# PALO ALTO NETWORKS LOGGING SERVICE

Log analysis is an important cybersecurity practice organizations perform to correlate potential threats and prevent successful cyber breaches. Unfortunately, managing log data on-premise is typically complex and costly. Palo Alto Networks® Logging Service introduces a simpler approach, managing valuable security logs while enabling innovative security applications in concert with Palo Alto Networks Application Framework.

### Logging Service Highlights

- Simplifies operations by eliminating burdensome log management activities.
- Leverages a flexible, cloud-based architecture to improve responsiveness to changing business needs.
- Enables actionable insights through the application of machine learning and advanced analytics to large volumes of data within the Application Framework.

## Challenges

Security products generate large amounts of valuable log data that can be correlated to identify evasive threats and prevent attacks. To convert these logs into actionable information, organizations need an affordable way to store, process and analyze as much log data as possible. Unfortunately, traditional hardware-based log collection comes with administrative overhead and scale limitations that make otherwise useful data unwieldy or unavailable.

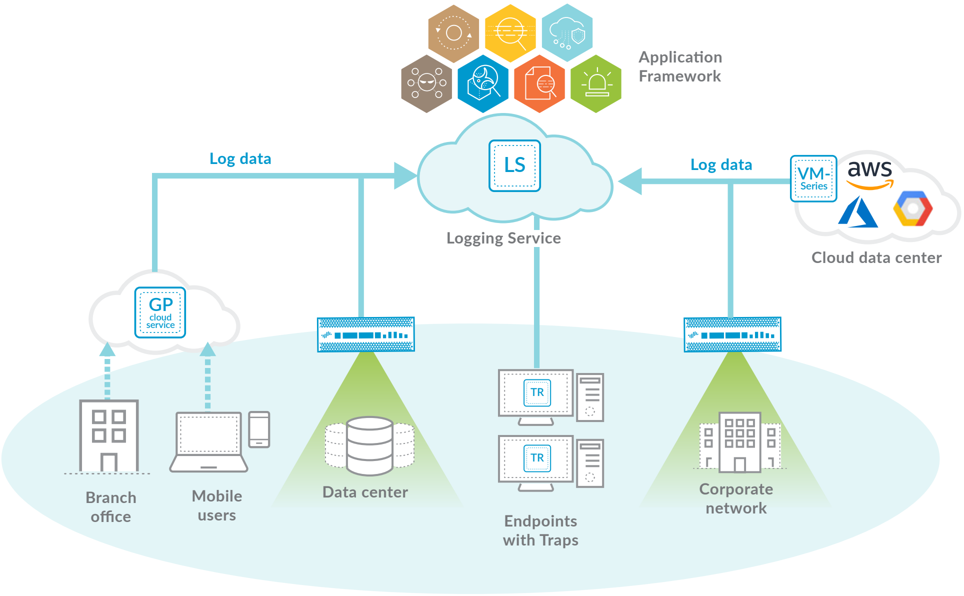
Adversaries constantly change tactics, making it harder to detect attacks. To protect your network, your organization must be able to perform advanced analytics on all available data and detect threats. Security applications that perform such analytics need access to scalable storage capacity and processing power. In the case of hardware-based log management products, such infrastructure and processing power may not be available at the click of a button, making these offerings less responsive to changing business needs.

Assessing the space, power, networking and high availability needs of logging infrastructure takes time and effort. In addition, the agility of organizations depends on the speed of shipping, installing and configuring the hardware. Ongoing maintenance and monitoring of the logging infrastructure take continuous investment of resources, requiring you to deal with activities that aren't core to your business.

## Palo Alto Networks Approach

Palo Alto Networks Logging Service is a cloud-based offering for context-rich enhanced network logs generated by our security products, including our next-generation firewalls, GlobalProtect™ cloud service, and Traps™ advanced endpoint protection. The cloud-based Logging Service lets you collect ever-expanding volumes of data without needing to plan for local compute and storage, and is ready to scale from the start. That means no waiting for the hardware to ship, and no planning for space, power and high availability requirements. Palo Alto Networks handles all the infrastructure needs, including storage and compute, to provide insights customers can use. If you already have on-premise log collectors, the Logging Service complements them by providing a logical extension of log storage to the cloud.

The Logging Service is the cornerstone of Palo Alto Networks Application Framework: a scalable ecosystem of security applications that can apply advanced analytics in concert with Palo Alto Networks enforcement points to prevent the most advanced attacks. You are no longer limited by how much hardware is available or how quickly sensors can be deployed pervasively throughout the network.



| Your Need | Our Approach |
|---|---|
| Central repository for next-gen firewall and cloud services logs | The Logging Service can collect logs from next-generation firewalls of all form factors as well as Traps management service and GlobalProtect cloud service. Logs are available in one location, so it's easy to apply analytics and correlation capabilities to identify threats. |
| Logging infrastructure that scales with changing business needs | The Logging Service was designed to scale quickly, and changes can be made with a few clicks. There's no need to wait for hardware to arrive before you deploy – just order, activate and use. It's that simple. |
| Insight into network, application and user behavior | The Application Command Center – part of Panorama™ network security management – and its reporting capabilities let you drill down into network, application and user behavior. With this level of context, you can make informed decisions about how to eliminate open attack vectors and improve your security posture. |
| Integration with other security infrastructure to gain value | At your prerogative, you can make the data and information hosted by our Logging Service available to your choice of third party or custom security application. You can also automate security workflows using Palo Alto Networks security infrastructure through the Application Framework. With the Log Forwarding app, you can forward log data from Logging Service to third-party log systems, such as security information and event management programs, or SIEMs. |

### Logging Service Requirements

For Palo Alto Networks next-generation firewalls and GlobalProtect cloud service:

- Firewalls and Panorama can connect to the cloud service.
- Firewalls and Panorama have version 8.0.5 of PAN-OS® or above.
- Panorama has the cloud services plugin – available in Panorama and on the Palo Alto Networks Support site – installed.

For Traps advanced endpoint protection:

- Traps management service is required.

### Maintaining Privacy

Palo Alto Networks Logging Service has strict privacy and security controls in place to prevent unauthorized access to sensitive or identifiable information. The service only allows authorized users to view data associated with their organization. You can find further information in the Logging Service Privacy Datasheet.

paloalto NETWORKS®

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