Akamai

FASTER FORWARD

Cyber Attacks Against Banks: Is the Nightmare Over?

Rich Bolstridge

Chief Strategist, Financial Services

Topics

- Akamai at a glance
- The Risks of Banking over the Internet
- A look back at the Bank Attacks. What did we learn?
- How the threats have evolved. What are we seeing now?
- Solutions
- Q&A

Akamai FASTER FORWARD

We are the leading cloud service for helping enterprises provide the best online experiences on any device

ABOUT US:

- Distributed cloud platform, on-demand scale
- Delivering 15-30% of all daily web traffic
- 2 trillion cloud interactions daily
- 150M mobile apps delivered daily
- Defending against attacks over 200Gbps
- Enabling >$250B in annual e-commerce
- A single network hop from 90% of internet users

CORP STATS:

$1.6B	2,000	5,000	4,000
Revenue	Locations	Customers	Employees

OUR HISTORY:

Founded 1998 and rooted in MIT technology—solving Internet congestion with math not hardware.

Topics

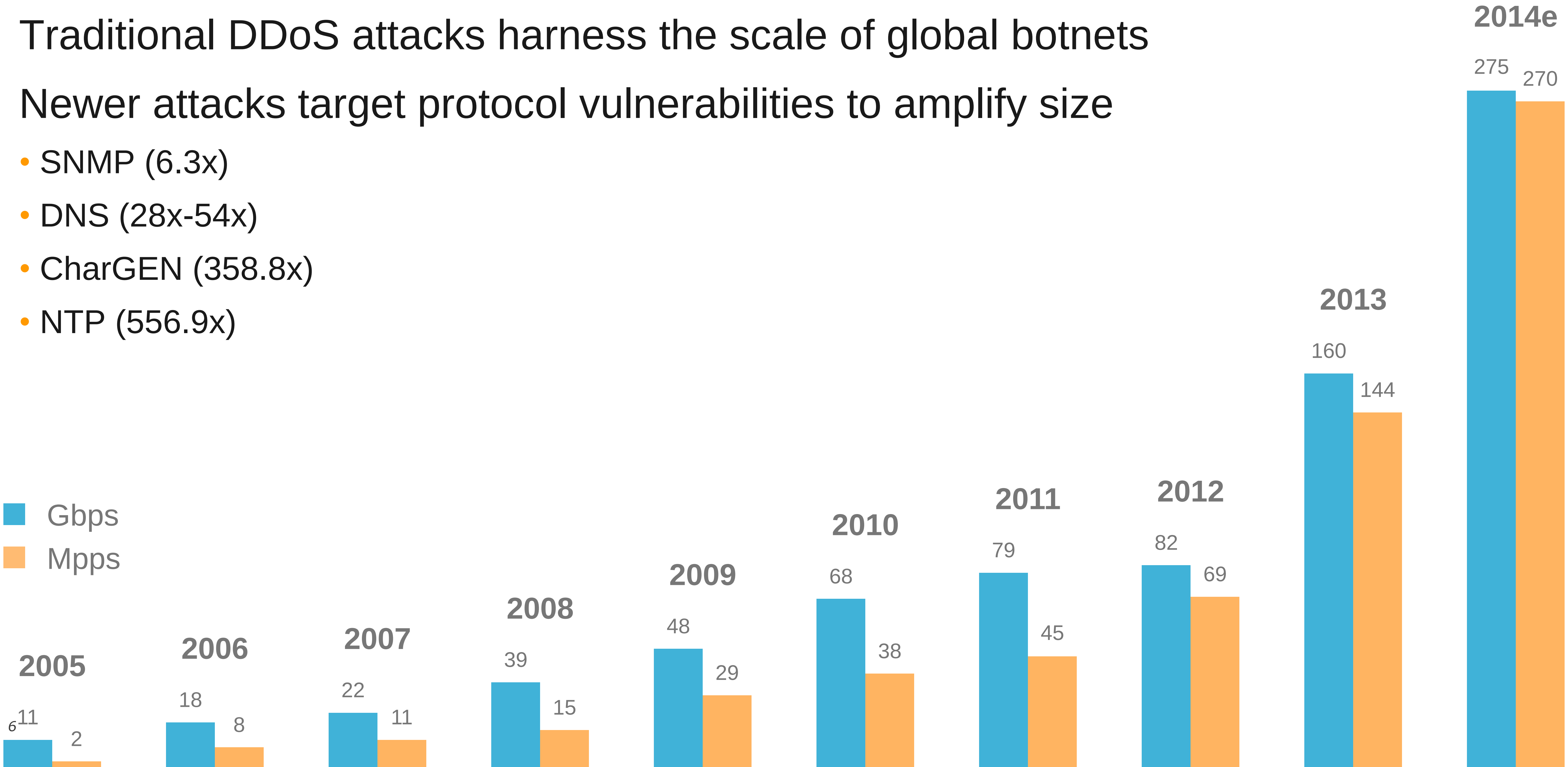
- Akamai at a glance
- The Risks of Banking over the Internet
- A look back at the Bank Attacks. What did we learn?
- How the threats have evolved. What are we seeing now?
- Solutions
- Q&A

Attacks Are Growing in Size

Traditional DDoS attacks harness the scale of global botnets

Newer attacks target protocol vulnerabilities to amplify size

- SNMP (6.3x)
- DNS (28x-54x)
- CharGEN (358.8x)
- NTP (556.9x)

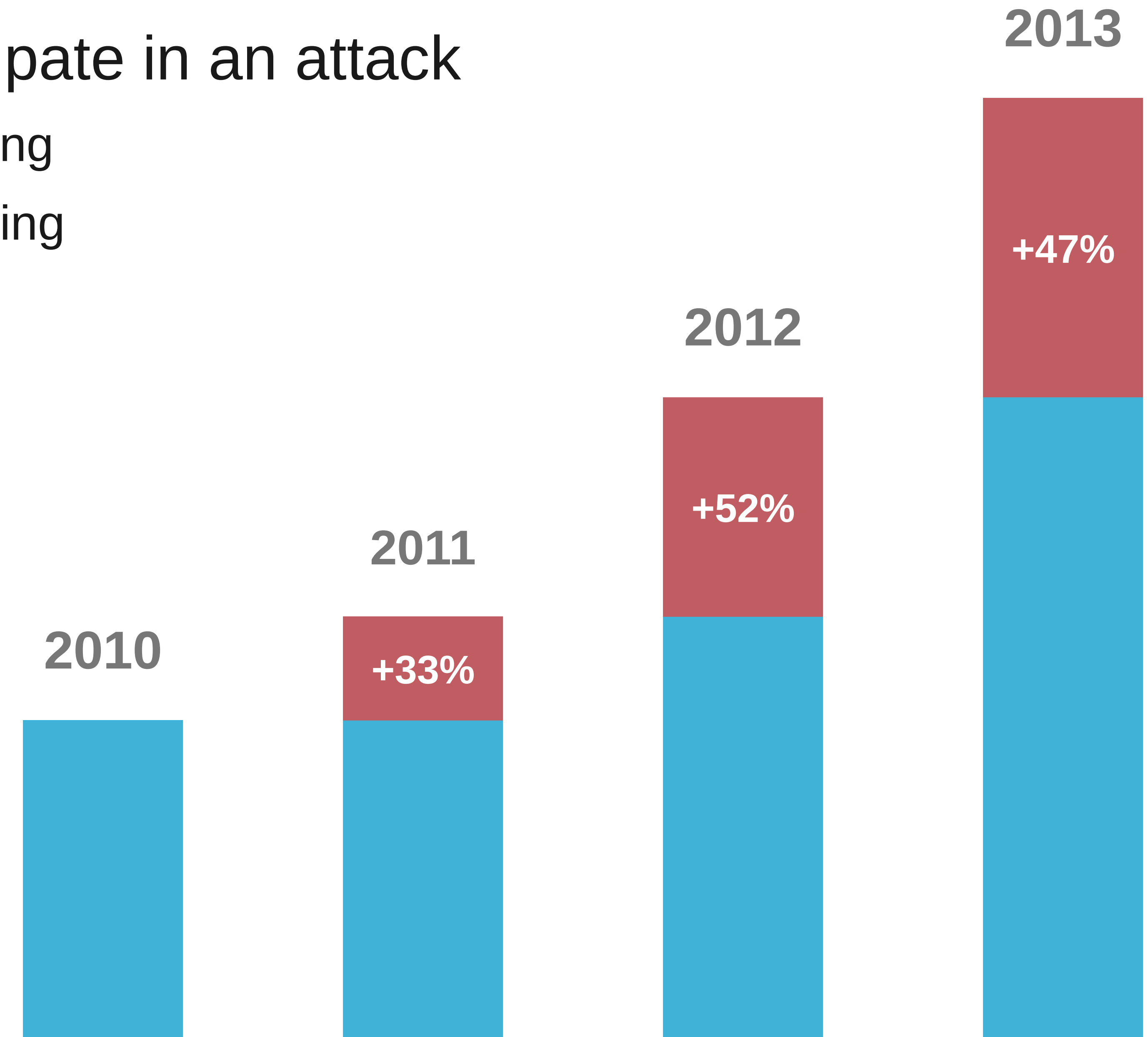


Organizations Are Being Attacked More Frequently

Increasing number of network- and application-layer attacks

Easier for attackers to launch or participate in an attack

- Knowledge of application vulnerabilities spreading
- Number and availability of attack tools proliferating

