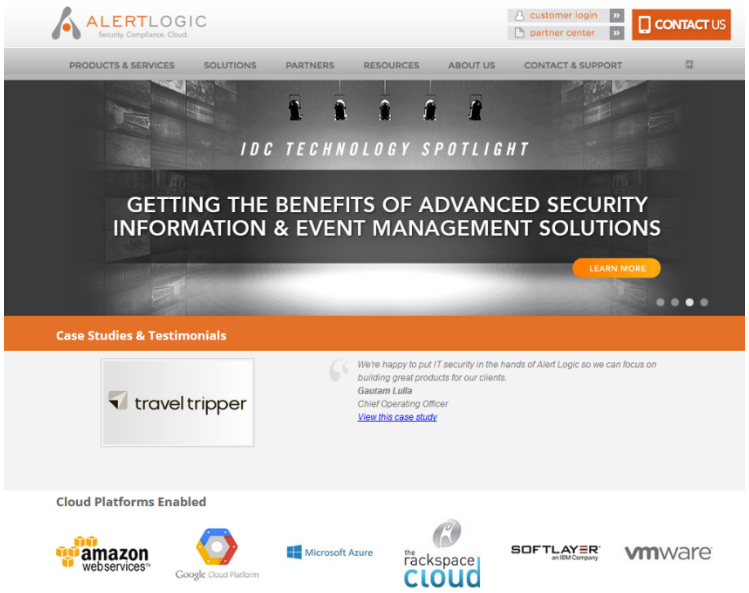
Cloud environments have a specific threat profile.

Well placed honeypots provide timely intelligence.

Apply intelligence to protect production systems.

Get Connected

www.alertlogic.com



IDC TECHNOLOGY SPOTLIGHT

GETTING THE BENEFITS OF ADVANCED SECURITY INFORMATION & EVENT MANAGEMENT SOLUTIONS

Case Studies & Testimonials

We're happy to put IT security in the hands of Alert Logic so we can focus on building great products for our clients.
Gautam Lulla
Chief Operating Officer
View this case study

Cloud Platforms Enabled

@alertlogic @mlee_security

linkedin.com/company/alert-logic

alertlogic.com/resources/blog/

youtube.com/user/AlertLogicTV

brighttalk.com/channel/11587

ALERT LOGIC®

Thank you

Will Semple – VP ActiveIntelligence

Brian Wilson – Director, Intelligence

Michael Laughlin – Tools Engineer

Thank you.

ALERT LOGIC®