

10

TOP THINGS

to look for in a Cloud Security Solution Provider

Searching for a Cloud Security Provider can be confusing. Many providers appear the same at first glance: similar metrics, similar promises. The fact is, the information you need to make a real comparison requires asking questions and probing for details that cloud services vendors don't always volunteer.

Use this list to be sure you've covered the essential elements for choosing the right cloud security provider to protect your organization from malicious cyberattacks.

- 1. Experience:** How long has the provider been in the cloud security business? How many cloud security clients around the world do they have now? (Insight into global attack vectors is useful.) Can they support your business in the way you need?
- 2. Capacity and Scale:** Many cloud security vendors imply they have enough scale, but the way they measure scale matters. You need to know if they can scale when you need them. Ask: What's the largest Distributed Denial of Service (DDoS) attack they can really handle? Can they show you they've actually done so, with real attacks on their network?
- 3. Performance, distribution, and availability:** Does the provider offer fully-integrated cloud security solutions incorporating a global network of servers supported by data-drive algorithms and automation? Can you choose between DDoS scrubbing, CDN networks, or both?
- 4. Collective Intelligence:** Does the cloud security provider have the scale and global traffic volume to generate meaningful intelligence? Are they prepared to leverage this accumulated expertise to benefit their entire customer base if, when, and before they are attacked? Do they use a comprehensive big-data analysis engine to identify a single attacker that may have an impact on other clients?
- 5. IP Reputation:** What sources does the cloud security provider use to assign a reputation score for IP addresses? Some IP reputation products have varying degrees of quality and use a binary risk score: attacker or not, rather than a range of scores based on malicious activity over time.
- 6. Accuracy:** Interpreting accuracy claims from different Web Application Firewall (WAF) vendors is tricky. Comparison between two vendors' accuracy rates is meaningless unless both were measured with the same test. Find out what was tested, who was tested, and how many tests comprise the final result. Make sure you compare apples to apples.
- 7. Continuous Improvement:** The key to accuracy is fine-tuning the rules regularly to stay up to date with evolving traffic. How often does the cloud security vendor test the security infrastructure—monthly, weekly, daily? How much traffic do they use for testing?
- 8. Time-to-Mitigate:** Does the cloud security provider's Service Level Agreement (SLA) commit to speed and quality of mitigation, or just to a response time? Most vendors can promise to respond within minutes, but that only promises an investigation. Specific and contractually guaranteed mitigation SLAs are a tangible metric you can use to compare protection more accurately.

10 Top Things to look for in a Cloud Security Solution Provider

- 9. The Human Factor (Security Operations Centers):** Many vendors claim to protect you with their 24/7 SOC. However, it's crucial to find out how many facilities your cloud security vendor has, where they're located, and how they are staffed. How many people are available at one time? What protocols do they use to ensure you stay covered between shifts during an ongoing attack?
- 10. Multi-layered Defense/Defense in Depth:** No single security solution is 100% effective. But if the tools you're combining are built on the same underlying technology or hardware, you'll have multiple layers with the same weaknesses and gaps for attackers to exploit. The best approach is to layer multiple, best-of-breed technologies on top of each other.

More and more organizations are relying on the cloud for Internet security. Cloud-based security can offer an enterprise more scale, more accuracy, and better performance than an on-premises solution alone. Choosing a cloud security solution to work successfully with your existing security infrastructure requires understanding what's really being offered.

Learn more in Akamai's free ebook, "[Why Cloud? The Buyer's Guide to Cloud Security.](#)"



@Akamai #MobileWeb



Share on Facebook



Post on LinkedIn



As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable, and secure for its customers. The company's advanced web performance, mobile performance, cloud security, and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise, and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.

©2016 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 12/16.