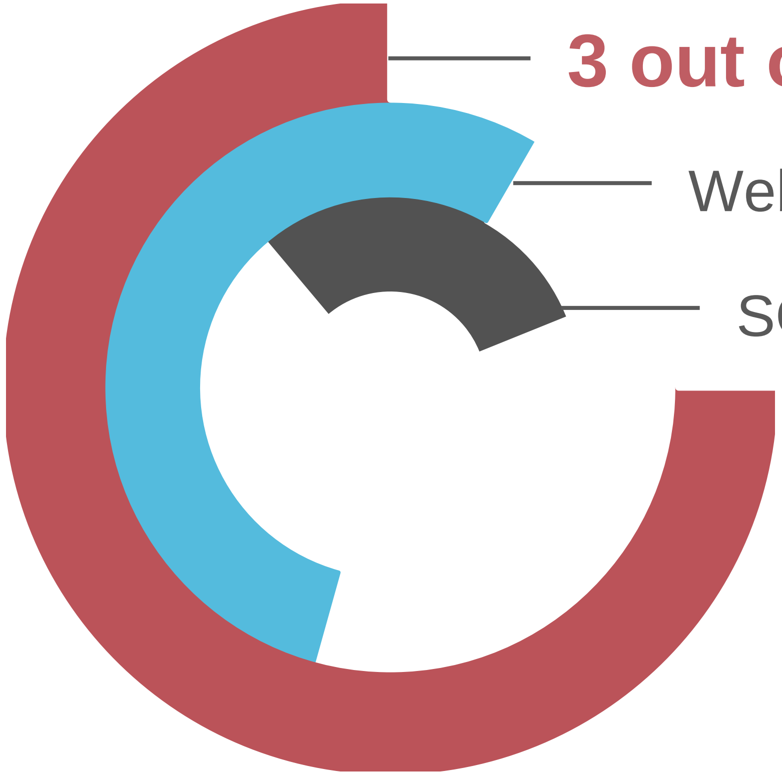


Source: Akamai

Targeting Applications for Data Theft

Increasing number of attacks focused on data and financial theft

Web applications are a primary target due to number of vulnerabilities



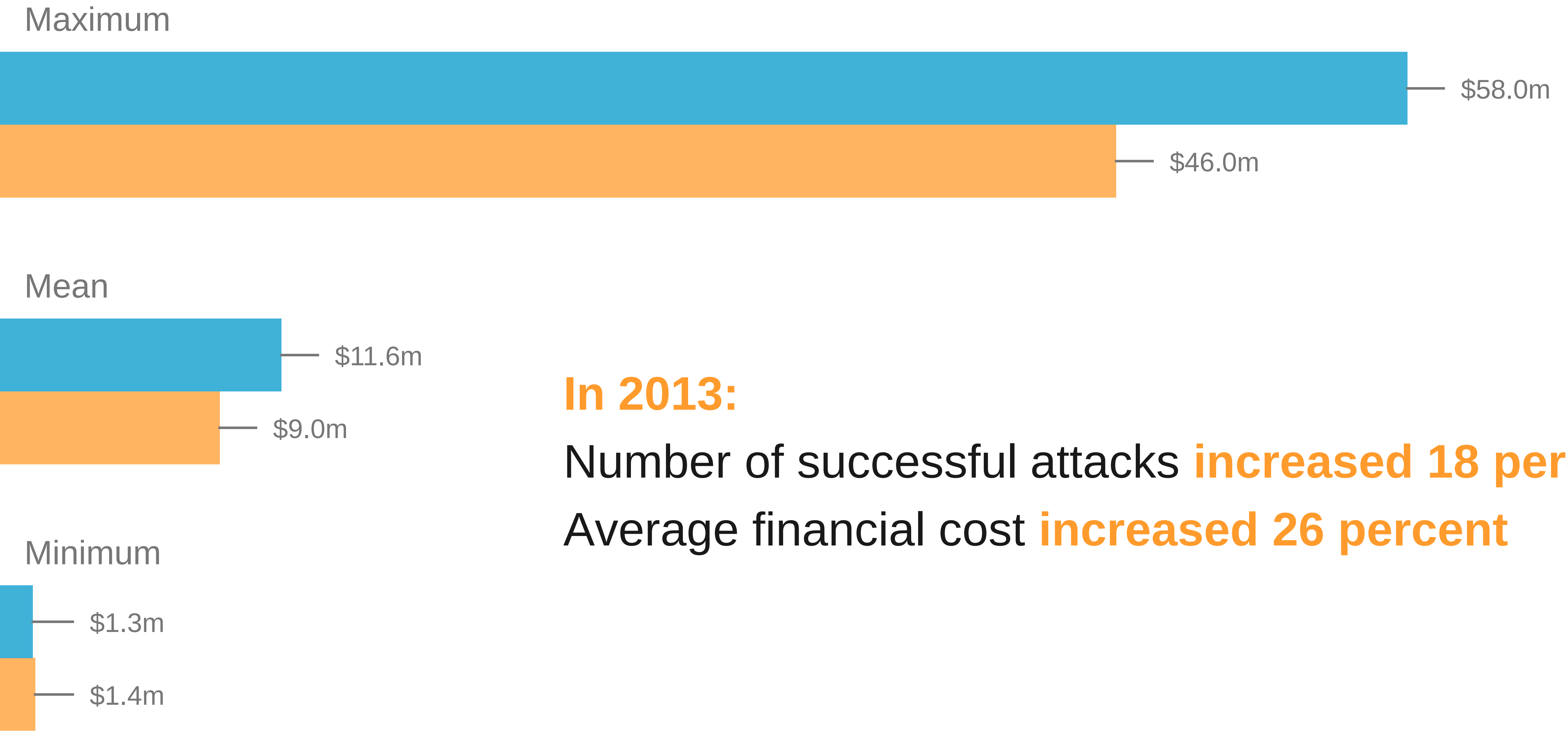
3 out of 4 companies will be targeted by Web application exploits

Web apps targeted in **54%** of hacking-based data breaches

SQL injection is the primary culprit in **30%** of data breaches

Source: Veracode

Financial Impact of Cybercrime Increasing



In 2013:

Number of successful attacks **increased 18 percent**

Average financial cost **increased 26 percent**

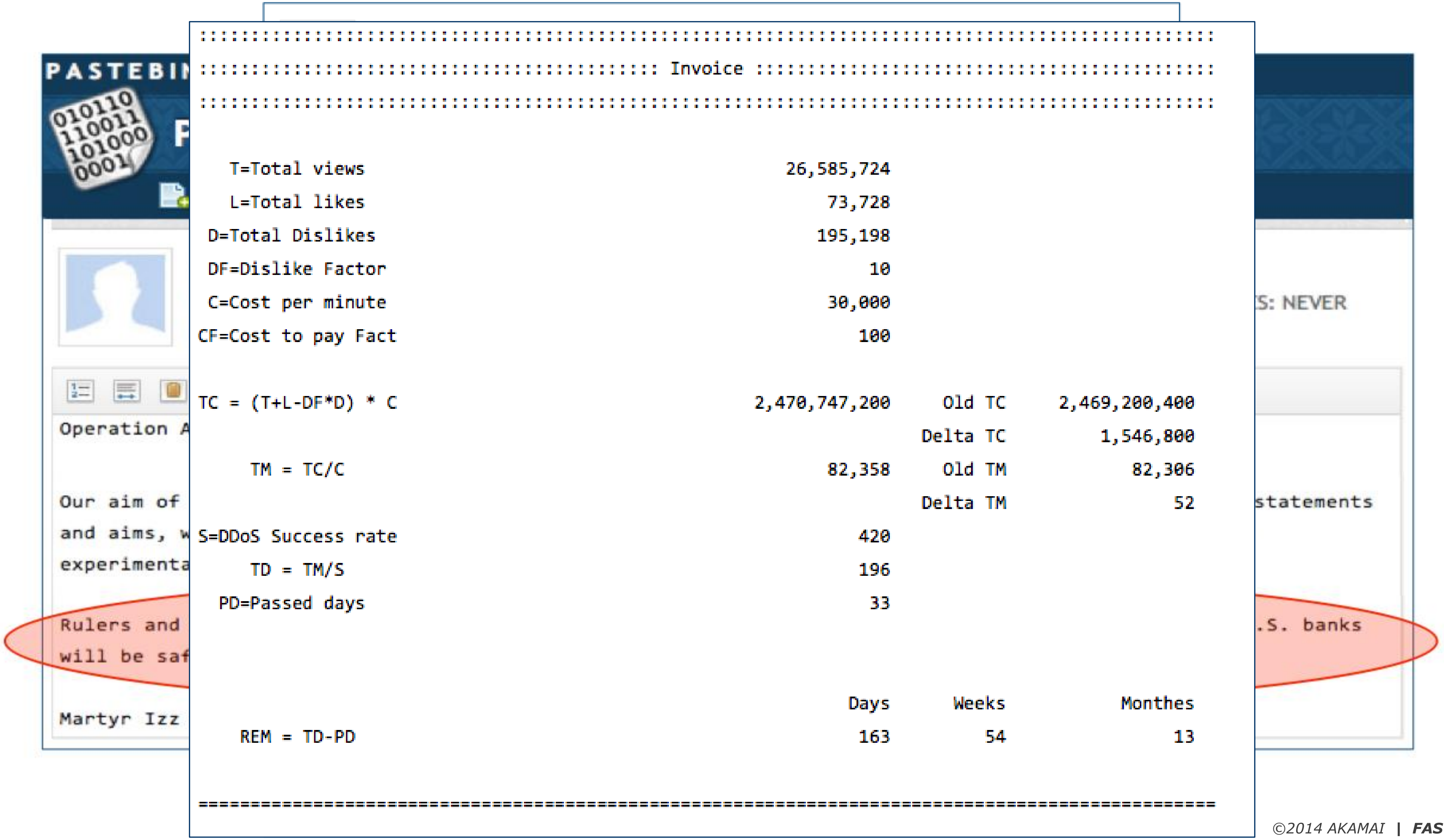
Source: Ponemon 2013 Cost of Cyber Crime Study

Topics

- Akamai at a glance
- The Risks of Banking over the Internet
- A look back at the Bank Attacks. What did we learn?
- How the threats have evolved. What are we seeing now?
- Solutions
- Q&A

Operation Ababil / 2nd Phase / 4th Week

“none of the U.S. banks will be safe from our attacks.”



