~~Palo Alto Networks Traps~~

~~Traps™ provides advanced endpoint protection that secures endpoints with a multi-method prevention approach that stops malware and exploits, both known and unknown, before they compromise endpoints, such as laptops, desktops and servers.~~

Palo Alto Networks Next Generation Firewall License Subscriptions

Next Generation Firewall License Subscriptions provide the following additional functionality to Palo Alto Networks Next Generation Firewalls:-

License	**Description**
Threat Prevention	For antivirus, anti-spyware, vulnerability protection. Includes built-in external dynamic lists that can be used to secure networks against malicious hosts and the ability to identify infected hosts that try to connect to malicious domains.
DNS Security	Full access to the continuously expanding DNS-based threat intelligence produced by Palo Alto Networks.
URL Filtering	Ability to not only control web-access, but how users interact with online content based on dynamic URL categories.
WildFire	Enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding, as well as the ability to upload files using the WildFire API.
Autofocus	Graphical analysis of firewall traffic logs and ability to identify~~ies~~ potential risks to your network using threat intelligence from the AutoFocus portal.
GlobalProtect	Mobility solutions and/or large-scale VPN capabilities. A license (subscription) is required for advanced GlobalProtect features (HIP checks and related content updates, the GlobalProtect Mobile App, IPv6 connections, or a GlobalProtect Clientless VPN).
Virtual System	Enables support for multiple virtual systems on firewalls that support virtual systems.
Decryption Broker	Allows the offloading of SSL decryption to the Palo Alto Networks next-generation firewall,~~and~~ so ~~decrypt~~ traffic can be decrypted only once. A firewall enabled as a decryption broker forwards clear text traffic to security chains (sets of inline, third-party appliances) for additional enforcement.

Palo Alto Networks Panorama

Panorama network security management enables you to provision firewalls centrally and use its functionality to create effective security rules as well as gain insight into network traffic and threats. As a centralized management system, it provides global visibility and control over multiple Palo Alto Networks next generation firewalls.

Palo Alto Networks Prisma Access

Prisma Access enables consistent security by safely enabling your users to access cloud and data center applications as well as the internet whether they are at your headquarters, branch offices, or on the road. Prisma Access consistently inspects all traffic across all ports, enabling secure access to the internet, as well as to your sanctioned SaaS applications, public cloud environments, and data centers and headquarters.

Palo Alto Networks Prisma SaaS

Prisma SaaS security service allows you to govern sanctioned SaaS application usage across all users in your organization to prevent the risk of breaches and non-compliance. It scans and analyzes all your assets and applies policy to identify potential risks associated with each asset. The service also performs deep content inspection and protects both your historical assets and new assets from malware, data exposure, and data exfiltration. ~~As the service identifies incidents, you can assess them and define automated actions to eliminate or close the incident.~~

Palo Alto Networks Prisma Cloud

Prisma Cloud provides visibility and threat detection to mitigate risks and secure workloads in a heterogeneous environment (hybrid and multi-cloud) with a single integrated platform by providing:

-

- ~~Providing~~ visibility, automation, detection and response across any compute, network or cloud service, with hundreds of out-of-the-box governance policies that help ensure compliance and enforce good behavior, and~~.~~
- ~~Addressing issues early and preventing alert fatigue by seamlessly integrating security early and throughout the application lifecycle~~
- ~~Leveraging~~ continuous vulnerability management and automated risk prioritization ~~across the entire cloud native stack and lifecycle~~.

Cortex Data Lake

Cloud-based, centralized log storage and aggregation of the context-rich enhanced network logs generated by Palo Alto Networks security products, including Prisma Access.

Palo Alto Networks Cortex

Underpinned by Cortex Data Lake Cortex provides centralized analysis, reporting, and forensics across all users, applications, and locations. ~~Underpinned by Cortex Data Lake which stores the context-rich enhanced network logs generated by Palo Alto Networks security products, including Prisma Access, for use by Cortex apps.~~

- Cortex XDR applies machine learning at cloud scale to network, endpoint, and cloud data, to enable you to quickly find and stop targeted attacks, insider abuse, and compromised endpoints.

Cortex XSOAR is an orchestration engine that is designed to automate security product tasks and human analyst tasks / workflows to help security teams build future proof security operations.

-

Palo Alto Networks Enterprise ~~Licence~~License Agreements

Enterprise License Agreements are volume licensing arrangements that can help~~s~~ organizations buy, consume, and manage the above Palo Alto Networks ~~the above~~ portfolio of services. Certain services and features may not be available or may not be available in all jurisdictions for access through an Enterprise License Agreement.