SECURITY SNAPSHOT

SECURITY IN THE CLOUD

KASPERSKY lab

THE GROWTH OF CLOUD USE

19.4% Worldwide spending on public cloud services will grow at a 19.4% compound annual growth rate (CAGR) from nearly $70B in 2015 to more than $141B in 2019.[1]

4 in 5 Nearly four in five respondents are concerned with uploading critical data to the cloud, according to a Dell Data Security Survey.[2]

62% Employees who say that direct and convenient mobile access to corporate information is essential if they are to be productive.[3]

$38,000 The average cost of a data breach for SMBs.[4]

Cloud computing is about access. Anytime. Anywhere.

Most companies understand the enormous benefits of keeping their employees connected while they are away from the office. Whether it's the use of mobile devices that access the cloud or public cloud services for storing important documents, it is vital that employees can pull up the information they need when they need it.

But that access comes with a price. When a single attack against an unprepared business can result in the loss of sensitive data, leakage of confidential information and damage to employee profitability, it's essential that companies protect themselves no matter where they access their data.

Furthermore, since cybercriminals know that large enterprises invest heavily in IT security, they are launching more and more attacks against small- and medium-sized businesses, which they now regard as a soft target. Your sensitive data, your company's privacy and your clients' confidentiality are more vulnerable as the number of attack surfaces increase. Given this complex threat landscape, how can a small- or medium-sized businesses protect that data when it is stored in the cloud? How can a business find the balance between operational efficiency and essential security?

Start by taking a closer look at the areas on the threat landscape where you may be the most vulnerable.

1. Roundup of Cloud Computing Forecasts and Market Estimates 2016
2. Recognize Your Security Shortcomings and Address Them With Confidence
3. Ponemon Institute's "The Security Impact of Mobile Device Use by Employees 2014"
4. Global IT Security Risks Survey 2015

GREATEST AREAS OF VULNERABILITY IN THE CLOUD

When it comes to cloud security, there are a number of areas where you have to make sure you have full protection. The top areas of vulnerability are those that expose more attacks surfaces and present the greatest drain on time and resources.

Data Breaches

Poor authentication standards, weak passwords or limited certificate management processes leave your company more susceptible to a data breach.

ACTION ITEM:
Institute clear guidelines about passwords. Consider implementing two-factor authentication for all areas where you access sensitive data. Manage your software certificates so that no one is working on a pirated or expired certificate.

Hacked Interfaces and APIs

Weak interfaces and APIs open up companies to confidentiality and accountability security issues. This tends to be the most exposed part of a system.

ACTION ITEM:
Be aware that your backend systems could be exposed over the web, especially when you are creating web, mobile and cloud applications. Your backend systems could also be exposed when working with partner or third-party developers of client applications. Have a multi-layered security solution in place to protect these interfaces and scan for breaches.

Patching Vulnerabilities

Unpatched systems and bugs that can be exploited are a huge issue for businesses who rely on the cloud.

ACTION ITEM:
Vulnerability scanning and patching bugs should be an automatic and regular part of the schedule. Choose a security software that includes vulnerability assessment and patch management.

APTs

Direct attacks on businesses through Advanced Persistent Threats are as much of an issue with cloud services as they are on standard networks.

ACTION ITEM:
Protect your system with a multi-layered security system that predicts, prevents, detects and responds to the most advanced threats.

Loss of Productivity

60% of businesses that suffer a data breach find their ability to function severely impaired.[5] With the number of attack surfaces that the cloud opens up, the risk of losing access to important data is high, as is the risk of employees losing time on the job.

ACTION ITEM:
Backups and a centralized cloud management system are an invaluable defense to secure your data, protect your reputation, and help you to focus on your core business.

5. Global IT Security Risks Survey 2015

READY, SET, GO! WITH KASPERSKY ENDPOINT SECURITY CLOUD

Kaspersky Endpoint Security Cloud was developed specifically to address the security challenges that small- and medium-sized businesses face when accessing the cloud.

For businesses with small IT teams or those who outsource their IT security, KES Cloud delivers industry-leading protection that's quick to roll out, easy to run and requires no additional hardware investment.

Even if your IT security resources are tight, you only need to spend 15 minutes with our product for immediate protection of your corporate network.

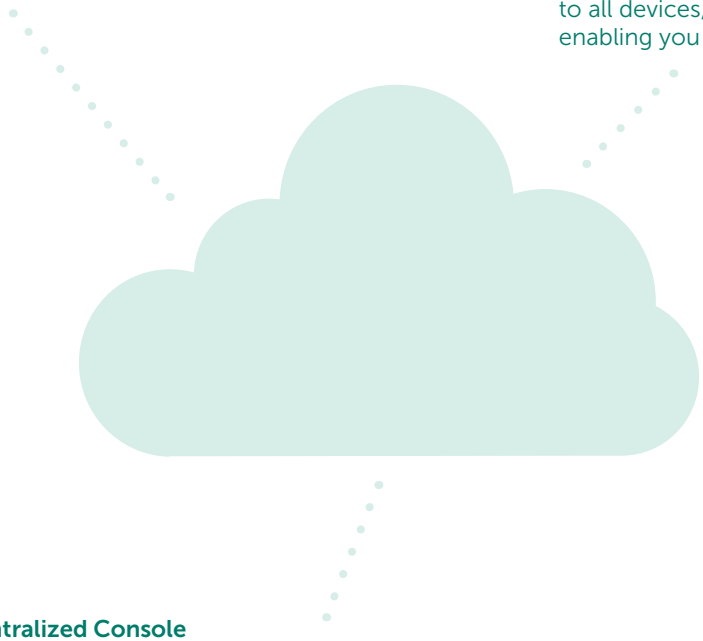
No training, no additional time to manage anything. You're up and running in minutes and protected immediately. Register now for Kaspersky Endpoint Security Cloud.

Ready-to-Run Cloud-Based Console

Manage security for multiple endpoints, mobile devices and file servers remotely, from anywhere, with our ready-to-run cloud-based console. Our web-based console means you have complete control over where and when you need to perform security tasks and maintenance.

Default Security Policies

Developed by Kaspersky Lab experts to provide immediate protection. Security policies are applied to all devices, regardless of type or platform – enabling you to protect users instead of devices.



Centralized Console

Flexible, simple administration capabilities. Because everything is centralized, administrators can monitor the security status of up to 1,000 corporate network nodes from any chosen online device, from any location. Reporting and license tracking are easily managed via a simple, intuitive interface.

Most Tested, Most Awarded Security

For three years in a row, our security technologies have been the most tested and most highly awarded. In a wide range of independent tests, our products consistently achieve more first place awards and more Top 3 ratings than any other vendor's (for details, please see http://www.kaspersky.com/top3).

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

Get Your Free Trial Today >

JOIN THE CONVERSATION


Like us on Facebook


Follow us on Twitter


Join us on LinkedIn


Watch us on YouTube

Review Our Blog

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:

usa.kaspersky.com/business-security

(866) 563-3099

corporatesales@kaspersky.com

KASPERSKY lab

THE POWER OF PROTECTION