PASTEBIN

Operation A

Our aim of

and aims, w

experimenta

Rulers and

will be saf

Martyr Izz

S: NEVER

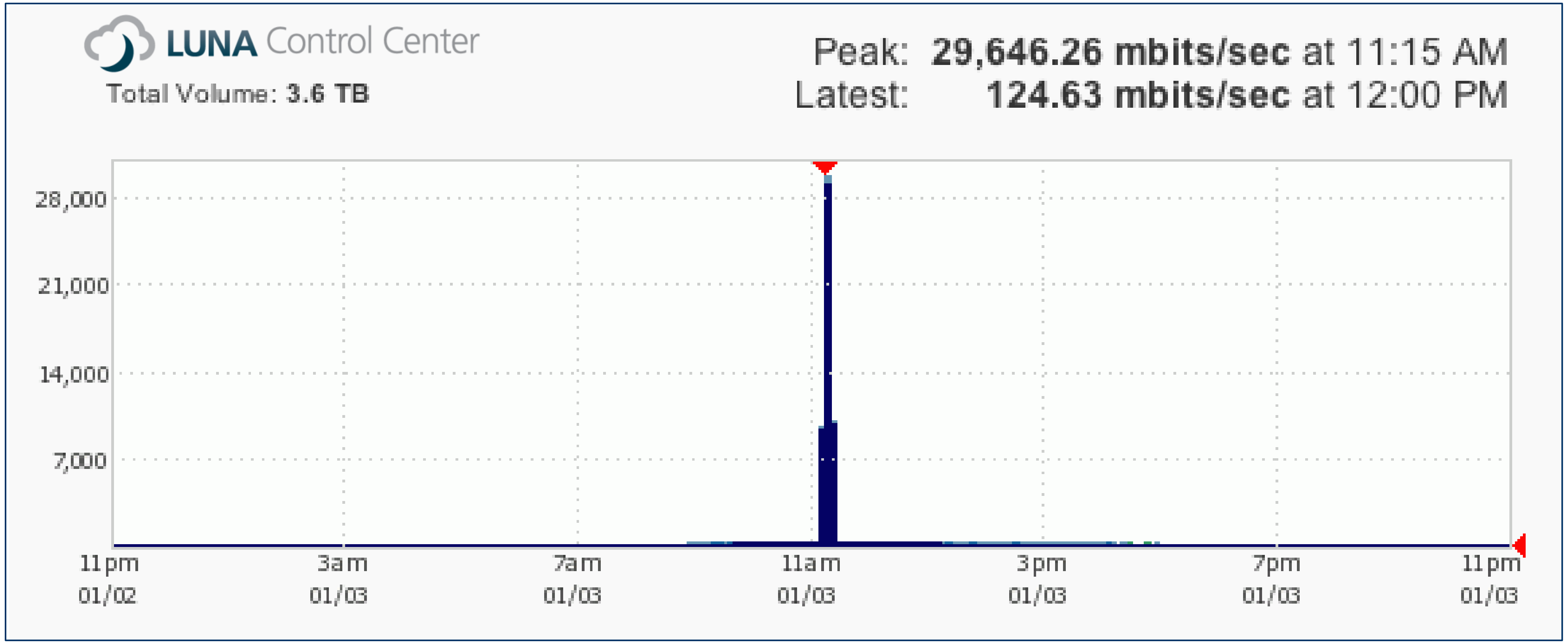
statements

.S. banks

```
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:::::::::::::::::::::::::::::::::::::::::::: Invoice :::::::::::::::::::::::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


   T=Total views                              26,585,724
   L=Total likes                                  73,728
 D=Total Dislikes                                195,198
 DF=Dislike Factor                                    10
 C=Cost per minute                                30,000
CF=Cost to pay Fact                                  100

TC = (T+L-DF*D) * C                        2,470,747,200    Old TC     2,469,200,400
                                                          Delta TC         1,546,800
     TM = TC/C                                    82,358    Old TM            82,306
                                                          Delta TM                52
S=DDoS Success rate                                  420
     TD = TM/S                                       196
  PD=Passed days                                      33



                                                    Days      Weeks          Monthes
    REM = TD-PD                                      163         54               13


================================================================================================
```

Lesson: Be prepared for “Instant on” massive attacks

- Top financial services firm with nearly 10M customers.
- Peak attack traffic was 30 Gbps, 30x normal daily high traffic.
- Attackers gave up after 15 minutes, and moved attack to another bank.
- 100% of the attack was on SSL.



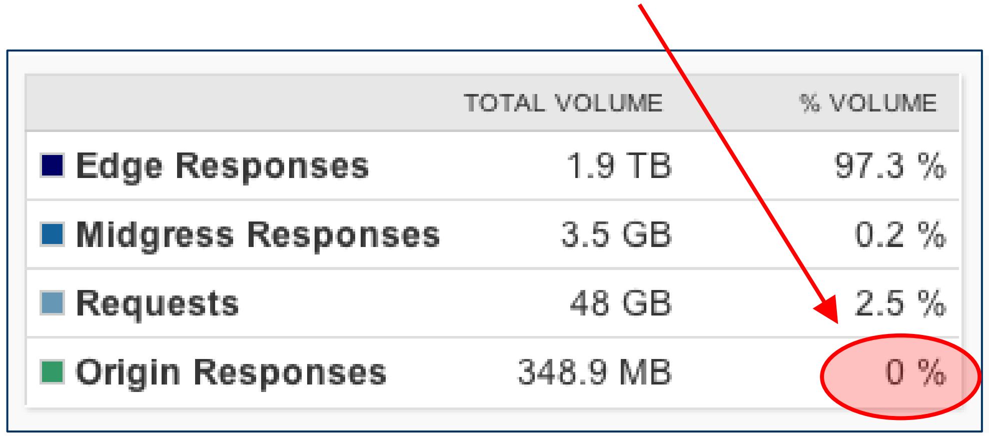
LUNA Control Center

Total Volume: 3.6 TB

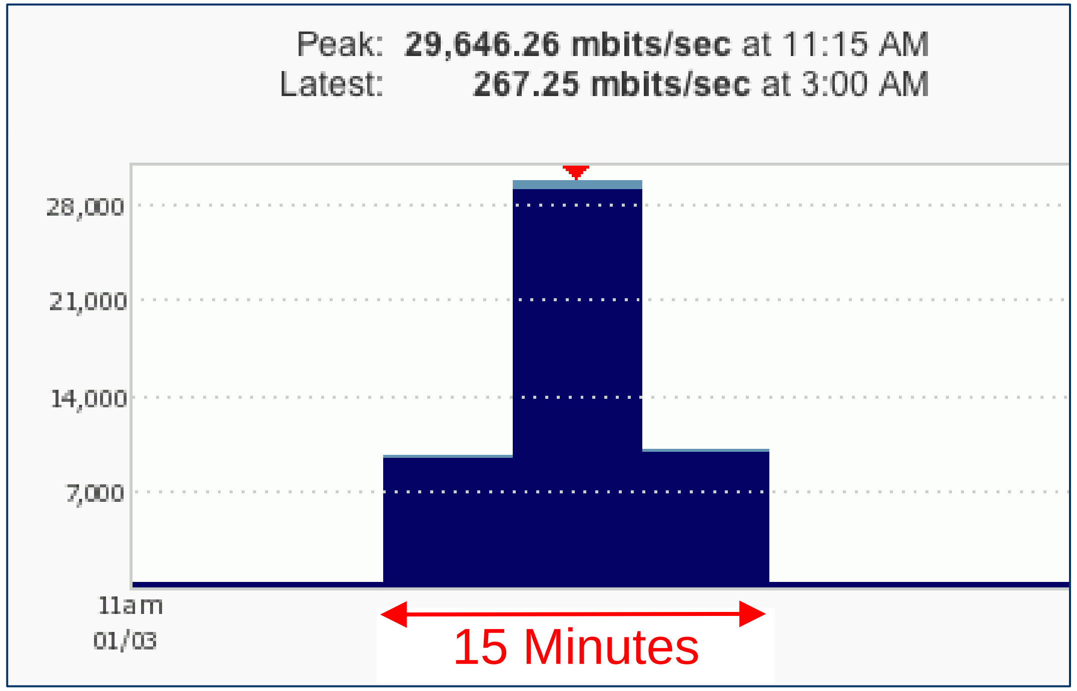
Peak: 29,646.26 mbits/sec at 11:15 AM
Latest: 124.63 mbits/sec at 12:00 PM

