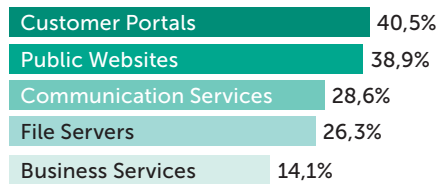# Kaspersky®
DDoS Protection

If your business has ever suffered a Distributed Denial of Service (DDoS) attack, you'll already know that the financial and reputational costs can be devastating. And if you have been lucky enough to avoid an attack so far, you need to be prepared for that luck to run out.
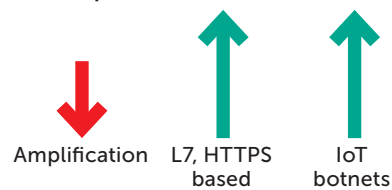
Kaspersky DDoS Protection delivers a total, integrated DDoS attack mitigation solution to ensure business continuity of your critical online resources and infrastructure. From continuous analysis of online traffic, through to alerting you to possible attack and then receiving your redirected traffic, cleaning it and returning 'clean' traffic to you, Kaspersky DDoS Protection provides everything your business needs to defend against – and mitigate the effects of – all types of DDoS attack.

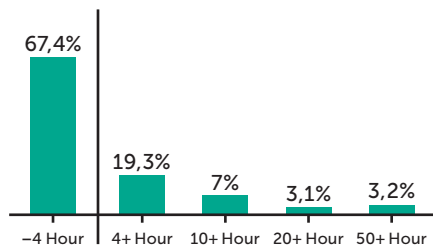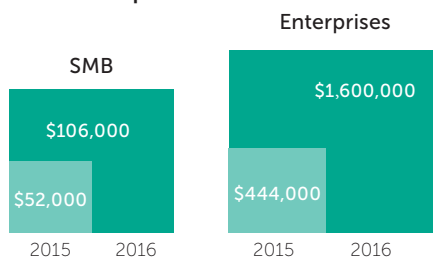## Kaspersky Lab IT Security Risks Surveys 2016

Attack targets

Customer Portals	40,5%
Public Websites	38,9%
Communication Services	28,6%
File Servers	26,3%
Business Services	14,1%

Landscape Attack

Amplification	L7, HTTPS based	IoT botnets

Attack Time

–4 Hour	4+ Hour	10+ Hour	20+ Hour	50+ Hour
67,4%	19,3%	7%	3,1%	3,2%

Financial Report*

SMB

2015	2016
$52,000	$106,000

Enterprises

2015	2016
$444,000	$1,600,000

* Data Security Breaches Caused by DDoS as a "Smokescreen"

Identifying the Danger Better, Faster

Kaspersky Lab's sensor, either installed in our DDoS Protection Cloud or at your premises, gathers data about your traffic, building up profiles of typical visitor behavior and different traffic patterns. Live traffic is then monitored in real time, so that any anomaly indicative of a possible attack can be identified and responded to immediately.

In parallel, our threat intelligence experts are continuously monitoring the DDoS threat landscape, working to identify planned attacks that could be directed your way.

Flexible DDoS Mitigation

The instant a possible attack scenario is identified, experts from the KDP Emergency Response team are alerted. With KDP Connect or Connect+, DDoS mitigation is automatically initiated while our engineers immediately run detailed checks to optimize mitigation depending on the size, type and sophistication of the DDoS attack.

