radware
Every second counts

Attack Mitigation Business Landscape

Sources of Insight into the Threat Landscape

SOURCE #1

Security Industry Survey (Quantitative)

330 Respondents globally

33% **large organizations**
annual revenue +$500M US

40% of the organizations conduct **business worldwide**

23 Industri

Telecomm
Internet
Cloud se
20.42%

Financial
13.15%

Compute
or servic
12.11%

Manufac
Producti
Distribut
6.57%

SOURCE #2

utive Survey (Quantitative)

security officers each
m a different organization

epth interviews
xperiences with
ATTACKS

SOURCE #3

Emergency Response Team - Case Studies

24/7 TEAM

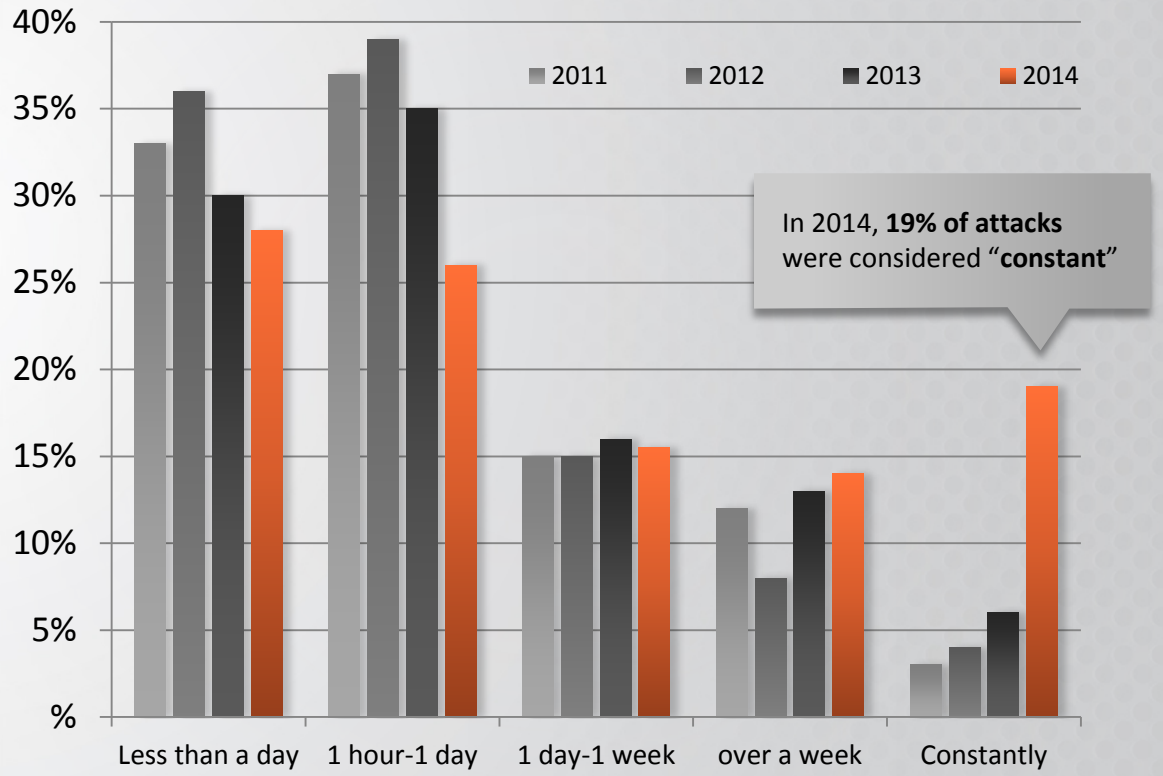
Team of security experts for fast mitigation under attack

