Adaptive Protection Against Web Application and DDoS Attacks

Akamai

Experience the Edge

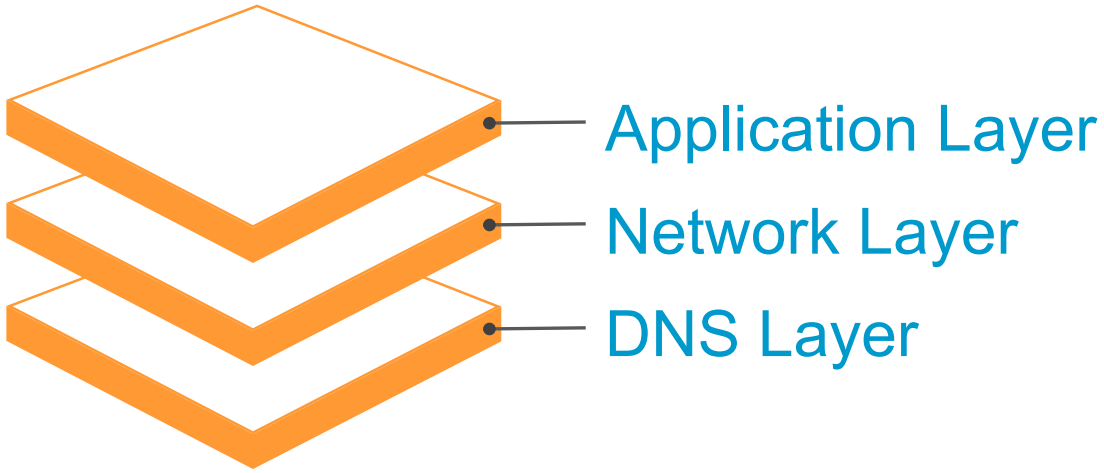
WAF
Critical protection for every business

Two types of attacks

Want *quick* money
- Target many at once
- Low effort to hide
- Known methods

Want *big* money or damage
- Target a few organizations
- High effort to hide
- Unknown/new vectors

Broad attack surface



Web Application Threats
DDoS attacks on the rise

↑ **16%** layer 3&4 attacks

↑ **38%** application layer attacks

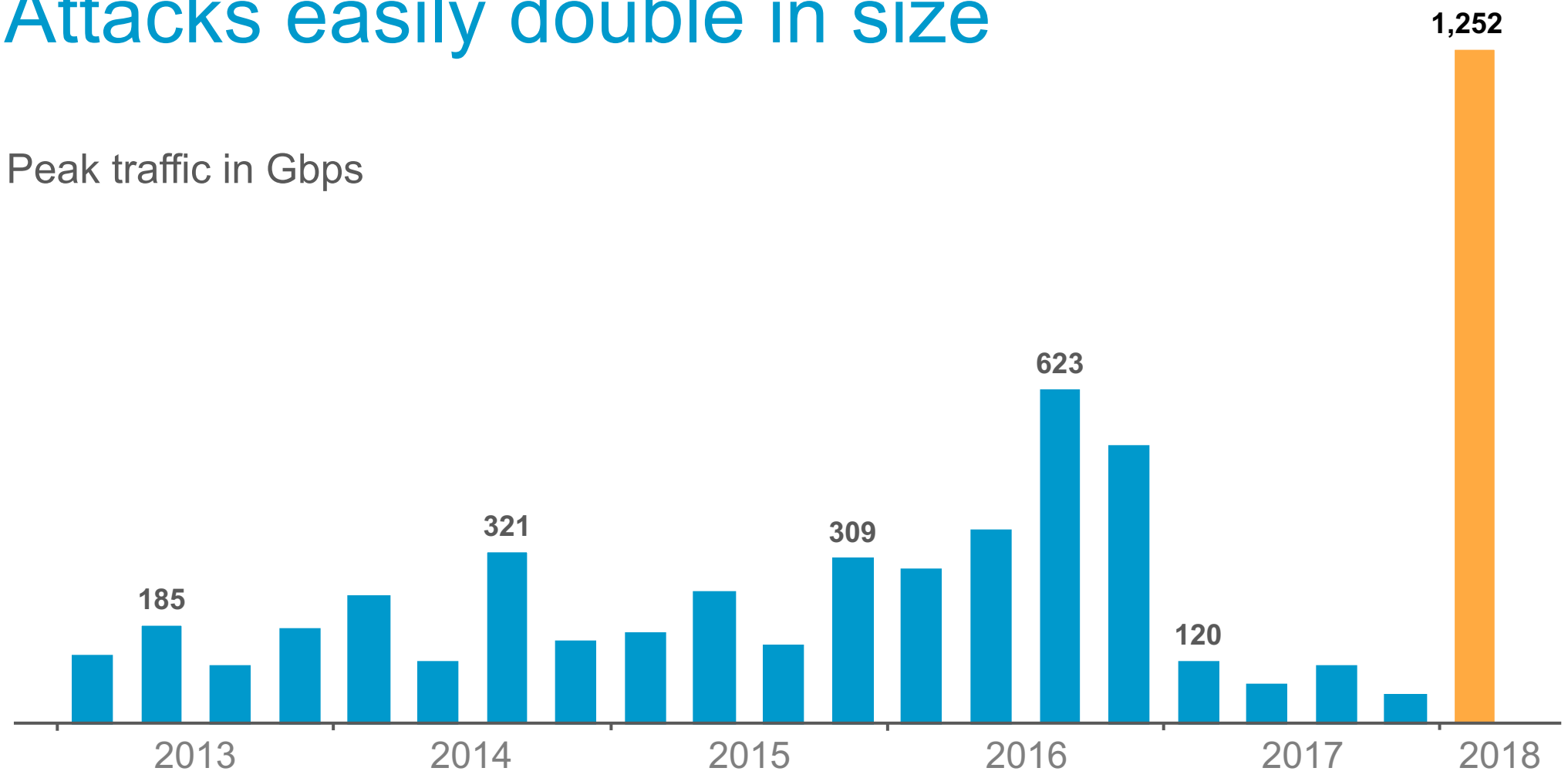
Results of DDoS attacks:

