THE NEXT EVOLUTION IN CLOUD SECURITY

Consistently protect your global organization and cloud applications in every location

Your Users and Applications Have Left the Building

Like many of your employees, Jane is always at work, even when she's not physically in the building. Jane is going where she's needed, such as stopping by field offices and getting face time with clients. She's working when she's at home as well as on the road. Wherever she goes, Jane needs the ability to access all her applications and the security to do so safely while consistently stopping threats and enforcing policies to protect data.

The First Generation of Cloud Security

Unfortunately, many "Cloud Security 1.0" products were designed to address yesterday's problems, and they fall short of fulfilling today's needs. Security should be consistent and comprehensive everywhere Jane goes, and wherever business data lives, but that's just not the case when the protection is different depending upon the locations of applications and users.

The first generation of cloud security consisted of point products that offered specific functionality without a way to coordinate protection. When security doesn't look at the big picture, it can be challenging to see all the ways data can be lost or stolen, or the subtle methods attackers use to hide in the paths least taken.

As a result, the deployment of proxies, secure web gateways, remote access VPN, DNS filtering services, and cloud access security broker (CASB) proxies have led to some security challenges that are difficult to overcome.

- **Blind spots:** Applications can be provisioned instantly in the cloud, creating new data security risks and threat vectors overnight. Traditional cloud security products are incapable of seeing all applications and data, creating policy gaps and blind spots.
- **Threat mitigation:** No application can be presumed safe, and threats to data and users need to be dealt with before they cause harm. You need to know who has access to your applications so you can control where the data goes and stop threats.
- **Deployment and management complexity:** It's difficult to keep adding more point products without creating administrative or budgetary burdens. This becomes worse when considering how to reconcile issues that affect different systems, such as policy changes or incident investigations.

Requirements for Better Security Outcomes

Inconsistent and ineffective protection increases exposure to risk, hurts productivity, and drives up operational expense—and that means it's time for change. The paradigm for cloud security must be reinvented. The next evolutionary step requires new thinking on how to build better protection for all applications, users, and branch offices. What would a better design look like? Next-generation cloud security must address several key needs:

- **Consistent security for applications and data:** Policy gaps and uninspected traffic are vulnerabilities in security posture. Next-generation cloud security must be able to connect and protect all applications, users, and offices in a consistent manner.
- **Flexible deployment models:** The first generation of cloud security was not flexible because it did not account for the wide variations in architecture that must be supported in complex environments. Organizations need flexibility and choice in how they get protection, whether in the cloud or in conjunction with virtualized or physical network security hardware. Next-generation cloud security should deliver security where it is needed, in a manner that doesn't require compromises or apologies for unmet needs.
- **Architecture:** To deal with cloud-scale problems, you need scalability, coverage, and frictionless deployment to make sure you can put protection where you need it.

Palo Alto Networks Next-Generation Cloud Security

Palo Alto Networks delivers upon the vision of next-generation cloud security with GlobalProtect™ cloud service and Aperture™ SaaS security service, enabling you to protect every corner of your organization with the networking and security to cover all your applications, no matter where you or your users do business.

GlobalProtect cloud service and Aperture help you address security in three critical areas:

- **Protect applications and data:** Control SaaS and cloud applications with API and in-line policies to address your CASB needs.
    - Manage shadow IT risk: Take back control over the applications your organization sanctions, tolerates, and blocks.
    - Enforce granular control: Establish who has access to your applications, whether in the cloud or the data center, as well as the methods and conditions for safe access.
    - Classify data and prevent leaks: Know where your business-critical data is, where it goes, and how to keep it safe by tying data security policy to content inspection.
- **Protect branch offices:** Get network security without an on-premises security appliance.
    - Enjoy consistent security: Establish consistent enforcement of security policy at all your locations.
    - Leverage flexible architecture: Deploy cloud-delivered infrastructure or add supplemental coverage with Palo Alto Networks hardware or virtualized security appliances.
    - Transition from Multiprotocol Label Switching (MPLS) to direct-to-internet safely: Support your cloud-first initiatives without the backhaul by securing internet paths from the branch.
- **Protect mobile workforces:** Safeguard all your users in any location.
    - Move past remote access VPN: Replace traditional remote-access VPN with an architecture designed for optimal, secure access to all applications.
    - Get global coverage: Your users work in locations where you may not have an office or data center. Get global coverage through a cloud-scalable infrastructure.
    - Scale quickly, as needed: Mobile users move around, creating variance in the demand at a given location. Automatically allow your cloud infrastructure to adapt to global demand changes.

These are just a few reasons to implement GlobalProtect cloud service and Aperture. Find out how to protect your organization by watching our Lightboard videos here.

GP cloud service

GlobalProtect cloud service – Rock solid security for mobile and branch users

AP

Aperture – Secure the business-critical data within your SaaS applications

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com