Lesson: The value of "Always-On" protection

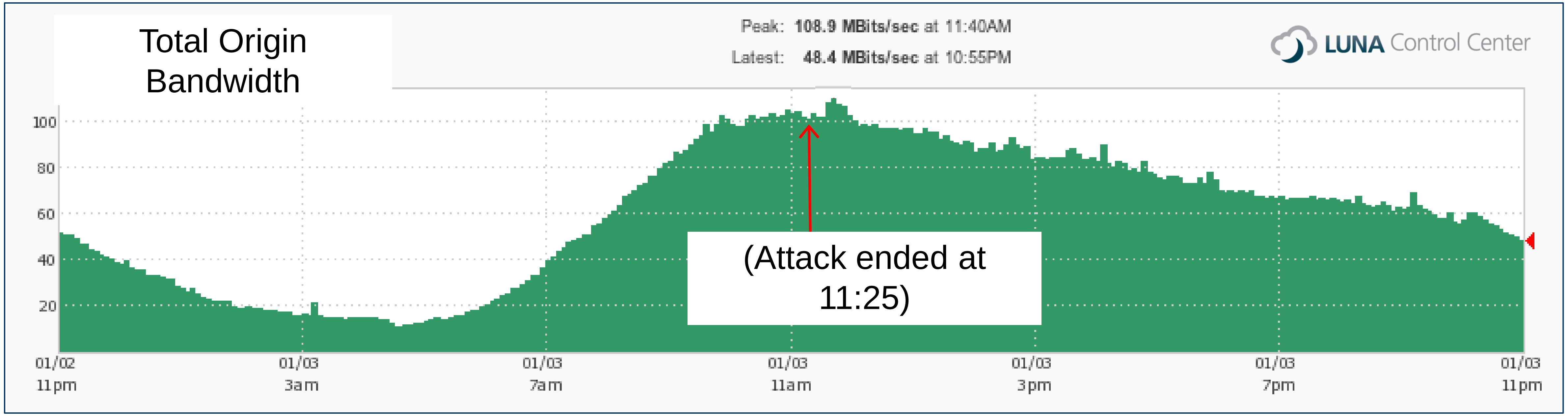
- Offload 100% of the attack.



	TOTAL VOLUME	% VOLUME
■ Edge Responses	1.9 TB	97.3 %
■ Midgress Responses	3.5 GB	0.2 %
■ Requests	48 GB	2.5 %
■ Origin Responses	348.9 MB	0 %

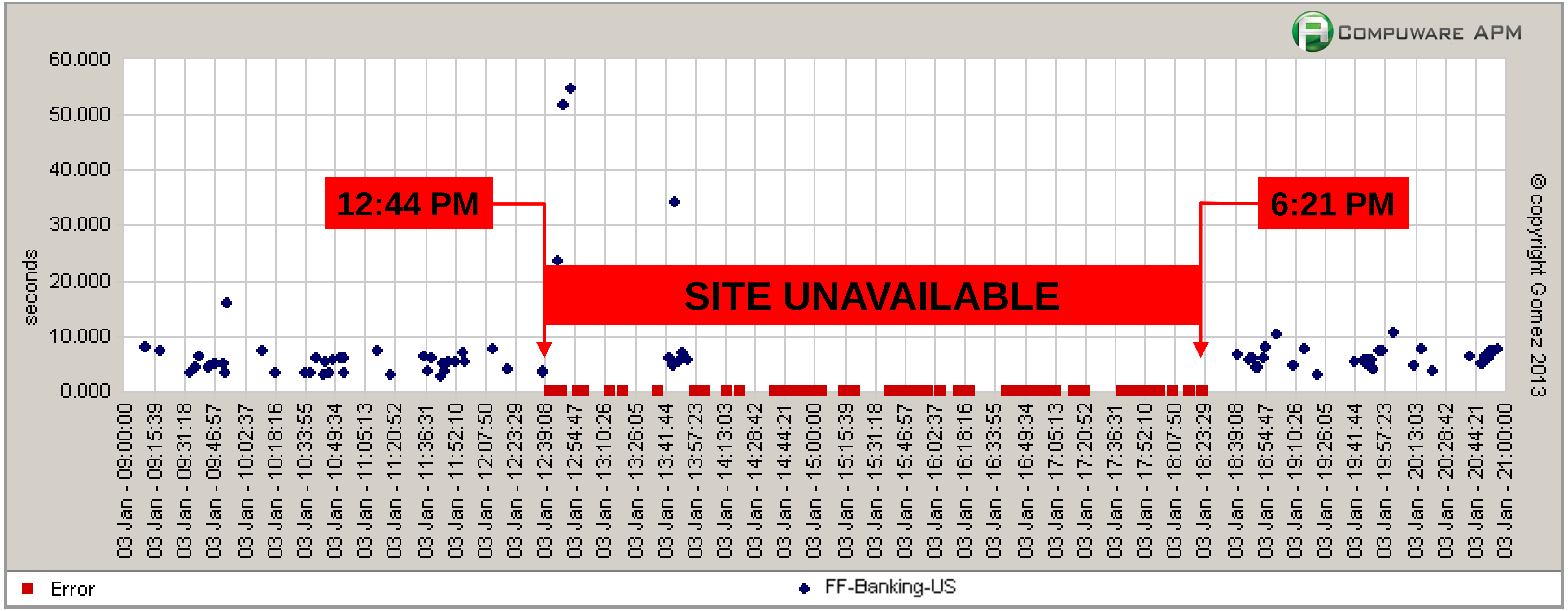


- "A bug impacting our windshield".



Lesson: Attackers look for soft targets

- 5 banks attacked in a single day. Average 15 minutes on protected sites
- Soft target found, and brought down for 6 hours.
- Bank attacked over 20 times after this event.



12:44 PM

SITE UNAVAILABLE

6:21 PM

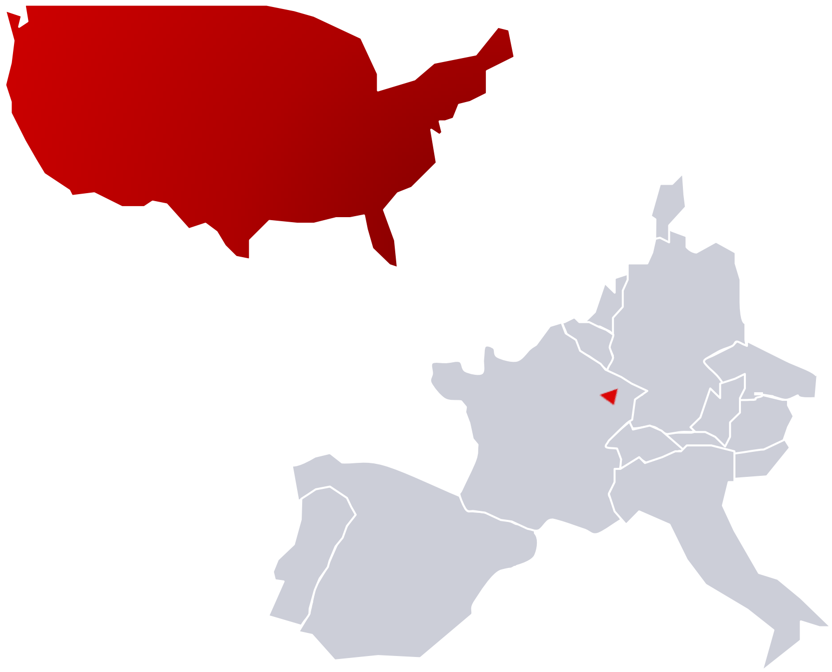
Lesson: The unforeseen risk of shared services DDoS

Case 1

Attack: DDoS attack on Brazil bank subsidiary.
Result: US Bank knocked out due to shared infrastructure in data center.

