

CORTEX DATA LAKE

Enable AI-based innovations for cybersecurity

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.

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 siloes 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.

Part of Cortex

Cortex™ is the industry's only open and integrated AI-based continuous security platform. It delivers radical simplicity and significantly improves security outcomes through automation and unprecedented accuracy.

Cortex Data Lake

Cortex Data Lake 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 multi-source artifacts for analytics. Cortex Data Lake 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 learns 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.

Cortex Data Lake 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 with apps built on Cortex.

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.

Cortex Data Lake 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. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Tight sensor integration allows new data sources and types to be continually added to evolve your defenses.






Cortex Data Lake	Global Threat Intelligence
 <p>Collect, integrate, and normalize your enterprise’s security data combined with trillions of multi-source artifacts for AI and machine learning.</p>	 <p>WildFire® is a malware prevention service that collects trillions of constantly growing threat artifacts from tens of thousands of independent organizations.</p>
	 <p>AutoFocus™ is a contextual threat intelligence service that further enriches WildFire data with context and classification, including tags for malware families, adversaries, campaigns, exploits and malicious behavior. Statistical analysis is performed on all artifacts to determine their prevalences and uniqueness.</p>
	 <p>MineMeld™ is a threat intelligence syndication engine that enables aggregation and indicator management from any source of third-party threat intelligence.</p>
	 <p>Directory Sync provides user and group context from on-premises directory infrastructure.</p>

Figure 1: Cortex Data Lake data sources

You Need To	Cortex Data Lake
Stitch together your enterprise’s security data	Collects data from Cortex XDR, Palo Alto Networks Next-Generation Firewalls, Traps™ management service, 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 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 format or email notifications with the Log Forwarding app.

Size Your Deployment

Use [this calculator](#) to determine the storage you need to support innovative apps and services across Cortex and Palo Alto Networks.

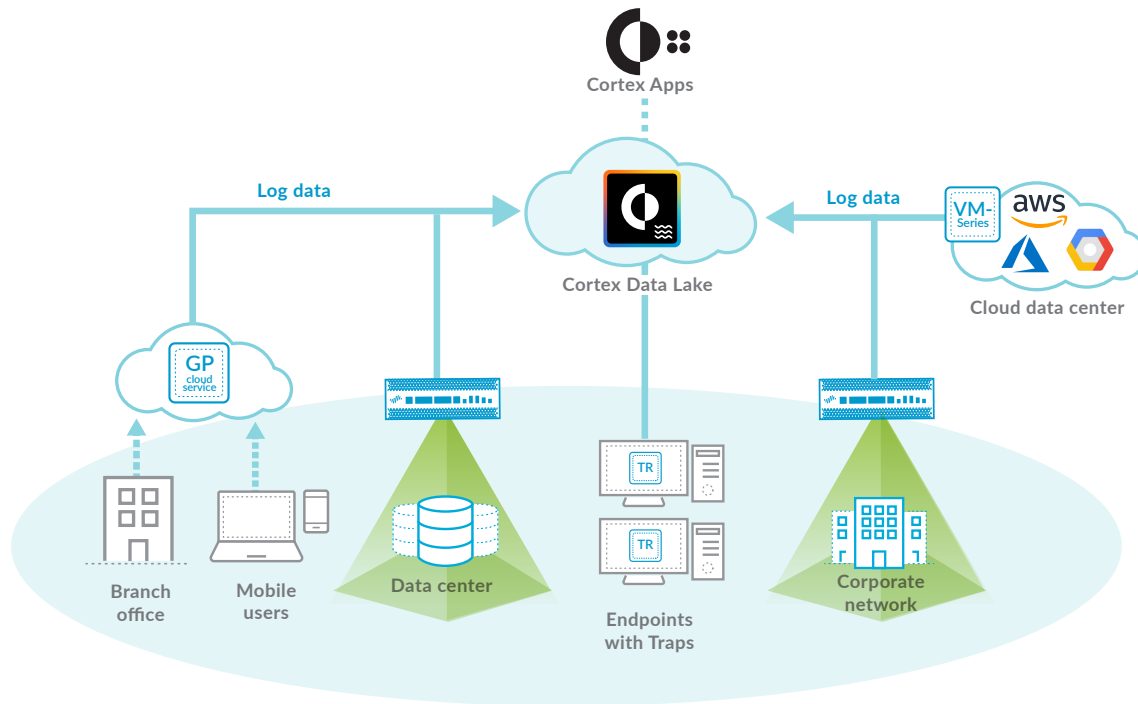


Figure 2: Cortex Data Lake integration

Trust and Privacy

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

Cortex Data Lake is hosted in SOC 2 Type II-compliant data centers, with data encrypted in transit. Customers authenticate to apps that are part of the Cortex Hub using single sign-on, including two-factor authentication. You can find additional information in [our privacy datasheets](#).

Products That Use Cortex Data Lake and Their Requirements

Palo Alto Networks Next-Generation Firewalls and Prisma Access:

- Next-Generation Firewalls and Panorama™ for 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.

Palo Alto Networks Traps for endpoint protection and response:

- Traps running version 5.0+ with Traps management service

Cortex XDR:

- Cortex XDR application (Traps agent included)

Licensing Information

- Cortex Data Lake is licensed separately and required for use of Cortex and associated apps.