CLOUD SECURITY OVERVIEW

The pure-cloud security solution

Your checklist for pure enterprise protection

From an architectural point of view, a true cloud solution will have key benefits over appliance-based security and hybrid solutions. A pure cloud solution will feature all of the following characteristics:

- ✓ **Device agnostic:** The cloud network should be independent of network gear, user devices, and operating systems. As long as you send your traffic through the cloud network, your users should be protected and your security should "just work."
- ✓ **No hardware, no software:** There should be no investment in infrastructure required to host or run your security solution.
- ✓ **Location independent:** Your security solution should need no pre-knowledge of where your users may show up in order to provide security; it should follow users wherever they go.
- ✓ **Gap-free:** The only way to protect users is to scan every byte traffic that comes in and goes out of your organization, and match it against millions of signatures, behavior patterns, and heuristics in real time.
- ✓ **Multi-tenancy:** With true multi-tenancy, each user is treated with individual policy. So regardless of where the HQ is, users can travel anywhere, use any device, and still get their company's policy locally.
- ✓ **Inline:** Inline security that sits between the user and the Internet is the only way to verify that content is clean and users are secure.
- ✓ **SSL aware:** Most online communications today are SSL encrypted and an increasingly high percentage of threats are hiding in SSL traffic. While many security appliances claim to inspect SSL, they either only inspect content "headers," or they introduce unacceptable latency to the user experience.
- ✓ **Real time:** The cloud network should update the protection capabilities and policy changes for every user and business location in real time.
- ✓ **Comprehensive logging:** The ability to log all Internet traffic activities occurring on behalf of the enterprise but outside its perimeter is one of the most critical capabilities a cloud service must deliver.
- ✓ **Single sign-on/ID federation:** A critical element, because there are simply too many applications to manage without it.
- ✓ **Detailed visibility:** Your cloud service should able to collect logs, correlate them across the world, sequence them, and present them in real time.
- ✓ **Continuous trust:** For every transaction, make sure nothing has changed, and dynamically verify the identity of the user. Change your authentication level and assign a risk level based on the new information. Block the botnet call home and change user access permission.
- ✓ **Behavioral analysis:** Being able to detect virus signatures is not enough; you need to be able to analyze the behavior of a transaction and detect when it behaves differently than expected in order to protect against completely unknown — zero-day — threats.
- ✓ **Layered security:** There is no silver bullet when it comes to security. A layered approach must be taken, whereby all network traffic is assessed from multiple angles, leveraging various techniques to ensure that threats are not missed.
- ✓ **Big analytics:** Powerful analytics and reporting are essential for organizations with strict privacy and other legal reporting requirements.

Learn about secure, scalable Zscaler™ cloud security:
▶ **WWW.ZSCALER.COM**