- ✓ **Flooded networks**
- ✓ **Overloaded infrastructure**
- ✓ **Distributed deployments**

GitHub MIRAI

Source: SOTI DDoS Attack update Summer 2017 vs. Summer 2018

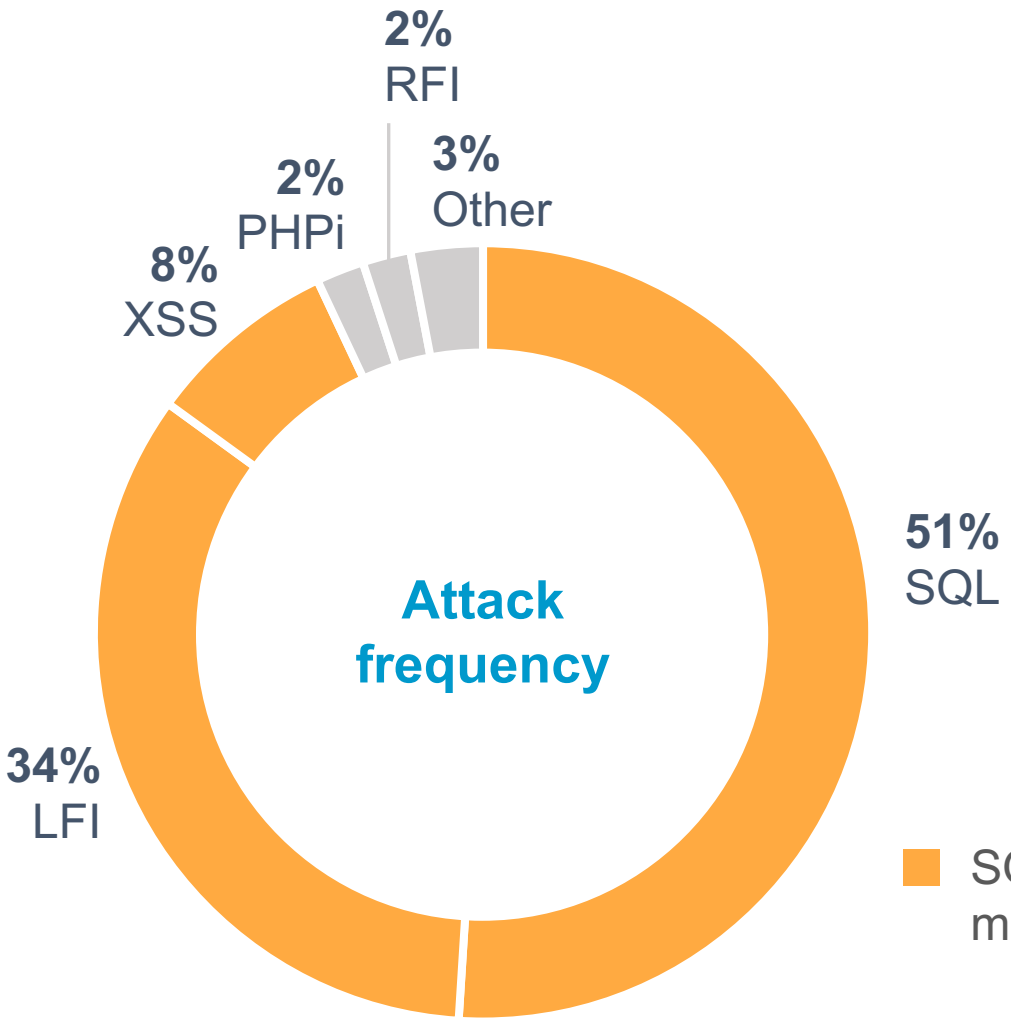
DDoS Attack Trends
Attacks easily double in size



DDoS attacks cost **$25 per hour**

Price Source: CIODIVE

Web Application Threats



Well-known attack vectors:

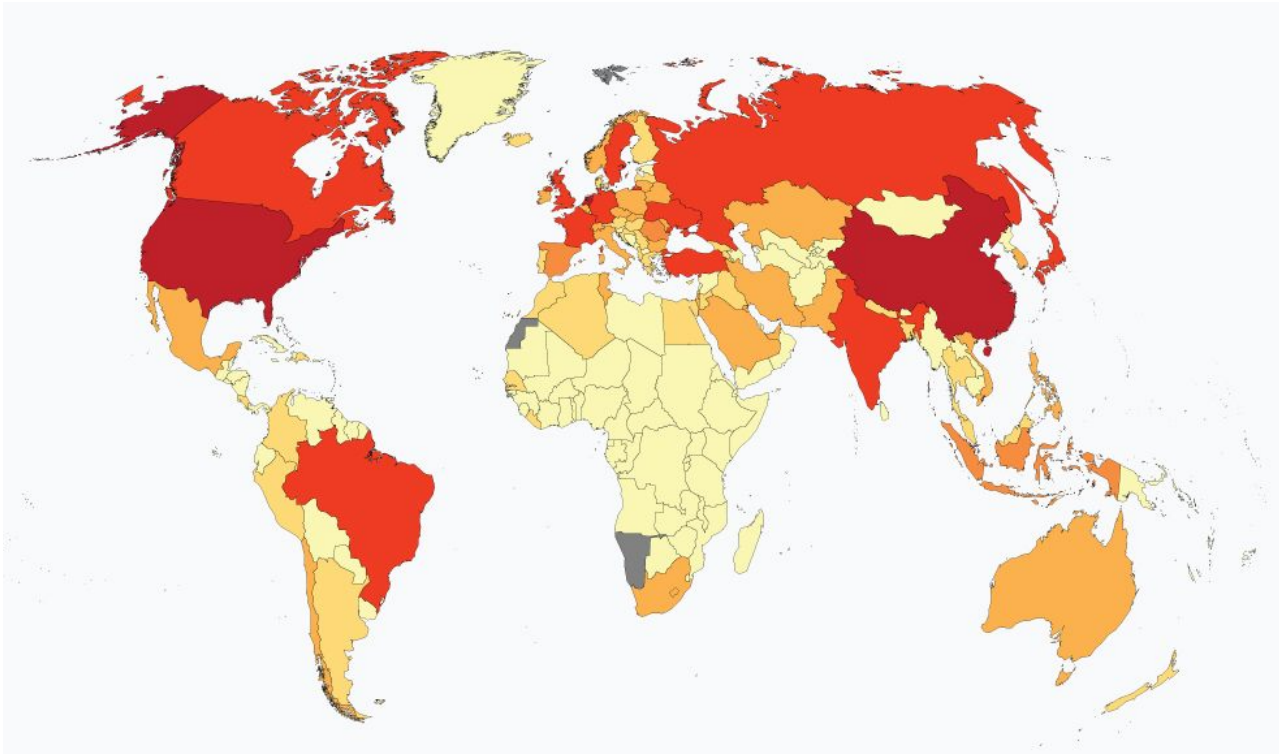
- ✓ **Are frequently used**
- ✓ **Create background noise to hide new attacks**

SQL, LFI, and XSS accounted for **93%** of malicious attacks in the most recent period.