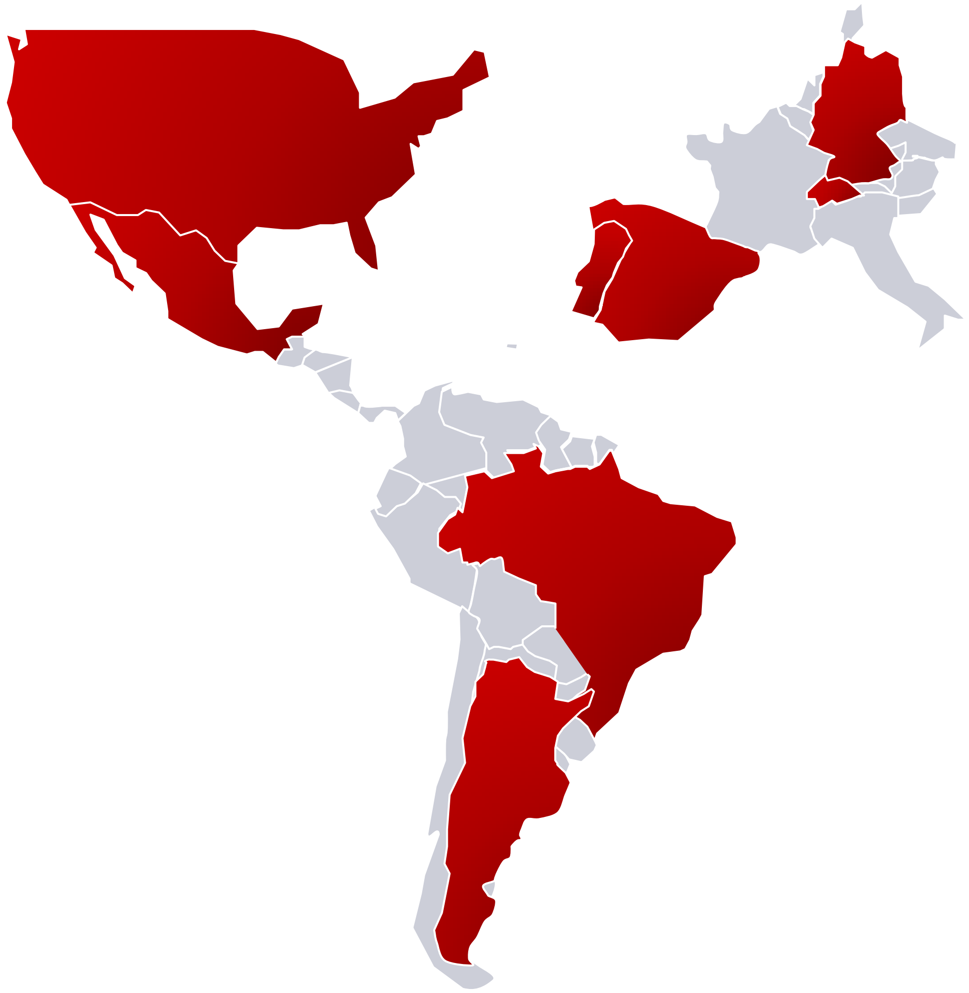
Case 2

Attack: DDoS attack against Luxembourg customer of US exchange.
Result: Market data unavailable to US subscribers during market open hours.



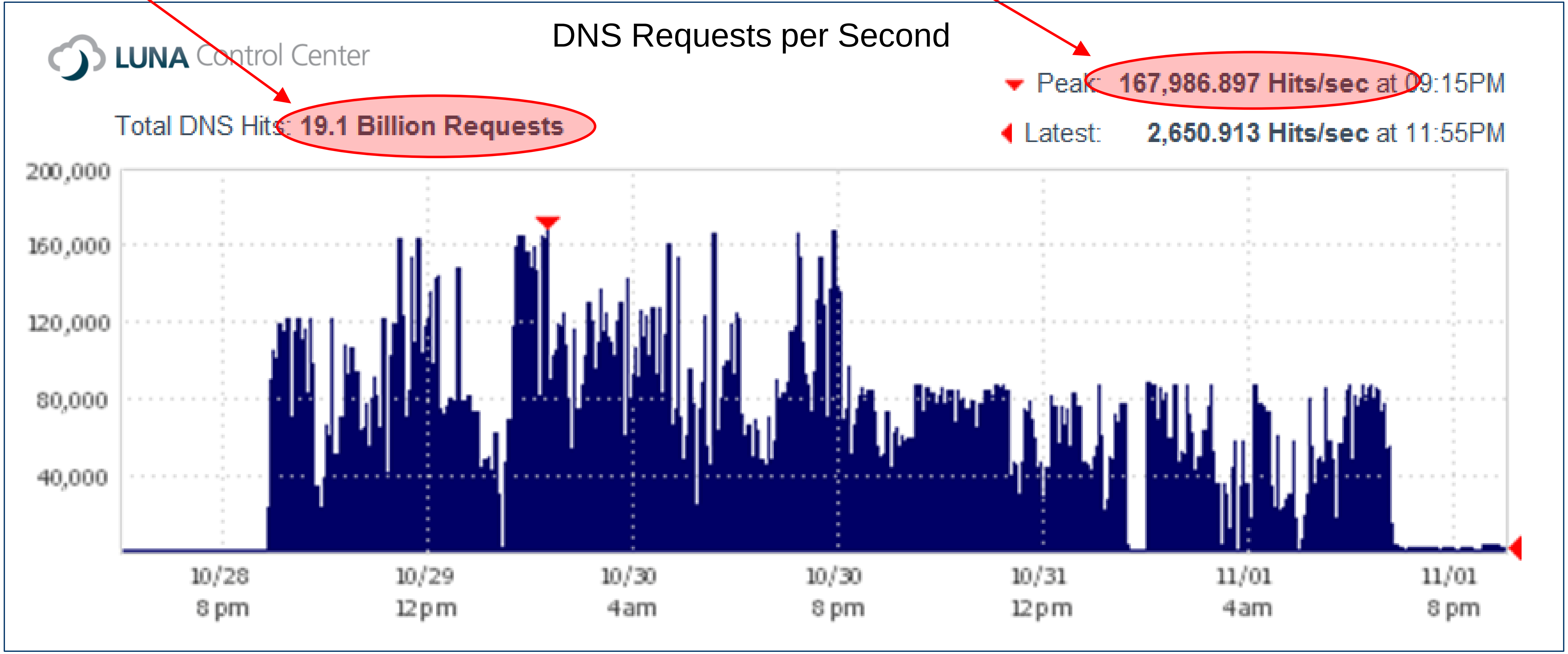
Case 3

Attack: QCF attacks name servers of a US bank, which is a subsidiary of a European bank.
Result: QCF unintentionally takes down a Global Bank.



Lesson: DNS is a soft spot

- DNS requests peaked at 168k per second.
- 19B hits in 5 days. Normally serve ~30M hits per week.



DNS Requests per Second

LUNA Control Center

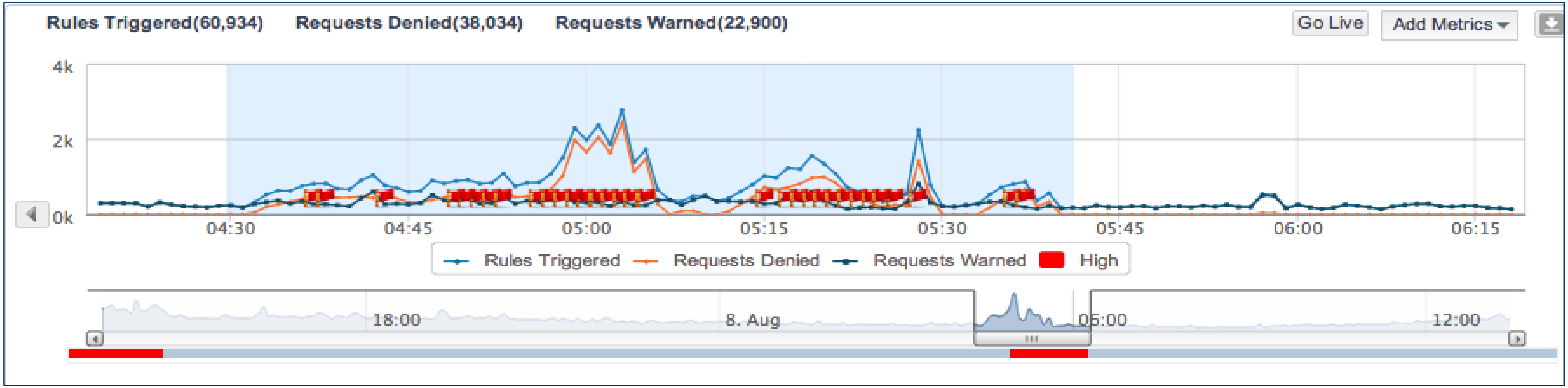
Total DNS Hits: 19.1 Billion Requests

Peak: 167,986.897 Hits/sec at 09:15PM

Latest: 2,650.913 Hits/sec at 11:55PM

Lesson: “We were doing OK until the attacks started coming in on SSL.”

