

Strata Logging Service

Enable AI-Based Innovations for Cybersecurity

Identifying and stopping sophisticated attacks requires using advanced artificial intelligence (AI) and machine learning across all your enterprise's data. Current approaches leave data hidden in silos across your security infrastructure, limiting the effectiveness of analytics. As data continues to grow, legacy hardware-based deployments can't scale, which introduces operational burdens and high costs—all with limited capacity that makes useful data unwieldy or unavailable.

Benefits

- Collect, integrate, and normalize your enterprise's security data.
- Apply advanced AI and machine learning with cloud-scale data and compute.
- Constantly learn from new data sources to evolve your defenses.

Strata Logging Service

Strata™ Logging Service enables AI-based innovations for cybersecurity with the industry's only approach to normalizing and stitching together your enterprise's data. Get public cloud scale and locations with assurance of the security and privacy of your data. Significantly improve the accuracy of security outcomes with trillions of multisource artifacts for analytics. Strata Logging Service can:

- Radically simplify your security operations by collecting, integrating, and normalizing your enterprise's security data.
- Effortlessly run advanced AI and machine learning with cloud-scale data and compute.
- Constantly learn from new data sources to evolve your defenses.

Never Worry About Complexity or Scale Again

Deploying massive data collection, storage, and analysis infrastructure is complex. You need to plan for space, power, compute, networking and high availability needs, increasing costs, and operational burden. Once deployed, the infrastructure needs ongoing maintenance and monitoring, taking time away from activities that drive your business forward.

Strata Logging Service is built to benefit from public cloud scale and locations. The cloud-based service is ready for elastic scale from the start, eliminating the need for local compute and storage. As your needs grow, you can add more capacity with the push of a button. The public cloud architecture lets you take advantage of global locations to solve local data residency and privacy requirements. Infrastructure—including storage and compute—is handled for you, letting you focus on solving new security challenges.

Unified Data That Continues to Expand

Organizations often lack the visibility they need to stop attacks. Data is typically locked in silos across cloud, endpoint, and network assets, preventing tools from effectively finding, investigating, or automating threat response.

Strata Logging Service is the industry's only approach to normalizing and stitching together your enterprise's data. It automatically collects, integrates, and normalizes data across your security infrastructure.

Strata Logging Service



Collect, integrate, and normalize your enterprise's security data combined with trillions of multisource artifacts for AI and machine learning.

Global Threat Intelligence



WildFire® is a malware prevention service that collects trillions of constantly growing threat artifacts from tens of thousands of independent organizations.



Cloud Identity Engine provides user and group context from cloud and on-premises directory infrastructure.

Figure 1: Strata Logging Service data sources

You Need To	Strata Logging Service
Stitch together your enterprise's security data	Collects data from GlobalProtect®, Palo Alto Networks Next-Generation Firewalls, and Prisma® Access.
Scale your data collection needs	Benefits from public cloud scalability and agility, with capacity increases available in a few clicks. You don't wait for hardware—just order, activate, and use.
Easily access normalized data for advanced AI and machine learning	Automatically normalizes data in a consistent format, ensuring the effectiveness of large-scale analytics.
Integrate with third-party security tools	Lets you choose to make your data available to third-party security tools via syslog servers, HTTPS servers, or email notifications via log forwarding.

Size Your Deployment

Use this [calculator](#) to determine the storage you need.