Web Application Threats

Attacks are on the rise:

- ✓ **Growing in scale**
- ✓ **Growing in sophistication**
- ✓ **Originating across countries**



Country	Count	Percentage
USA	238m	30%
Netherlands	94m	12%
China	56m	7%
Brazil	49m	6%
Russia	35m	4%

Source countries for web application attacks summer 2018

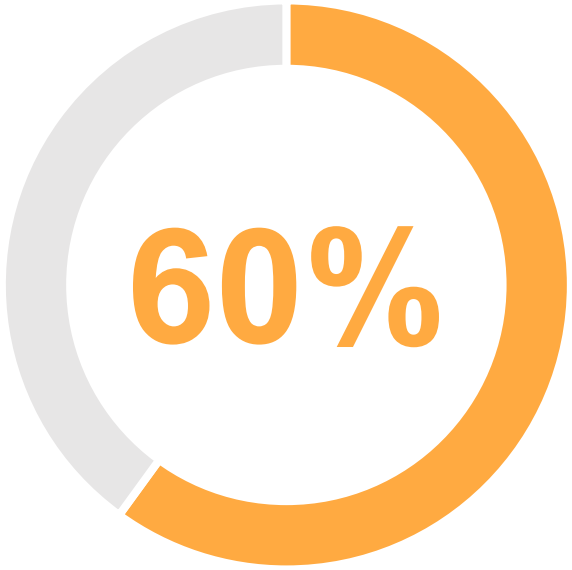
What Does This Mean for Your Business?

Web application attacks represent a large part of the **background noise**

It's difficult to **detect attacks** specifically targeting your business in that noise

Understand your website traffic and business for better **threat detection**

Threat from Operational Complexity
60% of security software remains unused



Top IT challenges are a lack of:

- ✓ **Business alignment**
- ✓ **Time/expertise to implement**
- ✓ **Staff to use product properly**

Source: Osterman Research

The Better Web Application Firewall
Not another thing to worry about

Edge security

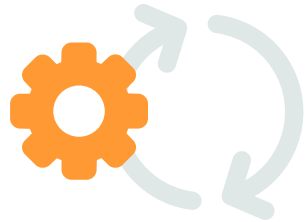
- ✓ **Massive scale to mitigate and absorb attacks**
- ✓ **Insulates from collateral damage by attacks against other customers**
- ✓ **Removes malicious traffic from servers and networks, avoiding overprovisioning costs**
- ✓ **Prevents performance degradation from attacks consuming vital resources**
- ✓ **Delivers better end-user experience with content caching**

The Better Web Application Firewall
Not another thing to worry about

Adaptive threat protection

- ✓ **Maintains accuracy in fast changing threat landscape**
- ✓ **Data driven, best-in-industry research team**
- ✓ **Analysis of 15% to 30% of all internet traffic**
- ✓ **Continuous rule testing and tuning**
- ✓ **Automated rules designed for low false positives**
- ✓ **Special protection with custom rules**

The Better Web Application Firewall
Not another thing to worry about



Simple operation

- ✓ **High degree of automation to increase operational agility and efficiency**
- ✓ **Automated rule updates offload your security teams**
- ✓ **Allows focus of resources and research on your high-value web assets**
- ✓ **Easy-to-read web analytics data in real time**
- ✓ **Dashboards support deep forensic analysis**

The Better Web Application Firewall
Not another thing to worry about

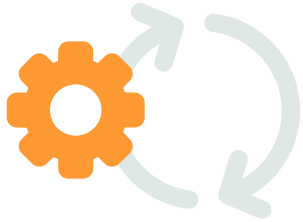
Integration that fits your business needs

- ✓ **Self-service integration for vital protection**
- ✓ **Guided by experts to build a defense-in-depth solution**
- ✓ **Managed services for a complete security solution**
- ✓ **Technical and threat research support when you need it most**

The Better Web Application Firewall
What does it mean?

