KASPERSKY VS. COMPLEXITY: THE BATTLE TO SIMPLIFY IT SECURITY
If you’re charged with IT security at your organization, your plate is already full. You’re likely responsible for Mobile Device Management (MDM); systems management; antivirus; encryption; and/or virtualization security. B2B International’s most recent survey of IT professionals identifies “preventing IT security breaches” as the primary concerns of IT managers, which means your to-do list isn’t getting any shorter. You have to keep your company safe from all current and future threats, a job that’s only getting more challenging.

According to the Ponemon Institute’s 2014 State of Endpoint Risk, “forty-four percent of respondents report a major increase in the number of malware incidents targeting their endpoints.”

---

**Complexity is the Enemy of Security**

Kaspersky Lab’s global team of IT security experts is focused on a single goal: saving the cyberworld. Unlike many of our competitors, we have remained steadfast in our commitment to protect customers from the evolving threat of malware since 1997. Kaspersky employs 2,500 professionals around the globe, including more than 800 dedicated anti-malware researchers and engineers monitoring and investigating the ever-changing threat landscape; developing the best anti-malware solutions; and providing you with the cybersecurity expertise you need to keep your business safe.

2 Ponemon Institute, 2014 State of Endpoint Risk, December 2013
Mobile is clearly on the rise, too, further complicating your IT security. In fact, there’s a very good chance you’re reading this document on your smartphone or tablet right now. With this growing trend comes the prevalence of corporate Bring Your Own Device (BYOD) policies—both official and ad-hoc. By 2016, 38% of organizations will have stopped providing mobile devices to employees, instead allowing employees to choose and use their own devices in the workplace. By 2017, half of employees will be using their own devices for work. At the same time, personal mobile devices used for work-related purposes represent one of the main hazards for businesses: 65% of IT Managers surveyed for a recent B2B International report saw a threat in their company’s BYOD policy.¹

²Ponemon Institute, 2014 State of Endpoint Risk, December 2013


The most frequent types of malware incidents ³

More than one response permitted

<table>
<thead>
<tr>
<th>Type of Malware</th>
<th>FY 2013</th>
<th>FY 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Malware</td>
<td>80%</td>
<td>86%</td>
</tr>
<tr>
<td>Web-borne Malware Attack</td>
<td>74%</td>
<td>79%</td>
</tr>
<tr>
<td>Rootkits</td>
<td>67%</td>
<td>65%</td>
</tr>
<tr>
<td>APTs/Targeted Attacks</td>
<td>54%</td>
<td>58%</td>
</tr>
<tr>
<td>Botnet Attacks</td>
<td>49%</td>
<td>46%</td>
</tr>
<tr>
<td>Spear Phishing*</td>
<td>48%</td>
<td>48%</td>
</tr>
</tbody>
</table>

*This response was not an option in FY 2012

The most frequent types of malware incidents ³

More than one response permitted

<table>
<thead>
<tr>
<th>Type of Malware</th>
<th>FY 2013</th>
<th>FY 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Malware</td>
<td>80%</td>
<td>86%</td>
</tr>
<tr>
<td>Web-borne Malware Attack</td>
<td>74%</td>
<td>79%</td>
</tr>
<tr>
<td>Rootkits</td>
<td>67%</td>
<td>65%</td>
</tr>
<tr>
<td>APTs/Targeted Attacks</td>
<td>54%</td>
<td>58%</td>
</tr>
<tr>
<td>Botnet Attacks</td>
<td>49%</td>
<td>46%</td>
</tr>
<tr>
<td>Spear Phishing*</td>
<td>48%</td>
<td>48%</td>
</tr>
</tbody>
</table>

*This response was not an option in FY 2012

³Ponemon Institute, 2014 State of Endpoint Risk, December 2013

B²B International, Global Corporate IT Security Risks, May 2013
While the number of endpoints is growing, malware is increasing along with it. Forty-four percent of IT managers report a major increase in the number of malware incidents targeting their endpoints. Not a surprise if you look at the facts. Kaspersky Lab detects 315,000 new malicious programs; 30 million spam email messages; and 270 million web-borne infections every single day. And mobile only increases your risk.

