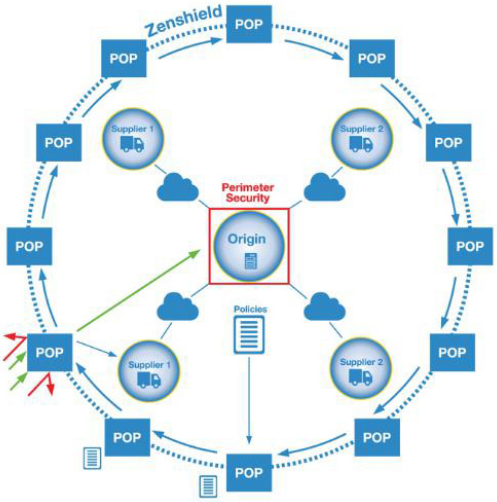
Written by Marco Attard
05 December 2014

Zenedge launches the next generation of its Zenshield DOME platform, a means to protect organisations against cyberthreats aiming to infiltrate by targeting the weakest link in a network chain.



According to Zenshield, Zenshield "applies concentric rings of common-rule security policies and templates to protect against cyber breaches"-- not only of central organisations, but also of connected partners, vendors and suppliers.

In other words, organisations can administer own security policies and oversee suppliers and vendor networks in order to create a cooperative, common-rule cybersecurity policy and template barricade. Meanwhile heuristic algorithms monitor supplier and vendor traffic and dynamically update security policies across the entire ecosystem.

It also vets 2nd and 3rd party systems connecting externally to an internal network, such as client side applications of the CDN, firewall and configuration management variety, thus reinforcing barriers between external client and internal enterprise systems.

"CISOs and hackers are discovering that the quickest path to breaking into a company's classified data comes through remote, often inconspicuous, interconnected 3rd parties, like vendors, suppliers and contractors," the company says. "It's a reminder that networks are only as strong as their least protected link, and that all vendors need to be assessed, vetted and protected against cybersecurity risks."

The Zenedge Zenshield DOME is available now.

Go Zenedge