GLOBALPROTECT CLOUD SERVICE

Global expansion, mobile workforces and cloud computing are shifting the locations of your applications, data and users. These changes introduce new opportunities for business efficiencies, but they also create a set of unique cybersecurity challenges.

GlobalProtect Cloud Service Snapshot

- Cloud-based next-generation security infrastructure helps minimize the operational burden associated with protecting remote networks and mobile users.
- A shared ownership model lets you focus on managing your next-generation security policies for remote networks and mobile users while Palo Alto Networks manages the security infrastructure.
- Based on the entire suite of PAN-OS-based security features and subscriptions, provides an alternative approach for protecting your distributed network from advanced cyberattacks.
- Reduced operational burden enables you to move your remote location and mobile user security expenditures to a more predictable operational expense (Opex) model.

Remote Network and Mobile User Security Challenges

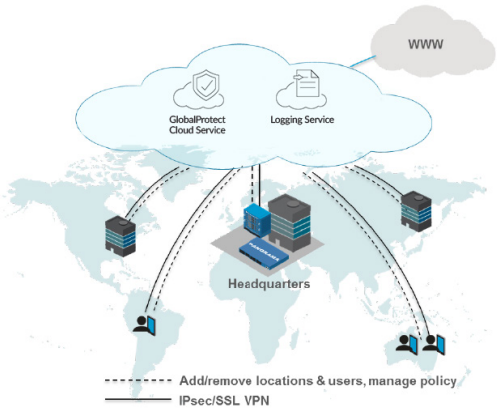
Industry best practices dictate that your security policies should be consistent from headquarters to remote offices to mobile users. Unfortunately, as your workforce and applications become more distributed, delivering consistent security becomes challenging.

- Backhauling and hairpinning are expensive and perform poorly. Funneling remote network and distributed mobile user traffic through the corporate gateway for access to the web or SaaS applications is expensive and often results in poor user experience.
- Alternative approaches result in inconsistent security. Remote networks have a subset of the chosen (corporate) security vendor features, while mobile users bypass or have no security. The end result is inconsistent security.
- Global deployments are complex and cumbersome to manage. For widely distributed organizations, point products from multiple vendors get deployed, leading to complicated management and operations overhead. The end result is costly and delivers inconsistent security.

Palo Alto Networks® GlobalProtect™ cloud service can help eliminate many challenges associated with deploying consistent security to your remote networks and mobile users.

GlobalProtect Cloud Service

GlobalProtect™ network security for endpoints extends Palo Alto Networks Next-Generation Security Platform to your remote networks and mobile users. GlobalProtect cloud service operationalizes next-generation security deployment to remote networks and mobile users by leveraging a cloud-based security infrastructure managed by Palo Alto Networks. Based on our Next-Generation Security Platform, GlobalProtect cloud service is managed by Panorama™ network security management, allowing you to create and deploy consistent security policies across your entire organization.

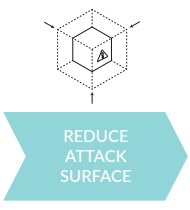


Prevention Philosophy for All Locations and Users

Supported by the entire suite of PAN-OS based security features and subscriptions, GlobalProtect cloud service allows you to implement a prevention philosophy that protects remote networks and mobile users with the same security functionality used to protect your network.

Safely Enable Network Activity

Knowledge combined with enforcement is a powerful security tool. GlobalProtect cloud service gives you complete visibility into all applications in use at remote networks and by mobile users, as well as the content within and the user. Armed with this knowledge, a more consistent security policy can be deployed globally to protect your network from known and unknown attacks.



Reduce the Attack Surface

Using the application identity as a means of enforcing a positive security model reduces the attack surface by enabling only allowed applications and denying all else. You can align application usage to business needs, control application functions (e.g., allow SharePoint® documents for all but limit SharePoint administration access to the IT group), and stop threats from accessing and moving laterally within your network.

Prevent Known Threats

Applying application-specific threat prevention policies to allowed application flows represents a key step in adhering to a prevention philosophy. Application-specific threat prevention policies can block known threats, including vulnerability exploits, malware and malware-generated command-and-control traffic.

Prevent Unknown Threats

Unknown and potentially malicious files are analyzed based on hundreds of behaviors. If a file is deemed malicious, a prevention mechanism is delivered in as few as five minutes. Once the prevention technique has been delivered, the information gained from file analysis is used to continually improve all other prevention capabilities.

