The Value of Cortex XDR Analytics and Prisma Access

A firewall, whether on-premises with Palo Alto Networks NGFWs or cloud-delivered with Prisma® Access, provides market-leading network threat protection, traffic inspection, and segmentation—also known as trust boundary enforcement.

With the dissolution of the perimeter, the network has evolved to embrace the cloud, and defense has had to move closer and closer to the user, identity, privilege, or device. The rise of Zero Trust has created the concept of inspecting everything and everyone, every time a connection is made. This now means that access is granted based on the who, what, why, when, and how of that particular moment.

Once the connection is established though, then what? How can the trust granted in the established connection be monitored to ensure the trust is not being abused?

Machine Learning Derived Analytics

This is where analytics can help. Machine learning-derived analytics can establish baseline models that learn normal behavior for a user, for a device, for traffic, and uniquely with Prisma® Access, *for a remote access tunnel*.

With these analytic engines, one can monitor the behavior of the user, device, traffic, and remote access tunnel on a continual basis, a concept that is extremely complementary to Zero Trust and can detect when these various trusts begin to act anomalously.

The value of network traffic anomaly detection cannot be underestimated, as it:

- Ties the architecture together with insights across trust boundaries.
- Detects compromised and unmanaged systems in the data center and remote sites.
- Provides anomaly detection at the application layer with no agent or instrumentation on the endpoint.
- Allows for the correlation of alerts and events between systems across the extended architecture end-to-end.

Cortex XDR

Cortex XDR® is uniquely positioned to take advantage of the cloud-centric architecture of Prisma Access and the ability for on-premises NGFWs at remote sites and individual endpoints to be connected to the same data lake for an end-to-end consolidation of telemetry collection. With this telemetry in the same place, behavioral analytics can create a baseline and monitor the end-to-end aspects of a Zero Trust architecture on a continual basis.

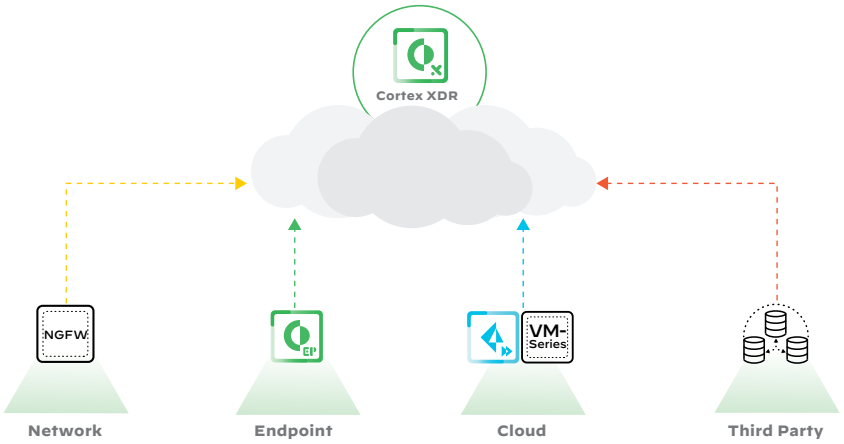

Figure 1: Cortex XDR collects and analyzes data from virtually any source

What Cortex XDR Brings to Prisma Access

The following matrix describes the benefits of adding Cortex XDR's behavioral analytics to complement Prisma Access.

Table 1: Cortex XDR + Prisma Access vs. Other SASE

Support Feature	Other Secure Access Service Edge (SASE)	Prisma Access	Prisma Access + Cortex XDR
Network Anomaly Detection - NTA	No	No	Yes
User Anomaly Detection - UBA	No	No	Yes
Entity Anomaly Detection - UEBA	No	No	Yes
Extended End-to-End Visibility	No	Network Only	Yes
Correlation with User Authentication	No	Yes	Yes
Inspection of All Ports and Protocols	Limited	Yes	Yes
Integrated Sandbox	Yes	Yes	Yes
Coordinated Firewall Response (EDL)	No	Yes	Yes
SSL Decryption	Yes	Yes	Yes
Dissolvable Endpoint Forensic Package	No	No	Yes
Supports End-to-End Zero Trust	No	Network Only	Yes

As described in the table above, Cortex XDR:

- Provides network traffic access (NTA) to both in-transit and over-the-tunnel traffic, and at the remote sites
- Provides user behavior analytics (UBA) by correlating user authentication of the remote session and the privilege/user of a remote site system
- Ingests and stitches Windows® Event Logs for entity anomaly detection, (UEBA)
- Provides a dissolvable forensics package that can be dropped onto an endpoint that is displaying anomalous network behavior
- Supports end-to-end Zero Trust monitoring by stitching together remote sites, remote users, remote devices and network traffic across local networks, trust boundaries and over remote access tunnels

A full list of the analytics-based detections Cortex XDR brings to Prisma Access includes:

- Authentication attempt from a dormant account
- DNS tunneling
- Failed DNS
- Failed login for locked-out account
- Failed login for a long username with special characters
- Kerberos pre-auth failures by host
- Kerberos pre-auth failures by user and host
- Multiple weakly encrypted Kerberos tickets received
- Random-looking domain names
- Weakly encrypted Kerberos ticket requested
- Failed connections
- High connection rate
- Large upload (FTP)
- Large upload (HTTPS)
- Large upload (SMTP)
- New administrative behavior
- Possible DCShadow attempt
- Possible DCSync attempt
- Recurring rare domain access
- Spam bot traffic
- Kerberos traffic from non-standard process
- RDP connection to localhost—for increased accuracy, you can also add the following optional data source: XDR agent
- Rare SSH session
- SMB traffic from non-standard process
- Script connecting to rare external host

Conclusion

Prisma Access is a compelling and powerful remote access product that is uniquely suited to the way business IT architectures are evolving within today's cloud-first paradigm.

The combination of Prisma Access's class-leading threat inspection, network segmentation, and remote access with Cortex XDR's network traffic analytics, user and entity behavior analytics, and network-triggered dissolvable forensic endpoint inspection extends the features of both products to support a tightly integrated, end-to-end Zero Trust architecture.

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