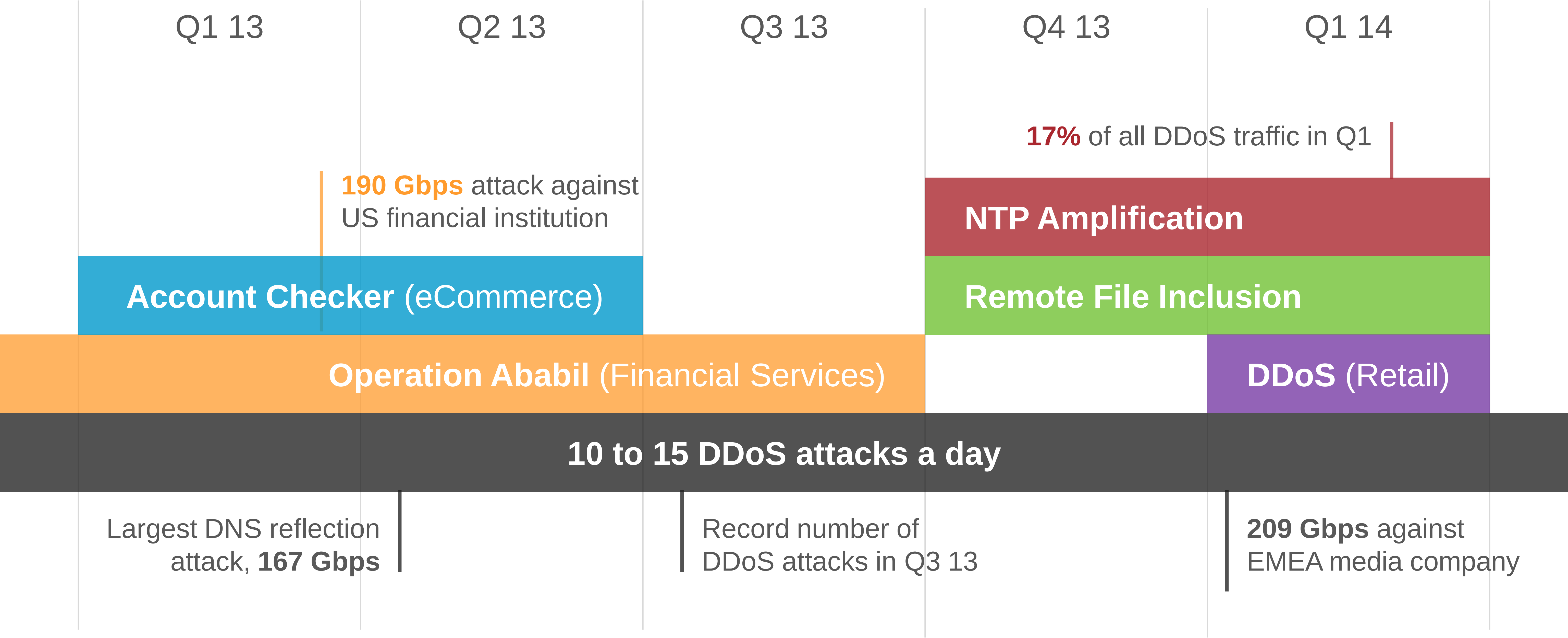
- Large US bank hit with 5 hour SQL Injection attack.
- Attack was SSL-based.
- SSL termination required to see requests “in the clear” and block.
- Packet-level inspection not effective. Clean-pipe services would not stop this.



Topics

- Akamai at a glance
- The Risks of Banking over the Internet
- A look back at the Bank Attacks. What did we learn?
- How the threats have evolved. What are we seeing now?
- Solutions
- Q&A

2013: Year of Evolving Web Security Threats



Q1 13

Q2 13

Q3 13

Q4 13

Q1 14

17% of all DDoS traffic in Q1

190 Gbps attack against US financial institution

NTP Amplification

Account Checker (eCommerce)

Remote File Inclusion

Operation Ababil (Financial Services)

DDoS (Retail)

10 to 15 DDoS attacks a day

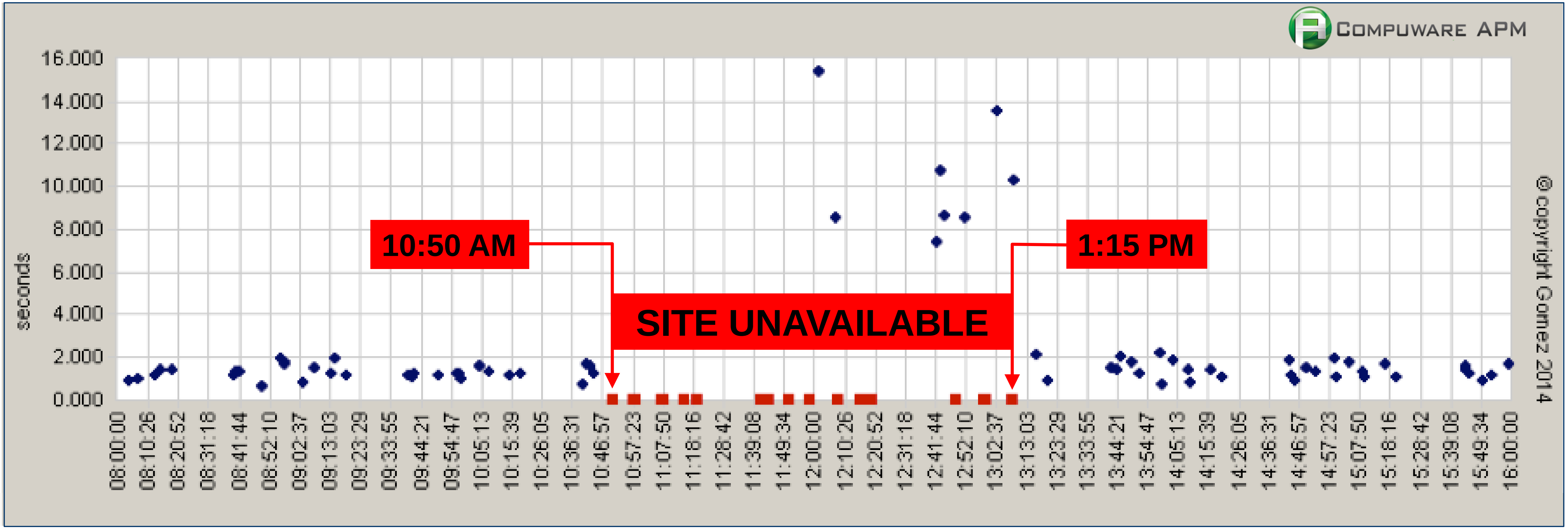
Largest DNS reflection attack, **167 Gbps**

Record number of DDoS attacks in Q3 13

209 Gbps against EMEA media company

Some banks are still not protected

- January 2014



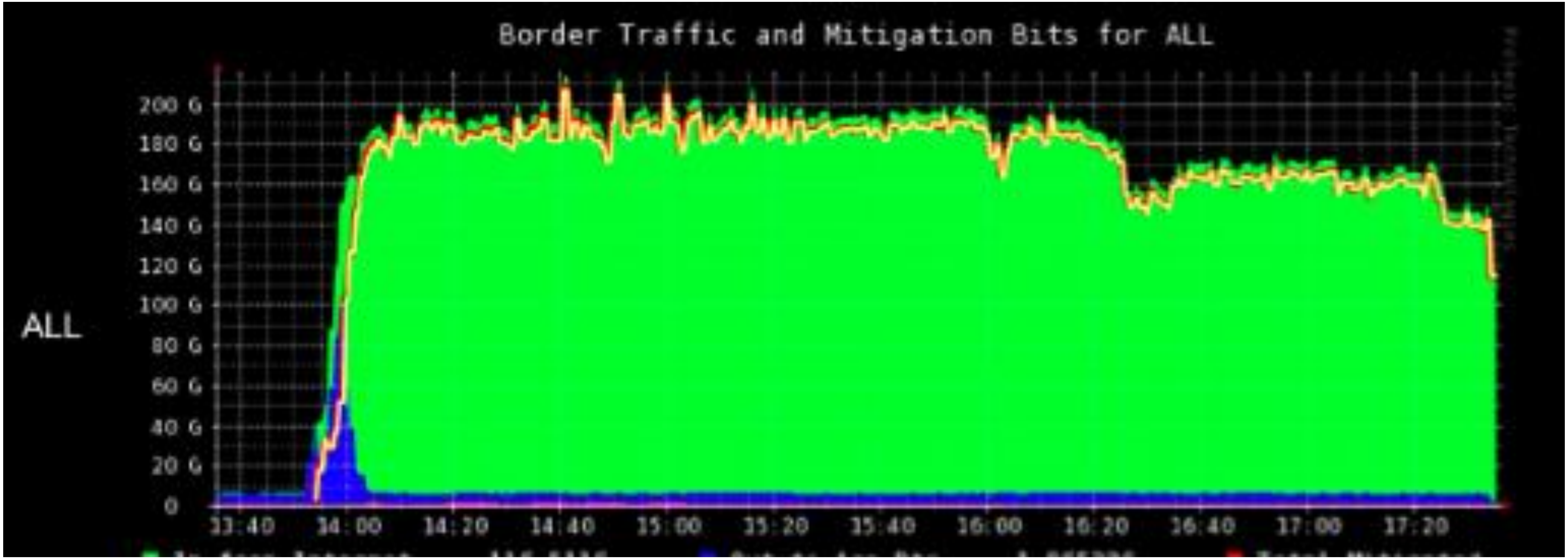
10:50 AM

SITE UNAVAILABLE

1:15 PM

Lesson: You can’t build big enough

- 240 Gbps attack.