Mobile-specific malware is growing exponentially. In 2011, Kaspersky researchers discovered 6193 mobile malware samples. By 2012, that number had increased to more than 30,000 and by April 2013, it jumped to 70,000 pieces of malicious files designed exclusively for mobile devices.

---

5. Ponemon Institute, 2014 State of Endpoint Risk, December 2013

---

What are the biggest threats to endpoint security? 
Two responses permitted

- More multiple mobile devices in the workplace
- More personal devices connected to the network
- More insecure mobile devices in the workplace
- Malware infections are more difficult to detect
- More offsite employees using insecure WiFi
- Employees believe productivity is more important than the security of devices
Just because it originates on a mobile device, doesn’t mean that mobile malware stays there. Because your employees access company networks on their phones and plug their devices into their work laptops and desktops, mobile malware creates risk for the entire organization. Did you know that malicious software introduced to your IT infrastructure via a mobile device can spread to 500,000 devices in just 100 seconds?

Adding insult to injury, while the battle is heating up, you’re being asked to do more with less. In a recent survey conducted by Kaspersky Lab, 70% of IT managers stated that their departments were under-resourced.

Even with an intact budget and a full staff, these are frightening statistics. Holding your security perimeter can feel like an overwhelming undertaking. Sometimes, the adoption of individual tools to address separate vulnerabilities can exacerbate your security concerns, increasing the level of complexity and requiring you to manage multiple platforms. If there are holes everywhere and you can’t see or understand what’s going on, how can you fix the problems? Complexity is truly the enemy of security.

---

9 Yu Zhang, Bharat Bhargava, “Fibonacci Modeling of Malware Propagation,” Purdue University: Purdue e-Pubs, 2008
10 2012 Kaspersky Lab, Survey on Global IT Security Risks
Because corporate IT environments are becoming increasingly complex, the task of managing them is also much more involved and time consuming than ever before. This growing complexity brings many disadvantages for businesses:

- **Increased costs** – More time and effort is being devoted to everyday systems management tasks.
- **Overloaded resources** – The list of regular IT management tasks expands whenever a new device or new software application is introduced onto the corporate network.
- **Impaired agility** – With so many routine IT management tasks filling the working day, there’s less time for IT personnel to help the business to introduce new services that could generate a competitive advantage.

- **Security vulnerabilities** – Manual processes, plus the need to use separate control consoles for different tasks, can create the ideal conditions for operational errors... and those errors can result in serious gaps in security.
- **Lack of visibility** – The sheer complexity of most corporate IT environments is making it difficult for IT personnel to gain a clear understanding of all of the hardware and software that’s operating on their network. Without an accurate view of their entire IT infrastructure, businesses are unable to:
  - Control how their IT estate is being used--to boost efficiency and meet compliance/legal obligations
  - Manage their IT environment – in order to maintain service levels and productivity
  - Secure all of their systems and sensitive data against malware and attacks
As your virtual perimeter expands, and you continue to do business wherever it makes sense on whatever device is at hand, you need protection that can help you reduce the complexity of these IT challenges and safeguard your business at all your endpoints – virtual, physical, and mobile.

But how do you select the right IT security solution for you? At Kaspersky Lab, our experts are on your side to help you reduce the enemy of complexity and fight cybercrime.

Kaspersky Lab’s Endpoint Security for Business; Security for Virtualization; and Mobile Device Management solutions can:

• fully guard your expanding perimeter beyond basic anti-malware protection
• reduce the number of individual tools
• safeguard both physical and virtual servers
• control and patch third-party applications
• establish and administer BYOD and other security policies
• protect and manage all your mobile endpoints
• prioritize fixes from a single console

If the above video does not play, click here.
To request a trial of Kaspersky Endpoint Security for Business, click here and start protecting all your endpoints today.

To learn more, call Kaspersky at 866-563-3099 or email us at corporatesales@kaspersky.com, or visit www.kaspersky.com/business.

© 2014 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners.