StackPath

The Business of Internet Privacy & Security

Michael Marques
March 14, 2018

Cybersecurity is the practice of protecting systems, networks, programs, and data from digital attacks.

”Cybersecurity is one of the most serious economic and national security threats our nation faces.”

– President Barack Obama

“My message for companies that think they haven’t been attacked is: “You’re not looking hard enough”.

– James Snook

By the year 2020, we won’t recognize the cloud.

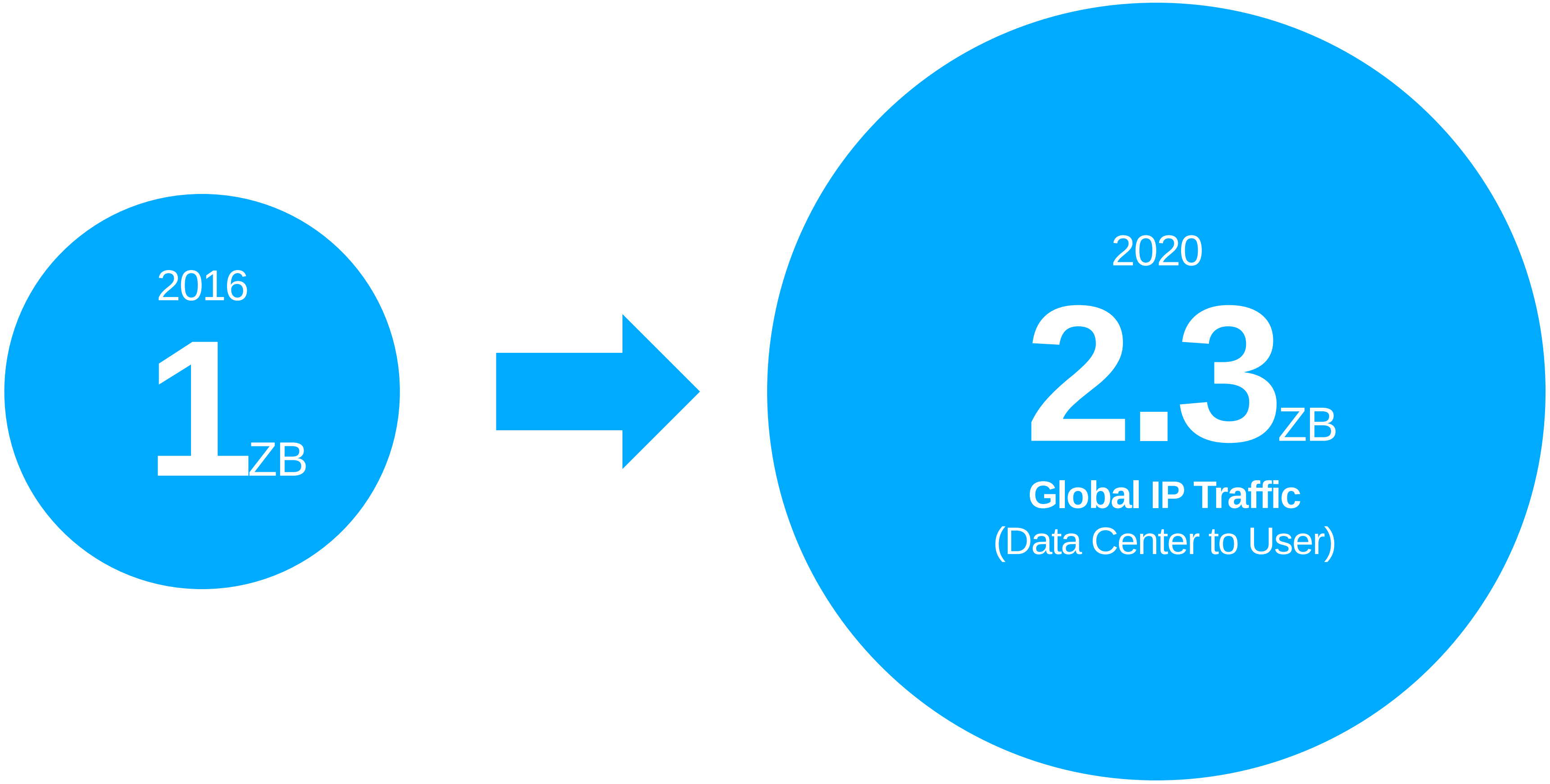
Global adoption of online Video

Proliferation of IoT devices

Exponential growth
in malicious activity

Radical evolution of edge services

One forecast says Internet traffic will have more than doubled.



2016

1ZB

2020

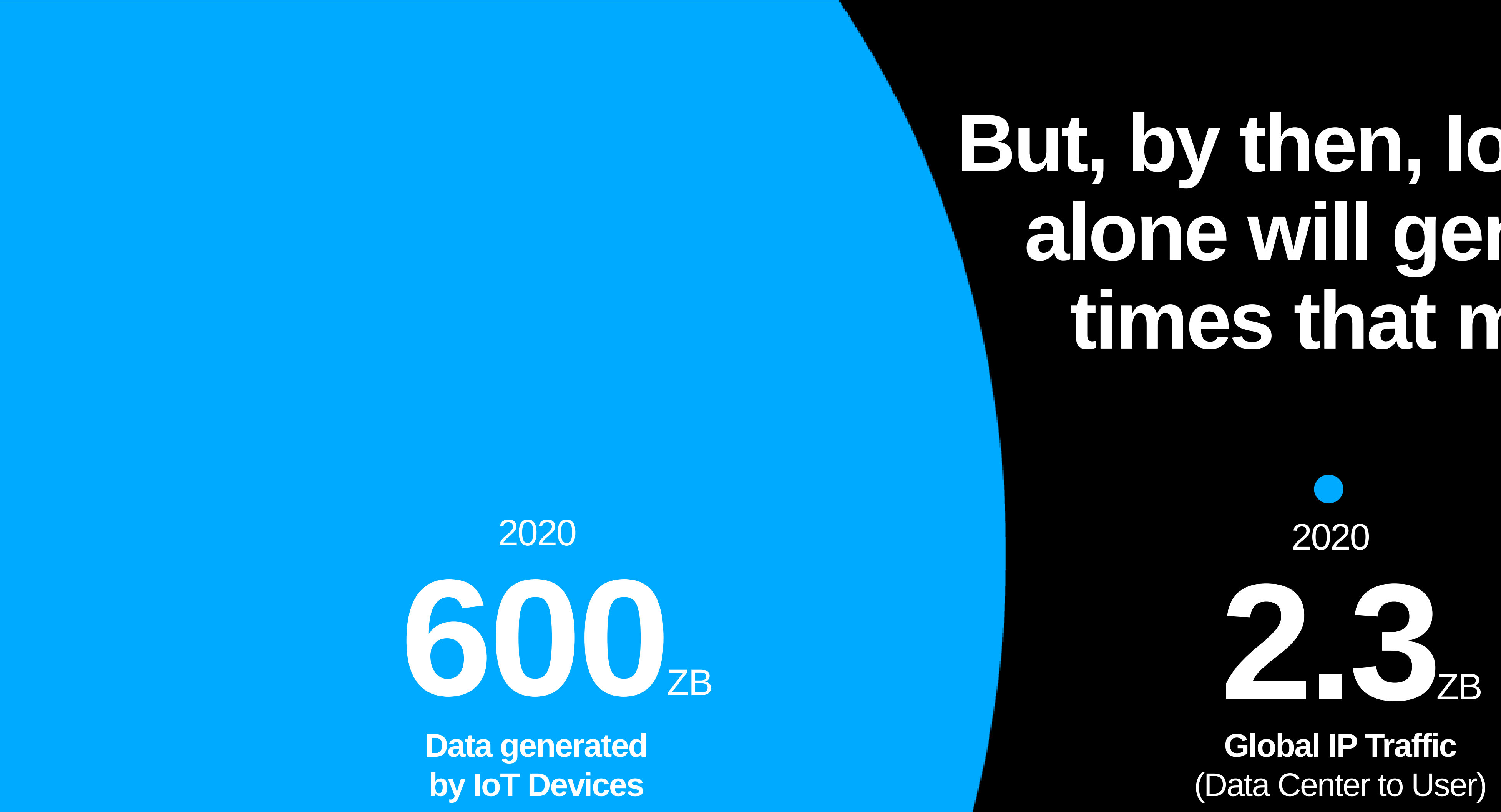
2.3ZB

Global IP Traffic

(Data Center to User)

Source: Cisco Global Cloud Index: Forecast and Methodology, 2015–2020

But, by then, IoT devices alone will generate 275 times that much data.



2020

600ZB

Data generated by IoT Devices

2020

2.3ZB

Global IP Traffic
(Data Center to User)

Source: Cisco Global Cloud Index: Forecast and Methodology, 2015–2020

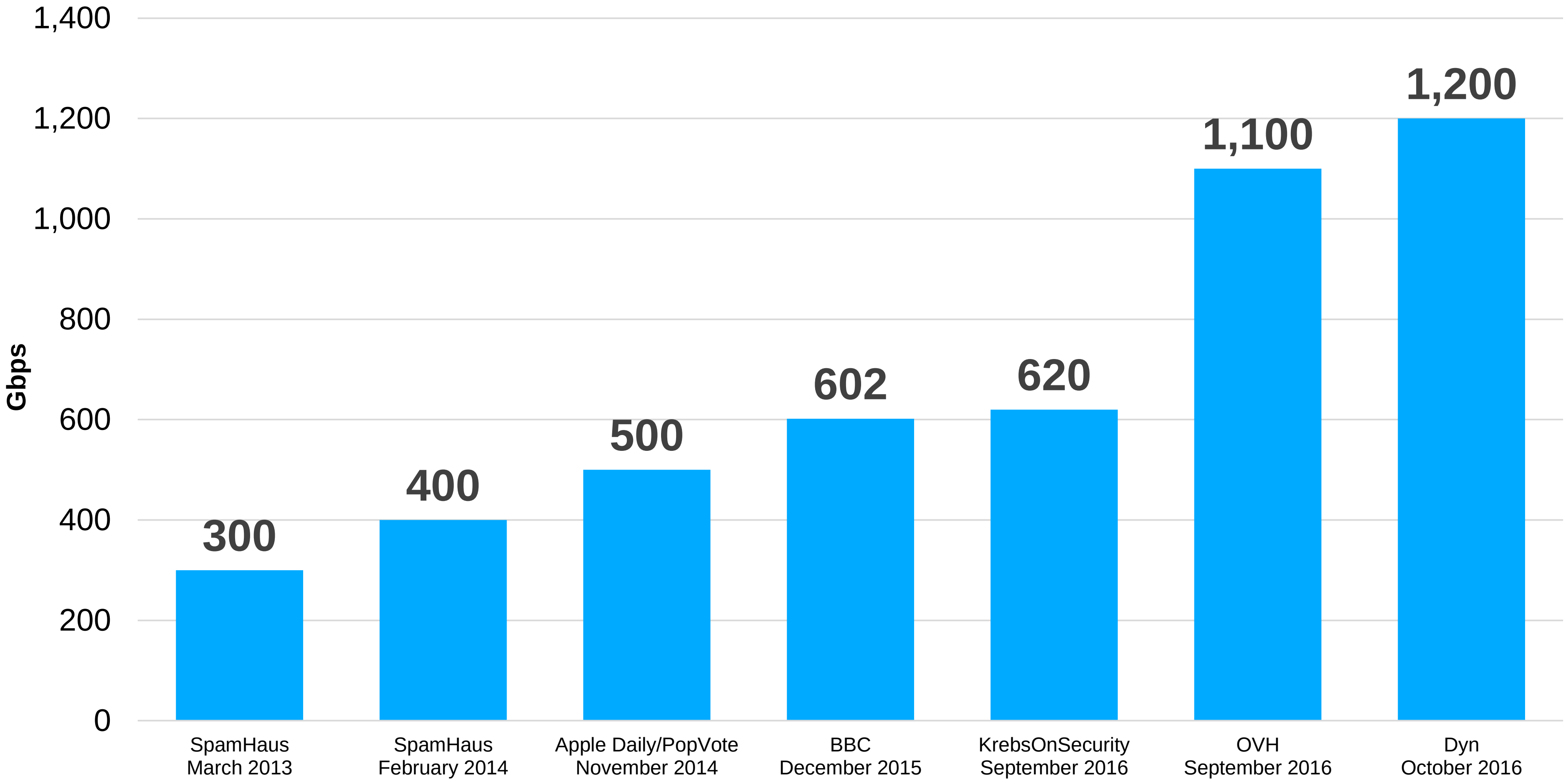
Meanwhile, malicious activity is more than keeping pace.

DDoS attacks are growing faster than ever.

2x
more DDoS attacks
<200Gbps
in 2016 than 2015

4x
more DDoS attacks
>200Gbps
in 2016 than 2015

135k
DDoS attacks/wk
on average from
7/15 to 12/16



Source: Active Threat Level Analysis System

Major companies regularly report large breaches.