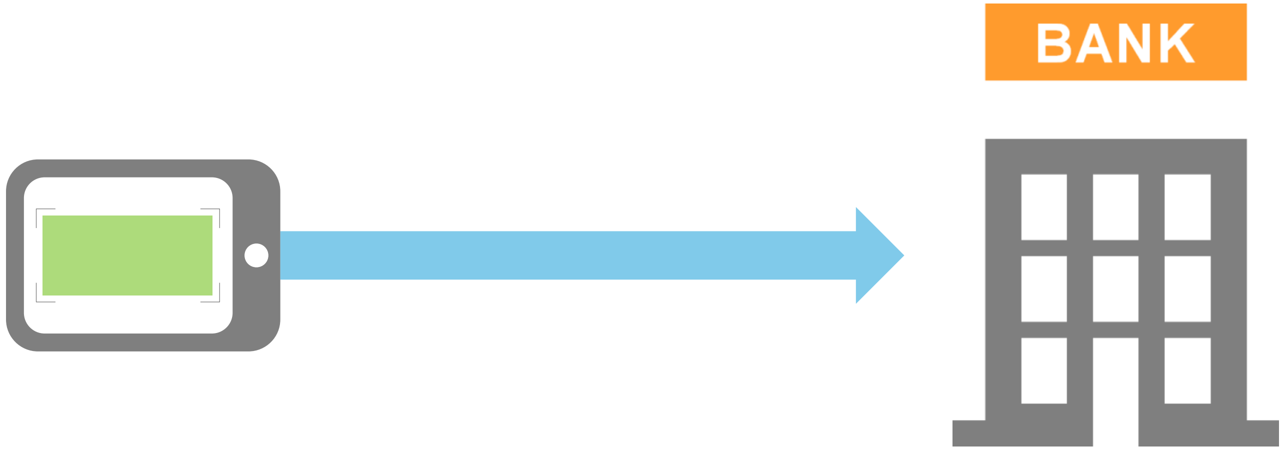


Not just DDoS: Mobile check deposit application attack

What happened

Anonymous attacker accessed URLs for mobile check deposit application 120,000 times over four hours

Web requests for “checkfront.jpg”, “checkback.jpg”, and more



How the attack was defeated

Web application firewall rate controls

Topics

- Akamai at a glance
- The Risks of Banking over the Internet
- A look back at the Bank Attacks. What did we learn?
- How the threats have evolved. What are we seeing now?
- Solutions
- Q&A

Total Risk Assessment – with and without Akamai

Adding 3rd party service adds risk

Using Akamai platform decreases other risks

- Blocks network layer attacks.
- Proven ability to handle the world's largest DDoS attacks.

Kona further decreases risk

- Expansive application layer protection.
- Rate limiting, origin cloaking, more…
- Can also protect DNS.

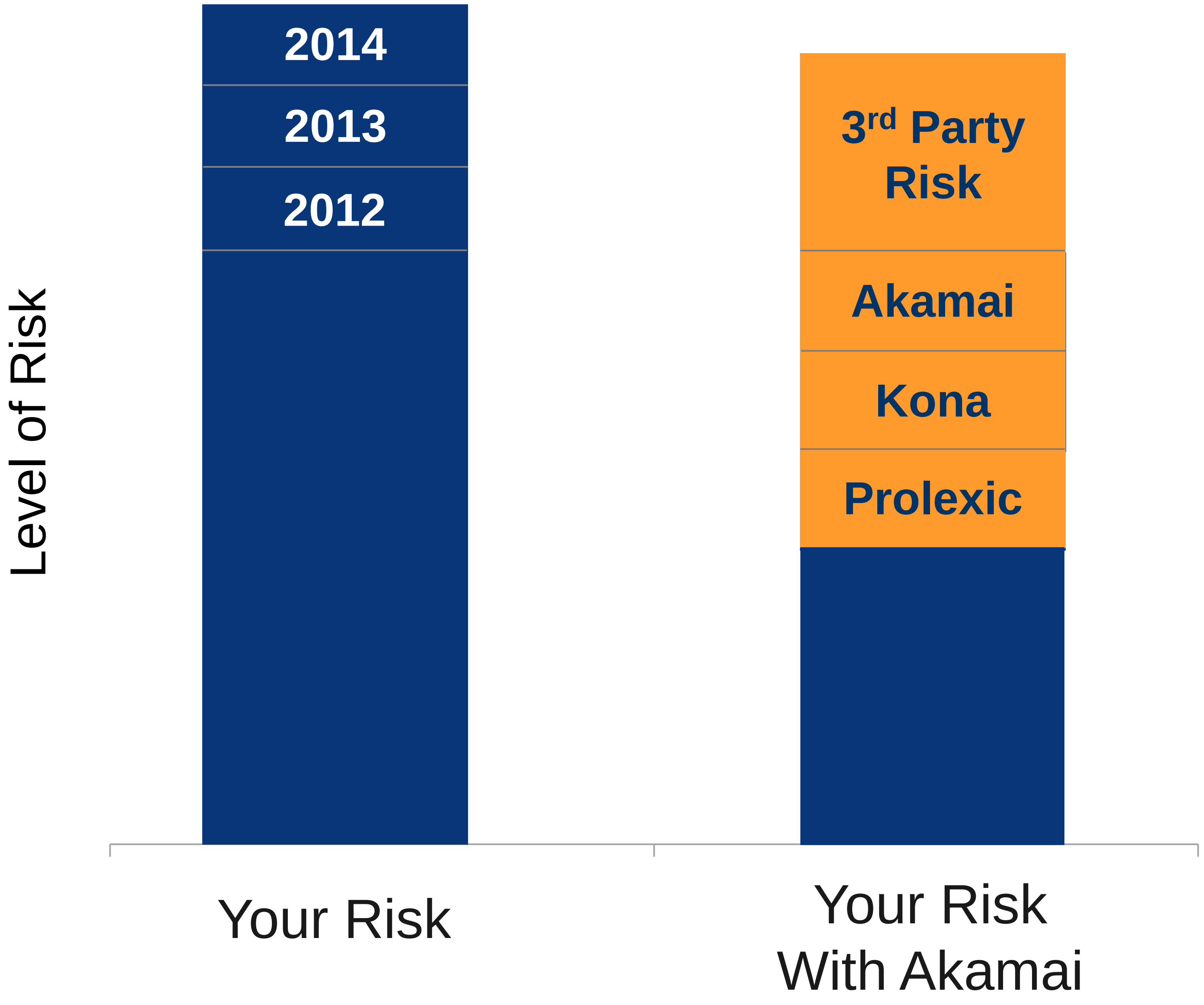
Future Akamai security products

- Major investments in our security division and product roadmap.

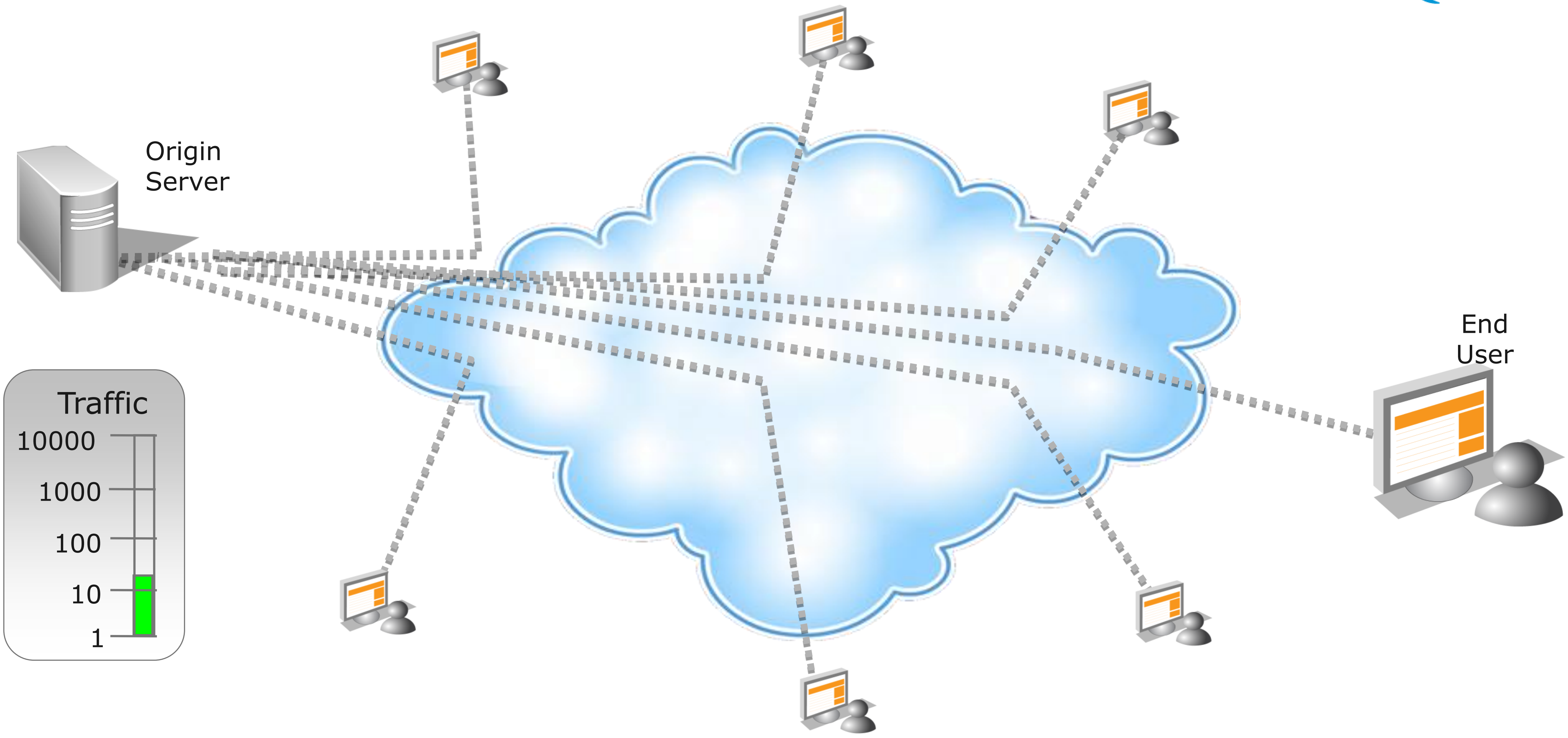
Risks are increasing

- Continuous threat of attacks against companies.
- DDoS masking fraudulent money movement.

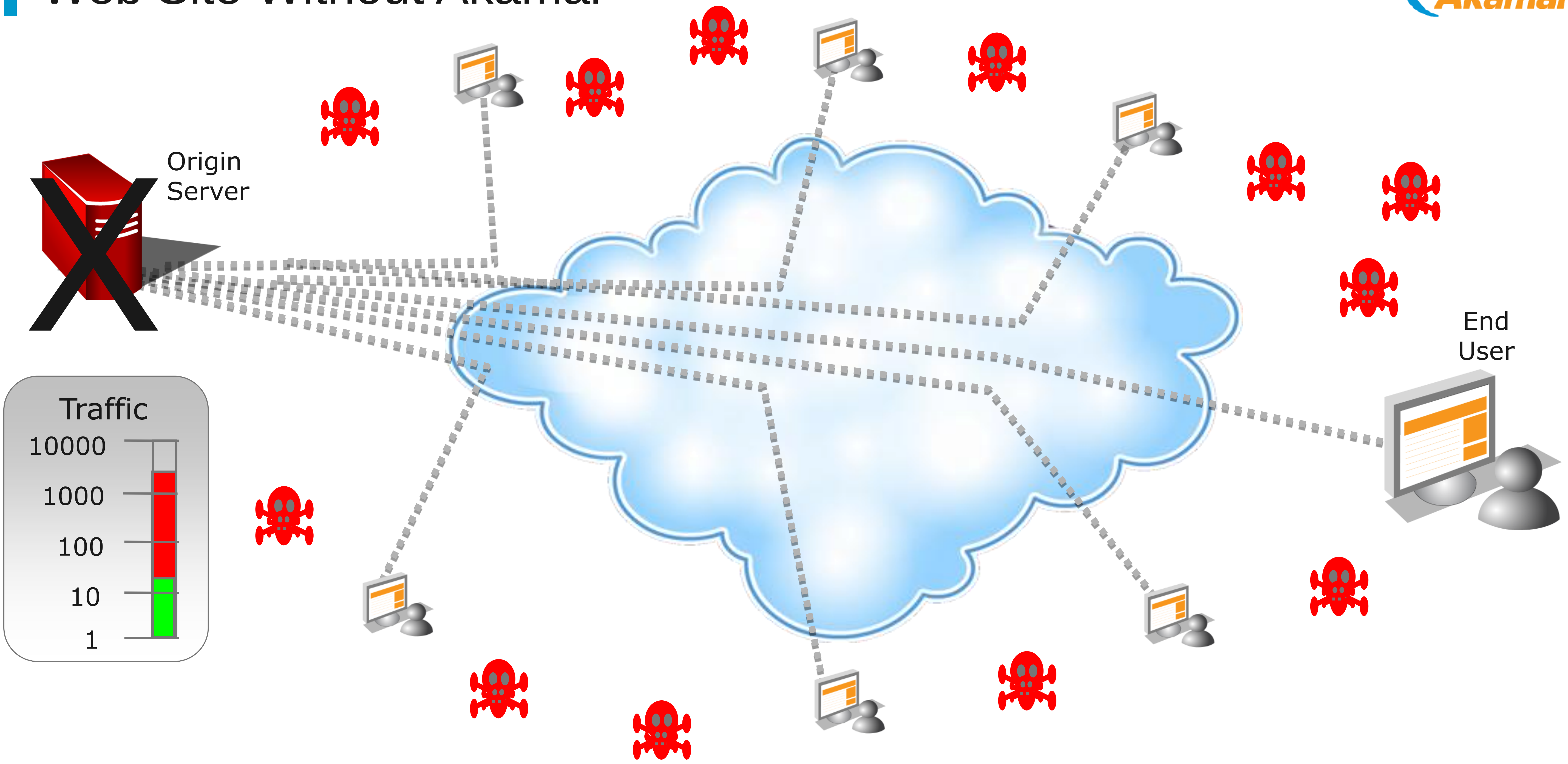
Where is your tipping point?



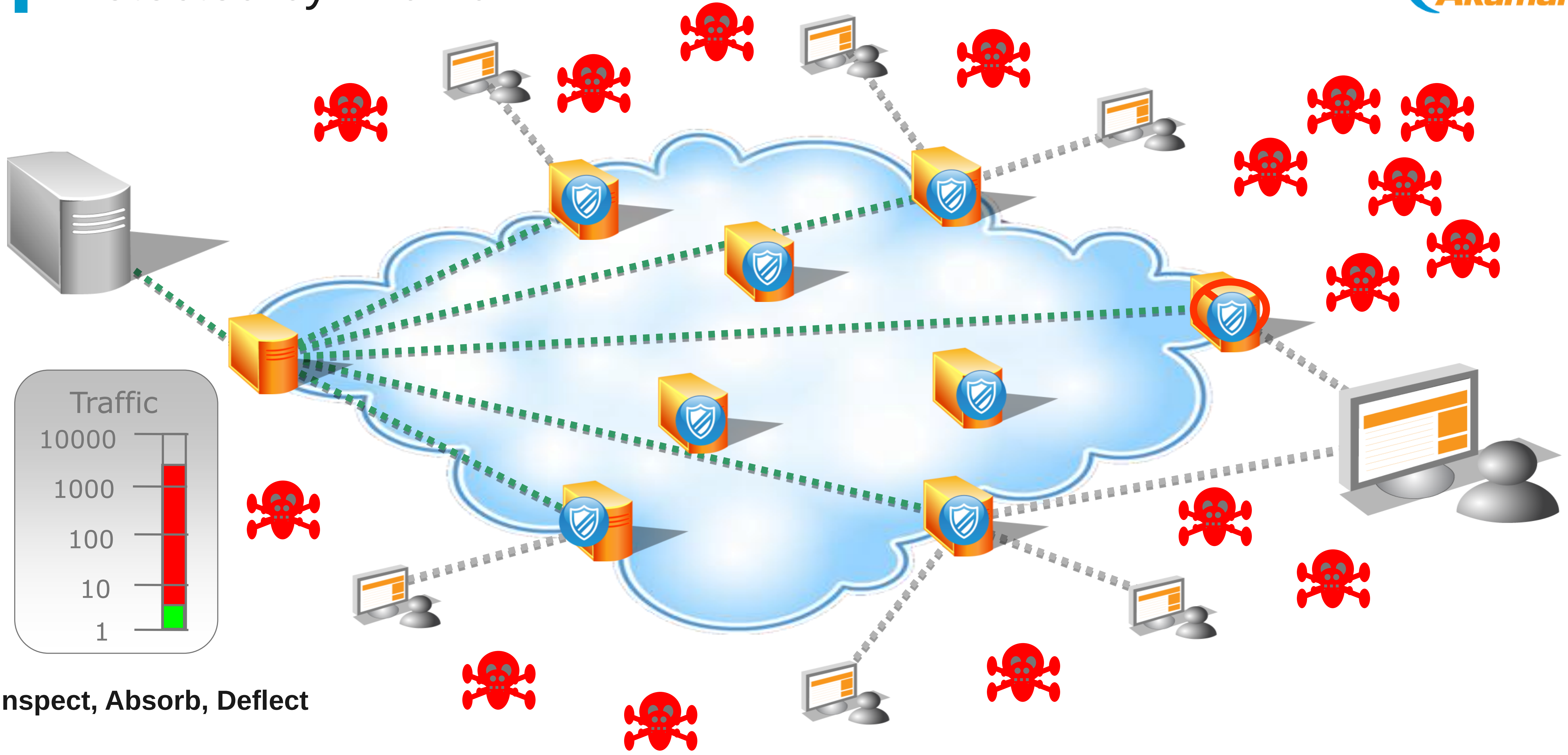
Web Site Without Akamai



Web Site Without Akamai



Protected by Akamai



Inspect, Absorb, Deflect

Akamai Client Reputation

Record past behavior — use the data to protect everyone

- Analyze activity across Akamai customers.
- Create a reputation score per client based on recent beha
- Filter potentially malicious clients at the edge
- Risk score ranges from 1-10, based upon:
  - Persistency of the attacker
  - Severity of the attack
  - Magnitude of the attack
  - Distribution of the attack across multiple hosts

Maximize Business Value with Protect + Perform

Improve Customer Experience

- Faster websites and mobile apps
- Improve availability and customer satisfaction
- Increase employee productivity

Protect the Customer

- DDoS protection
- Data breach protection
- Threat intelligence

Enable Innovation

- Quickly introduce new banking services
- Leverage cloud services
- Reduce business risk

Thank you!

Questions?

Rich Bolstridge
Chief Strategist, Financial Services
ribolstr@akamai.com
+1.617.444.2889