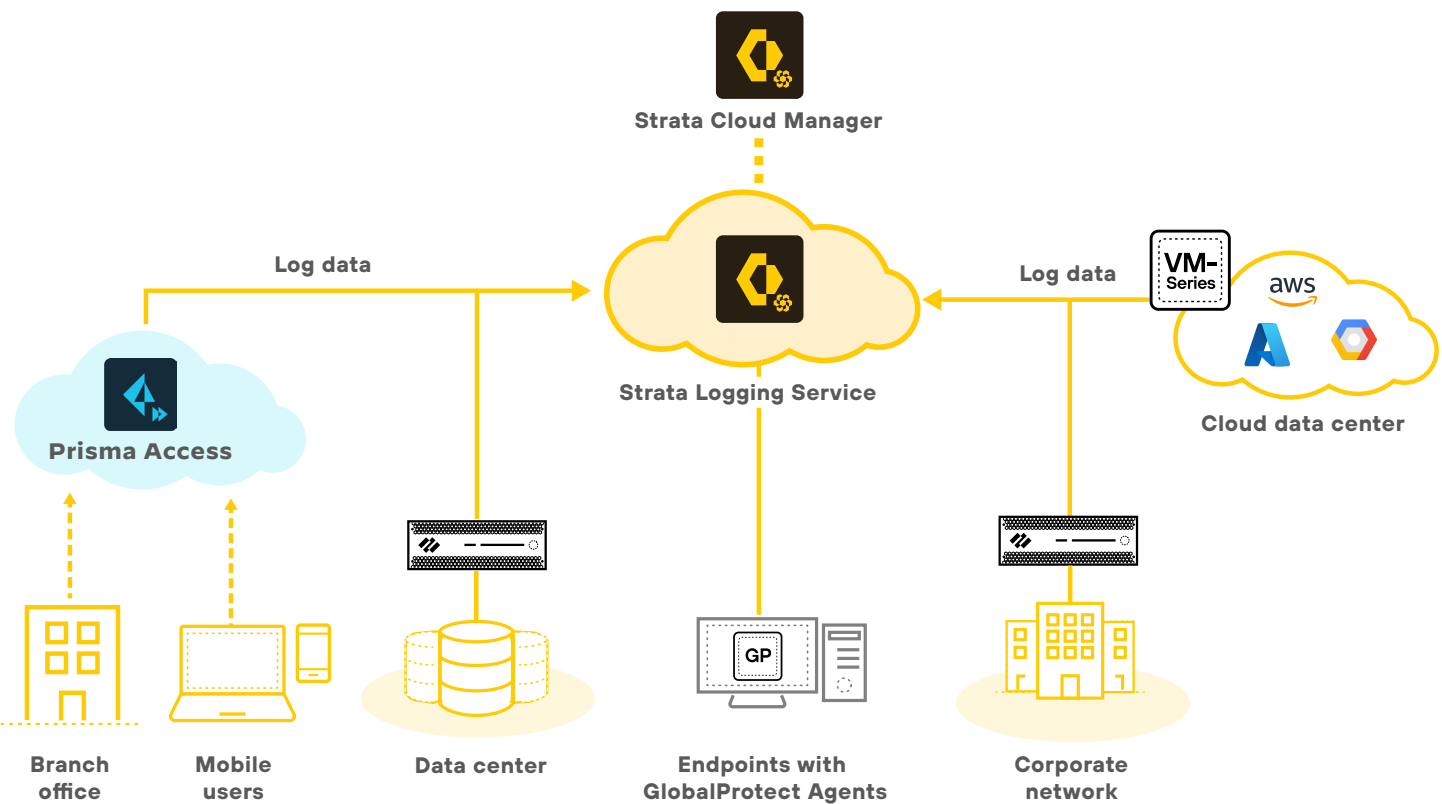


Figure 2: Strata Logging Service integration

Trust and Privacy

Strata Logging Service has strict privacy and security controls in place to prevent unauthorized access to sensitive or identifiable information. Strata Logging Service ensures the privacy of your data by limiting access to your authorized users and apps, which you can revoke at any time. The Strata Logging Service infrastructure is secured with industry-standard best practices for security and confidentiality, including rigorous technical and organizational security controls.

Strata Logging Service is hosted in SOC 2 Type II-compliant data centers, with data encrypted in transit. You can find additional information in our [privacy datasheets](#).

Products That Use Strata Logging Service and Their Requirements

Palo Alto Networks Next-Generation Firewalls and Prisma Access:

- Next-Generation Firewalls and Panorama® network security management with the ability to connect to the cloud service
- Next-Generation Firewalls and Panorama running PAN-OS® 8.0.5+
- Panorama with the Cloud Services plugin installed
- Strata Cloud Manager



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

© 2024 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
strata_ds_strata-logging-service_050224