2013
YAHOO!
3B user accounts

2014
micros®
500M account records

2014
ebay
145M user accounts

2014
THE HOME DEPOT
53M customer accounts

2016
UBER
57M user & driver records

2016
Wendy's
>1K restaurants

2016
Dropbox
68M user accounts

2017
ESEA
ESPORTSENTERTAINMENT
1.7M user accounts

2017
EQUIFAX®
143M consumer records

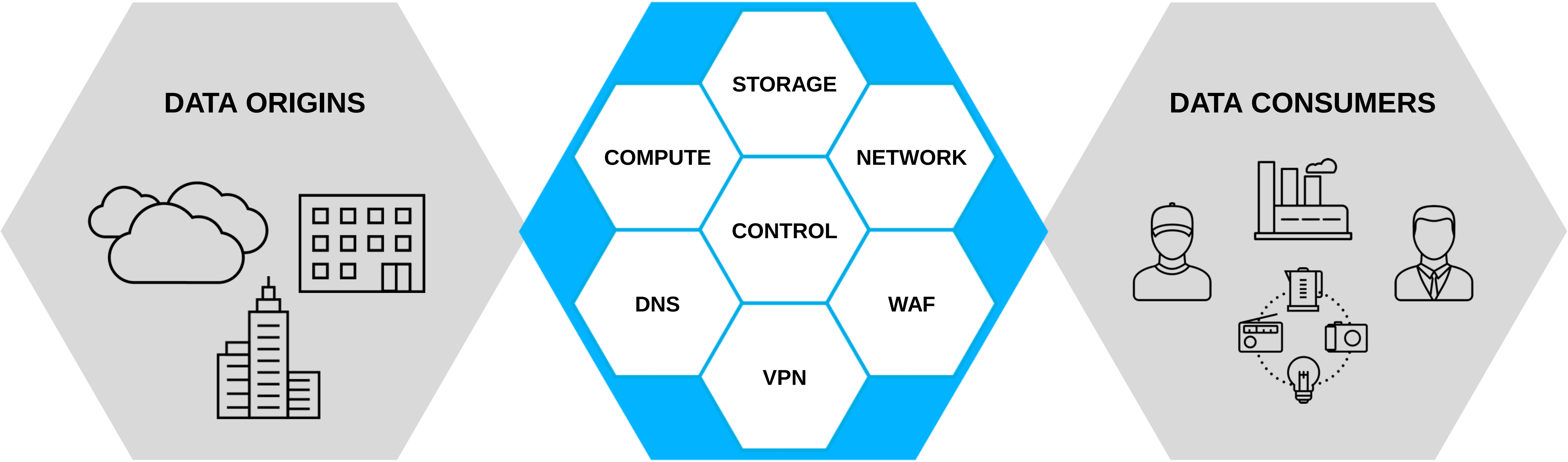
2017
dun & bradstreet
33M corporate contacts

2017
verizon✓
14M subscriber accounts

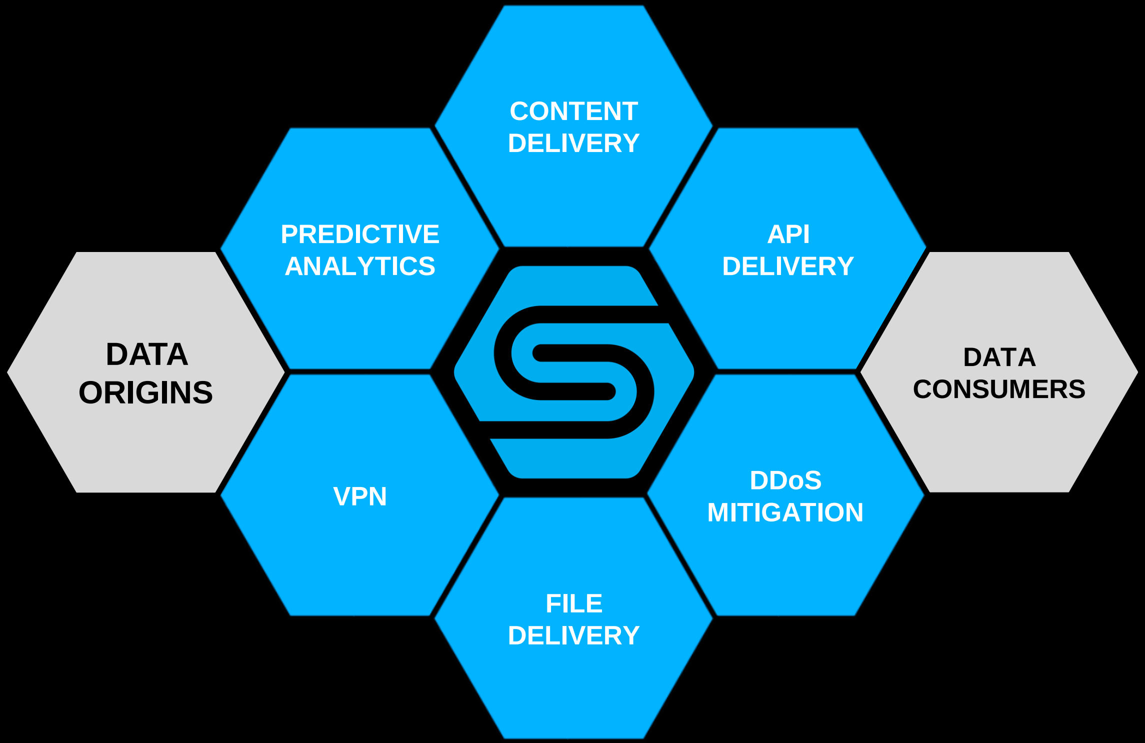
2017
alteryx
120M household records

StackPath is building a platform of secure services at the cloud’s edge.

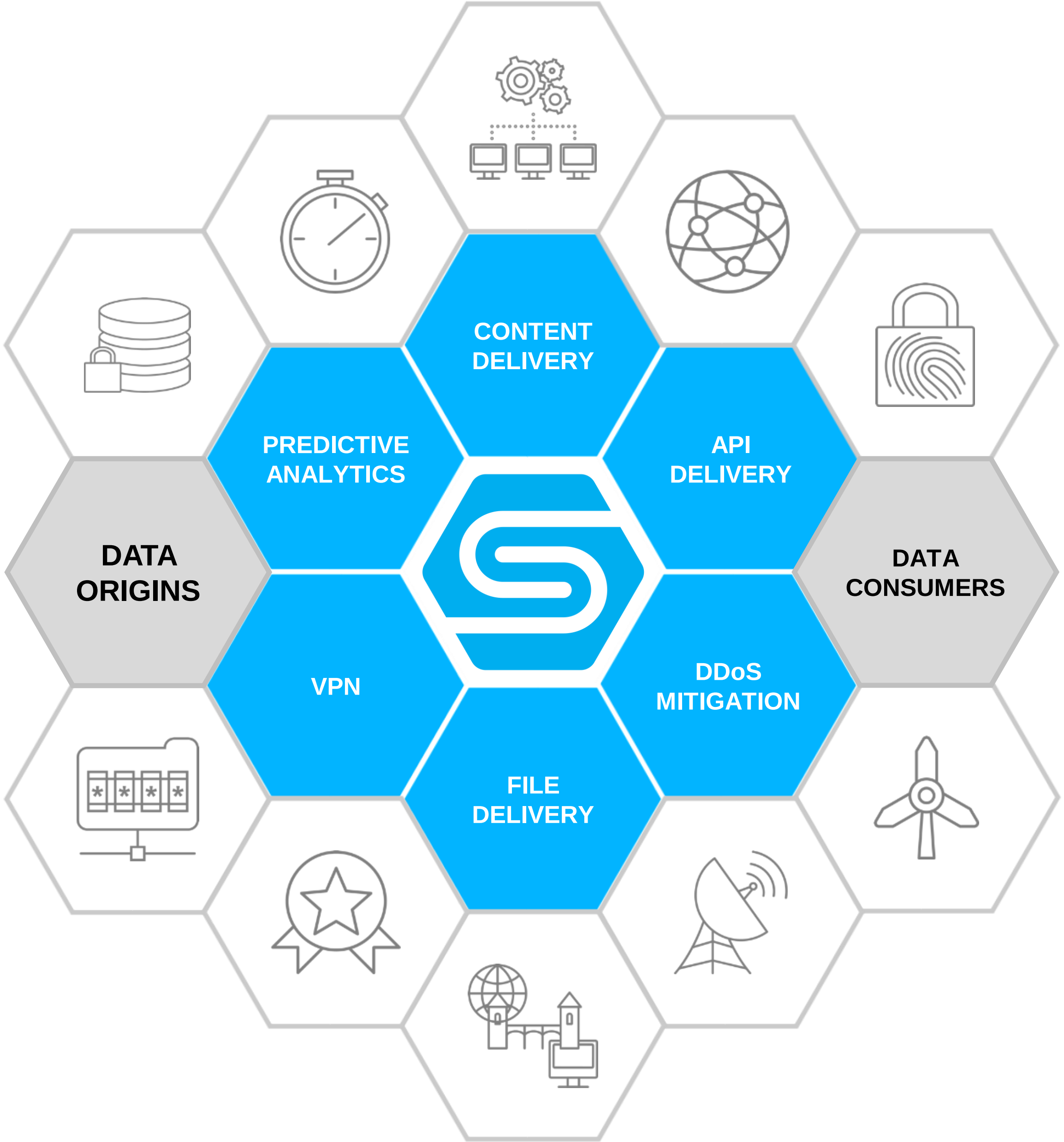
Its core is an advanced, global infrastructure designed and automated for cloud scale.



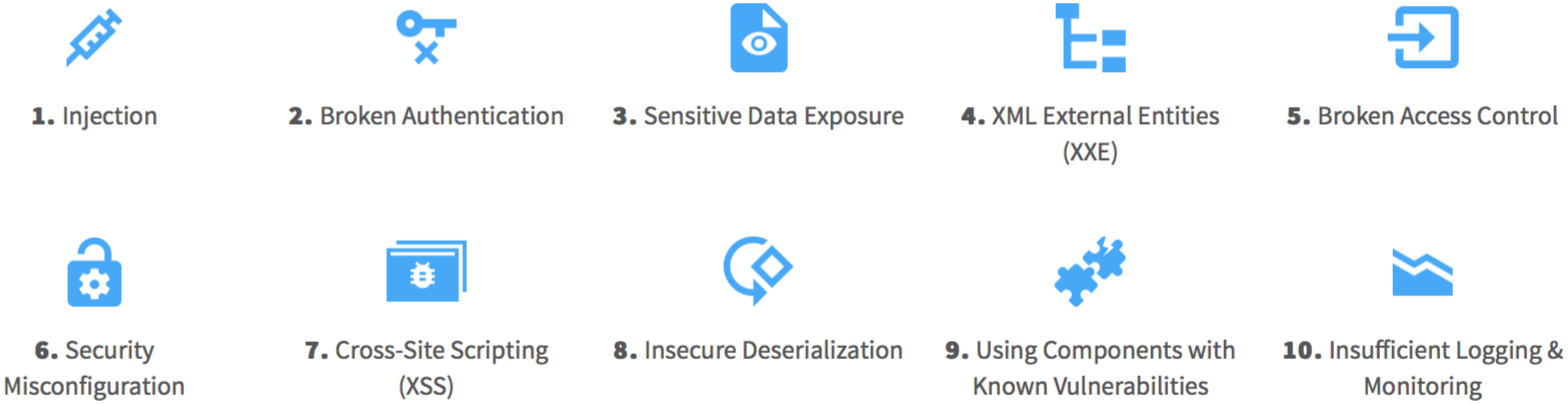
That infrastructure provides the foundation and building blocks with which we can deliver highly-secure edge services.



A multi-sided platform, ready for however the Internet grows and whatever we— or our customers— can innovate.



OWASP’s Top 10



1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Developers Should:

- Set goals and security requirements
- Design your security from the start
- Set frameworks & open sources
- Continue to learn
- Log and monitor

Everyone Should:

- Set up a VPN – Don’t trust unsecured or public Wi-Fi
- Use email encryption
- Set your account information to private
- Change your password and don’t use for multiple accounts
- Log out as soon as you’re done with a site
- Provide only the minimum amount of information required when creating an online account
- Have a credit card only for online purchases
- Monitor your accounts
- Keep your anti-virus software current
- Be smart – Don’t wire transfer money, send W2s, or help out a Saudi prince

RESOURCES

- StackPath: www.stackpath.com
- Homeland Security Stop. Think. Connect. Toolkit: https://www.dhs.gov/stopthinkconnect-toolkit
- National Cyber Security Alliance: https://staysafeonline.org/stay-safe-online/
- FDIC: https://www.fdic.gov/consumers/assistance/protection/idtheft.html
- Federal Trade Commission: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- Global Knowledge: https://www.globalknowledge.com/us-en/content/articles/10-ways-everyone-should-approach-cybersecurity/

StackPath

Thank you

Michael.marques@stackpath.com