Colombian Hackers | OpUsa | OpISRAEL | Boston's Children Hospital

The Rise of the Continuous Attack

Attack duration continues to evolve and expand

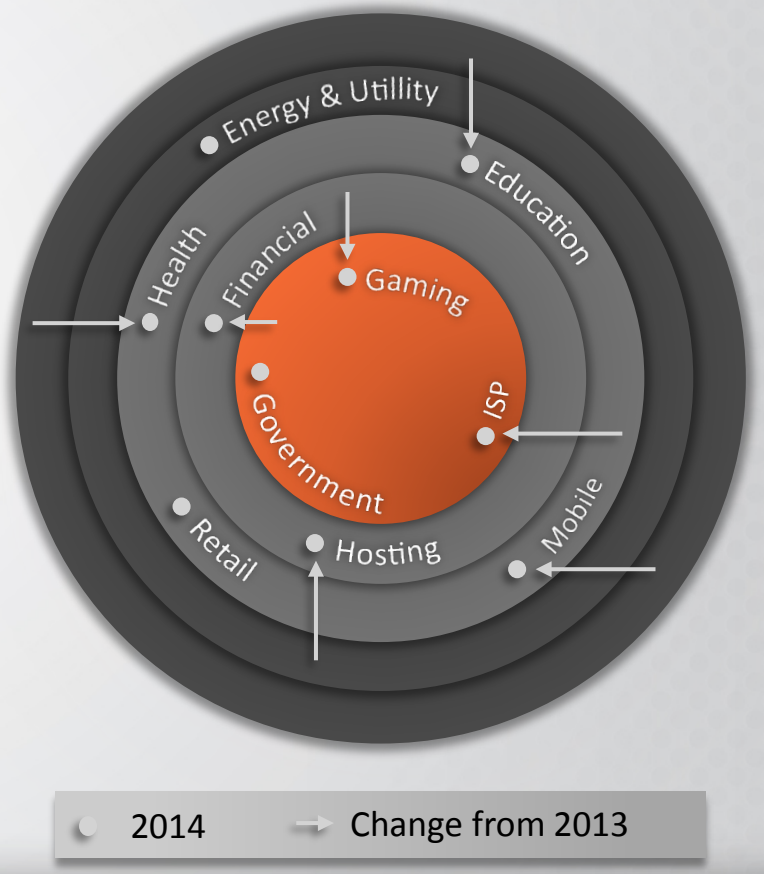
- Roughly half of attacks last more than one day
- **52%** of respondents felt they could only fight a campaign for a day or less.
- **19%** of attacks are considered “constant” in 2014
- Organizations reported week-long and month-long attacks in previous years but never more than 6% reported “constant” attacks



No One is Immune – Unexpected Targets

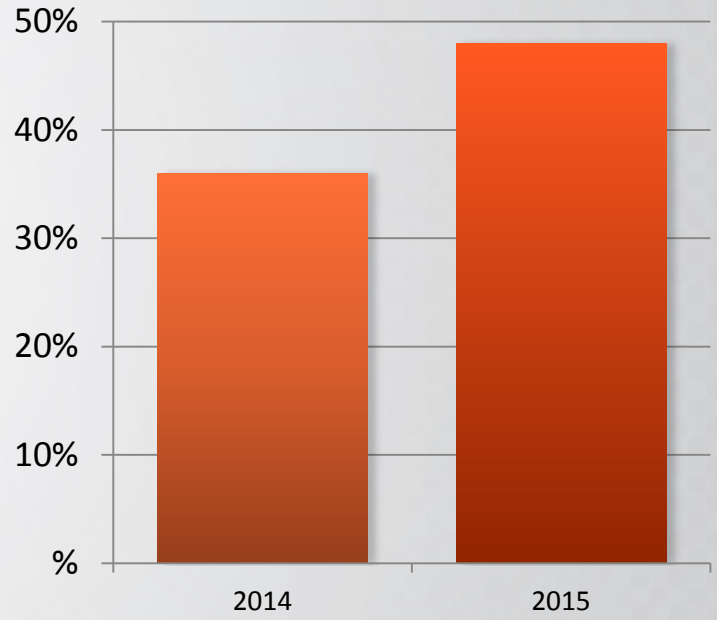
Threats in new industries, organizational sizes and technology deployments

- Healthcare and Education – unexpected targets now at risk
- Gaming, Hosting and ISP companies – increased likelihood
- Financial Services – the only industry to have a reduced risk



Hybrid Solutions are Gaining Ground

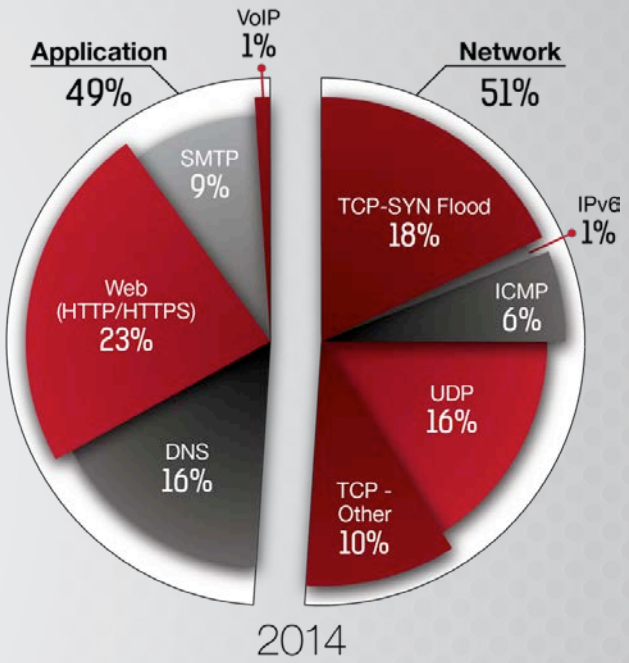
- Over a third (36%) are already using a hybrid solution with both customer premise equipment (CPE) and cloud solutions
- By 2015, nearly half (48%) will employ hybrid protection
- Both on-premises and in-the-cloud mitigation is a must
  - Cloud mitigation for volumetric attacks
  - On premise for immediate mitigation lower-rate attacks, SSL-based attacks

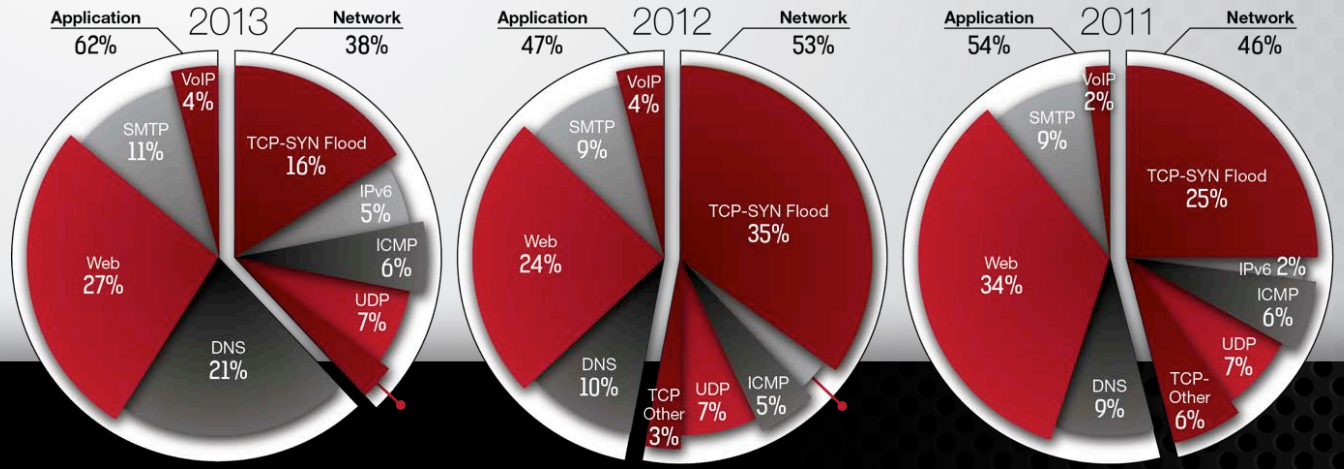


Organizations currently using and planning to use a hybrid security solution

Network vs. Application Attacks

- Attacks evenly split across network and application layers
- Web-based attacks remain the single most common attack vector
  - 1 in every 4 are HTTPS
- Increase reflective attacks cause UDP attacks to increase
  - From 7% in 2013 to 16% in 2014
- Reflective attacks represent 2014's single largest DDoS "headache"





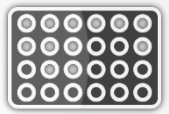
Successful Attack Mitigation Strategies

Be mindful of the C.H.E.W. threats – Cybercrime, Hacktivism, Espionage and Cyber War

Both detection and mitigation are important - success hinges on the **quality of both**

Timing is everything – provide solutions which ensure **the shortest time to mitigate**

Use multiple layers – a **hybrid solution** that integrates on-premise detection and mitigation with cloud-based protection - to block volumetric attacks



Choose a solution with the **widest coverage** to **protect from multi-vector attacks**

SSL attacks remain a major threat – SSL-based DoS/DDoS mitigation solution deployments **must not affect legitimate traffic** performance

A **single point of contact is crucial** when under attack - it will help to divert internet traffic and deploy mitigation solutions