With KDP Control you decide when we should start mitigation in line with your cyber security policy, business objectives and infrastructure environment. It's your business and your online assets we care about and we have the flexibility to address different configurations.
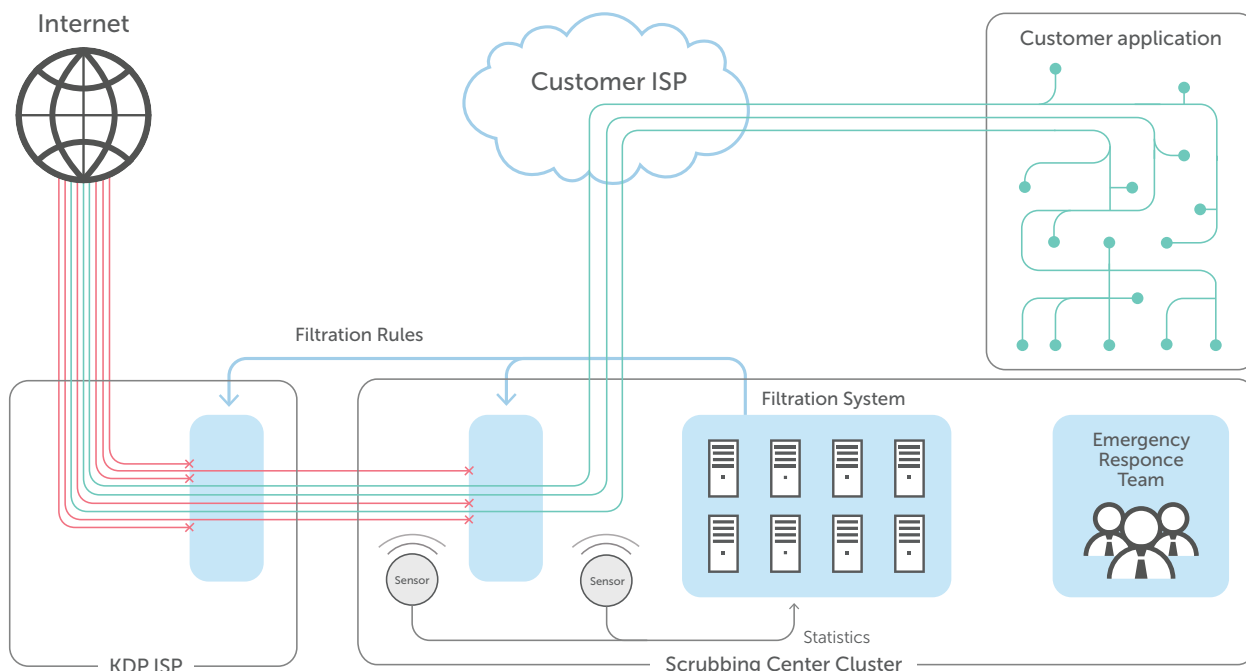
You're Under Attack – and it's Business as Usual

During the attack, with all your traffic passing through our cleaning centers:

* Your infrastructure is no longer being overwhelmed by the sheer volume of 'junk traffic'.
* Our cleaning process is identifying and discarding all junk traffic.
* Legitimate traffic is being delivered straight back to you as 'clean'.

... and the entire process is totally transparent to your employees and customers.

The DDoS attack is effectively neutralized: your business remains fully functional and unaffected.

Internet

Customer ISP

Customer application

Filtration Rules

Filtration System

Emergency Responce Team

Sensor

Sensor

Statistics

KDP ISP

Scrubbing Center Cluster

DDoS Attack Landscape

Kaspersky DDoS Protection is an effective solution to mitigate all types of DDoS attack, such as volumetric **(amplification, direct flood), TCP short-packet, TCP connect, L7 (HTTP) and SSL (HTTPS)**. Each type of attack targets various elements of IT infrastructure – Internet channel, network equipment, applications – and different types of attacks in combination can increase the damage. With our unique combination of continuous traffic monitoring, statistical analysis, behavior analysis and vast experience – plus our KDP Emergency Response team – we can provide protection against all types and combinations of attacks.

Kaspersky Advantage

• Smart and comprehensive mitigation of all DDoS attacks
• Flexible and full coverage of volume attacks
• Unique sensor technology for real-time traffic inspection
• Rapid protection and support by Emergency Response Team 24/7
• Highly scalable cleaning centers in Amsterdam and Frankfurt

---

Select the Right DDoS Mitigation Strategy

DDoS protection products are key in a comprehensive and multidimensional cyber risk management strategy to secure your digital business assets, online services, productivity and reputation in line with your objectives, resources and network infrastructure. Kaspersky Lab offers:
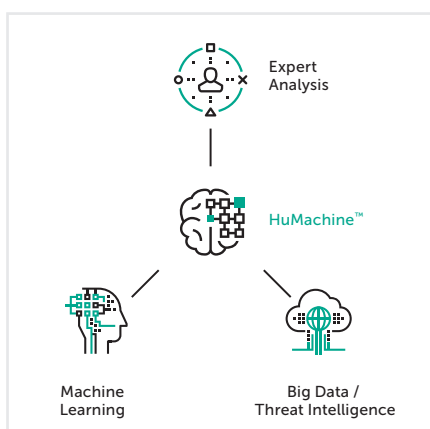
• **KDP Connect** – Always-On DNS traffic Redirection, clean traffic delivery via Proxy, GRE tunnels or leased line
• **KDP Connect +** – Always-On BGP traffic Redirection, clean traffic delivery via GRE tunnels or leased line
• **KDP Control** – On-Demand BGP traffic Redirection, clean traffic delivery via GRE tunnels or leased line

KDP Emergency Response Team

The dedicated **emergency response team** of Kaspersky Lab experts is available 24/7 to monitor anomalies in the client's traffic so the onset of any attack can be detected as soon as possible, and filters can be modified as required. This feature is very important, because cybercriminals can modify their DDoS attacks on the fly to increase the damage. The rapid response from the protection system makes it possible to successfully overcome dangerous changes in the behavior of an ongoing attack.

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com**

To find out more about how to protect your organization against DDoS attacks, please contact your local Kaspersky Lab reseller, or visit **www.kaspersky.com**

www.kaspersky.com