Edge security for scale and performance

Adaptive threat protection



Simple operation with high automation

Integration that fits your business needs

Web Application Security
Adaptive protection with more than just a firewall

Extend your security perimeter far beyond your site
Scale your defense with a cloud edge WAF

Protect against all network layer DDoS attacks
Reverse-proxy drops all traffic not on port 80 and 443

Refuse requests from countries outside your business
Geo-based blocking of IP addresses

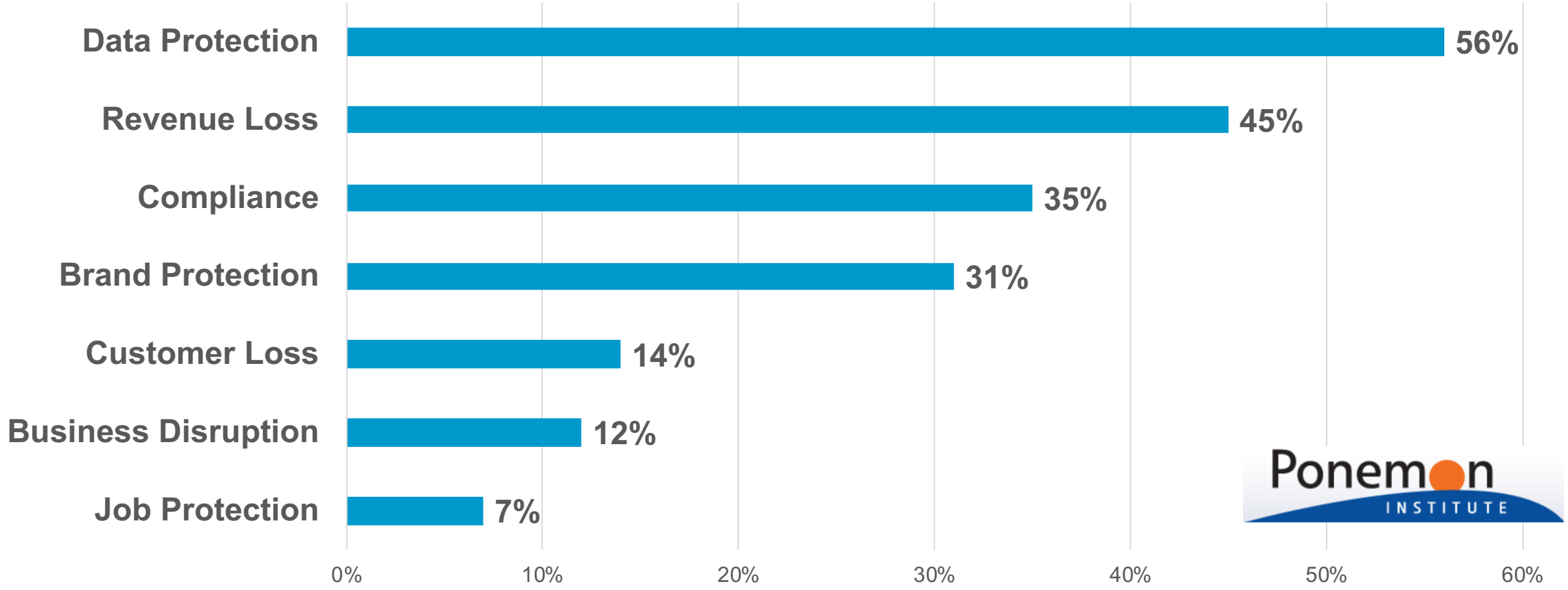
Protect from known attackers
Positive or negative security model (black or white lists)

Protect against application layer DDoS attacks
Rate controls block traffic that acts too fast or too slow

Use best WAF rules in the industry with confidence
Data driven, continuously monitored and refined

Protect content servers, improving end-user experience
Dynamic and static content caching

Web Application Protection
Addressing organizations' top concerns



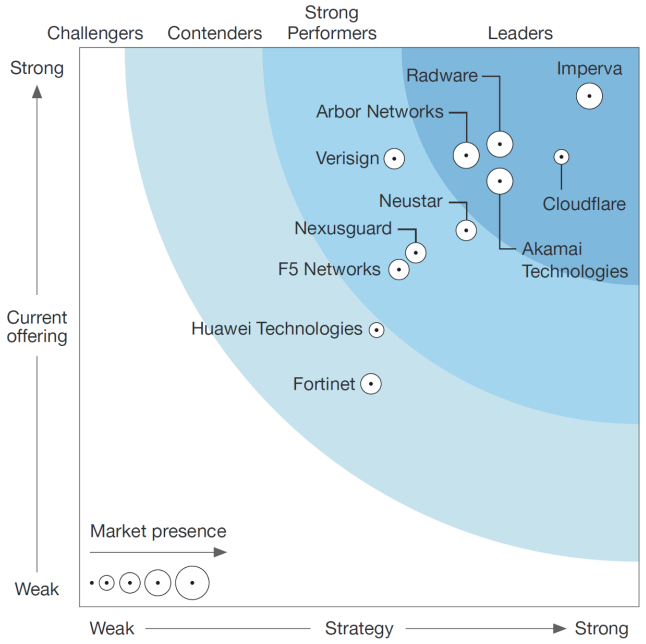
Ponemon INSTITUTE

Source: Ponemon Report 9/17

Market Leader in Security
Named as a leader by Forrester and Gartner

Forrester Wave
Web Application Firewalls, Q2 2018

Forrester Wave
DDoS Mitigation Solutions, Q4 2017



Gartner Magic Quadrant
Web Application Firewalls, Aug 2018

Forrester Wave

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgement at the time and are subject to change.

Gartner Magic Quadrant

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Akamai.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

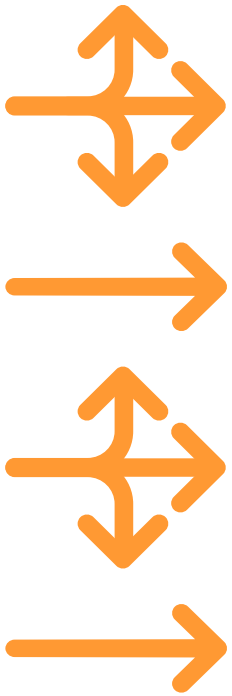
What to Expect
More mature and advanced attacks

- ✓ **Fast-changing threat landscape with new attack vectors, volume and variety**
- ✓ **Attacks tuned to exploit specific vulnerabilities**
- ✓ **Attacks tuned to avoid detection**
- ✓ **Attacking via the API layer**
- ✓ **Zero-day attacks**
- ✓ **Leveraging of bot networks**

Kona Site Defender

Protection against most sophisticated attacks

Attacks



More aggressive protection

Granular rule tuning

Protecting larger footprint

Outbound protection

WAF

Automated rule updates

Customizable rules

Reporting tools

API protection

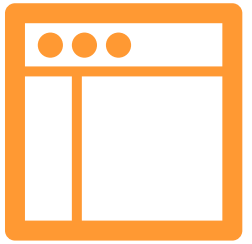
Performance acceleration

DDoS protection

Application protection

Kona Site Defender

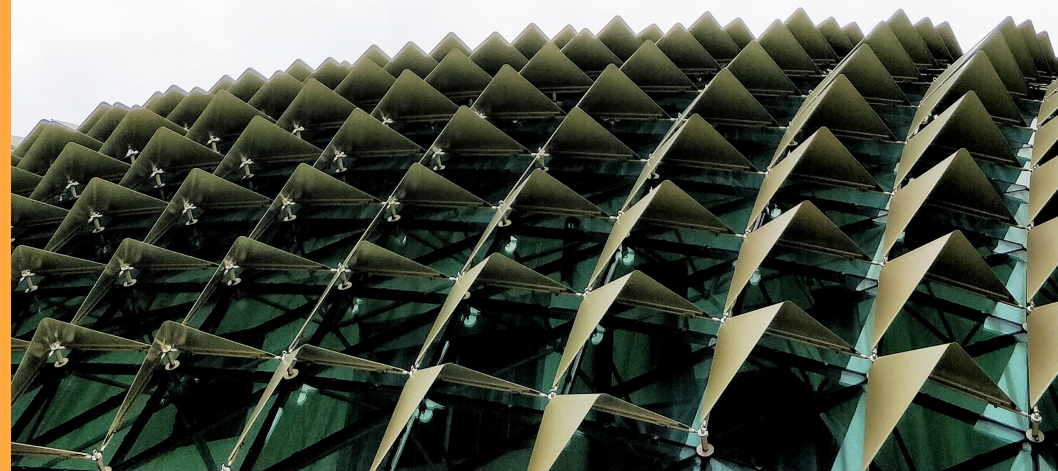
- Robust and customizable protection
- Customized integration
- Self-managed or Akamai managed
- Additional custom rules, whitelists and strong rate controls
- Detailed threat reporting tools for in-depth forensic analysis
- Optional add-ons for additional protection
- Powered by Akamai Intelligent Edge Platform



Your site

Protection against the most sophisticated attacks.

Kona Site Defender




Akamai
Experience the Edge