GlobalProtect Cloud Service for Remote Networks

GlobalProtect cloud service for remote networks allows you to extend the prevention philosophy for your corporate network to your remote networks, safely enabling commonly used applications and web access. Remote networks are connected to GlobalProtect cloud service via an industry-standard IPsec VPN-capable device or SD-WAN fabric. GlobalProtect cloud service, managed by Panorama, takes advantage of our full suite of Next-Generation Security Platform features. AutoFocus™ contextual threat intelligence and Aperture™ SaaS security can be deployed to complement GlobalProtect cloud service.

GlobalProtect Cloud Service for Mobile Users

Mobile users pose a unique security challenge. They need to access corporate and web resources from any device, yet they need the same protection from threats regardless of location. GlobalProtect cloud service for mobile users enables you to deliver consistent security policies to all users and devices. GlobalProtect cloud service for mobile users interacts with the GlobalProtect app on users' devices to provide user and device information for additive security policy enforcement.

Scalability and Resiliency

GlobalProtect cloud service leverages a cloud-based infrastructure, allowing you to avoid the challenges of sizing firewalls and compute resource allocation, minimizing coverage gaps or inconsistencies associated with your distributed organization. The elasticity of the cloud scales as demand shifts and traffic patterns change. All GlobalProtect cloud service locations are connected through a full mesh VPN without the complexity of configuration, since the only IPsec connection required is from the remote site to the cloud. GlobalProtect cloud service does the rest.

Policy Consistency With Centralized Management

GlobalProtect cloud service is managed using the same Panorama deployment you may already use to manage

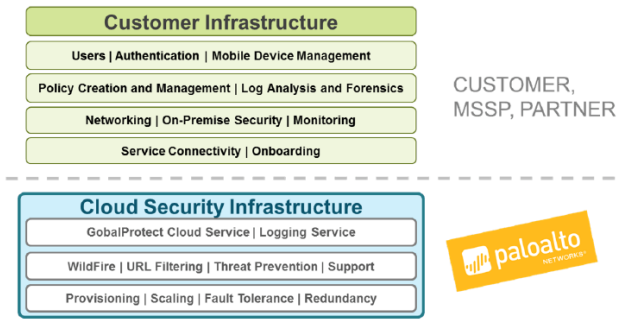
existing Palo Alto Networks physical or virtualized next-generation firewalls. Policies for your remote networks and mobile users can be created using objects in place for your existing firewall deployment, further enhancing operational efficiencies.

Logging and Reporting

Supporting GlobalProtect cloud service is a cloud-based logging service that can be used to collect all logs generated by remote networks and mobile users. Using Panorama, you can query Palo Alto Networks Logging Service for analysis, report generation or incident forensics.

Shared Ownership Model

GlobalProtect cloud service reduces the operational burden of deploying security to remote networks and mobile users through a shared ownership model. Palo Alto Networks manages the infrastructure, ensuring reliability, scalability and availability. Meanwhile, the customer, partner or service provider uses Panorama to focus their efforts on managing location and user onboarding as well as policy deployment.



How It Works

Getting started with GlobalProtect cloud service is simple.

1. Activate GlobalProtect cloud service using an authorization code that will enable the total bandwidth and/or the number of mobile users purchased.
2. Install Panorama and the GlobalProtect cloud service plugin. If Panorama is deployed already, only the plugin is required.
3. Onboard the remote sites with Panorama, assigning desired bandwidth to each location. Onboard mobile users with User-ID or other supported mechanism.
4. Use Panorama to create device groups, then create and deploy security policies to GlobalProtect cloud service.
5. Connect the remote networks and mobile users via IPsec/SSL VPN. For remote networks, SD-WAN is supported as a connectivity alternative.

GlobalProtect Cloud Service Licensing Options

GlobalProtect cloud service includes licensing options for remote networks and mobile users.

- GlobalProtect cloud service for remote networks is licensed based on a bandwidth pool that can be divided among each location with the GlobalProtect cloud service plugin in Panorama. Bandwidth tiers range from 200 Mbps to 100,000 Mbps.
- GlobalProtect cloud service for mobile users follows a similar tiered pricing model based on number of users, with tiers from 200 users to 100,000+ users. GlobalProtect cloud service for mobile users requires the GlobalProtect client or app on each endpoint. Supported endpoints include Microsoft® Windows®, Apple® macOS®, Apple iOS, Android®, Google® Chrome™ OS and third-party client support for Linux®. View a complete list here.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com

globalprotect-cloud-service-ds-060817