Palo Alto Networks Integration with Azure Information Protection

Enforce DLP policies on assets protected with Azure Information Protection

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: Aug 24, 2022

Table of Contents

The Challenge

With today's growing remote workforce and cloud transformations, there is increasing complexity due to growth in structured data like databases and unstructured data like emails, documents etc. In order to stay secure, it is imperative for organizations to protect those. Enterprises are facing increasing complexity, more administrative effort and incomplete protection of sensitive data – whether on the network, in the cloud or in the hands of the remote users.

Benefits of Integration:

With this integration, Prisma Access can detect documents that are using Azure Information Protection labels, allowing customers to enforce policies at the network level that can prevent sensitive information from being sent outside of the customer's organization. These policies can be applied to remote offices and mobile users who are connecting to the corporate network via GlobalProtect or Prisma Access. Customers can leverage AIP labels to create and enforce Prisma Access DLP policies in order to mitigate chances of data theft, data exfiltration or inadvertent loss of data.

1. **Increased Visibility:** The customer will get more visibility into the document/ sensitive data flow through the network beyond just the Microsoft ecosystem

2. **Enhanced Security:** Customers can leverage pre configured labels to enforce DLP policies. Prisma Access can enable policy enforcement for assets protected by Azure Information Protection

3. **Shared Classification Context:** Due to syncing of Azure Information Protection's labels, duplication of efforts in two different platforms will be reduced

Azure Information Protection (AIP): Control and help secure email, documents, and sensitive data that you share outside your company. From easy classification to embedded labels and permissions, enhance data protection at all times with Azure Information Protection—no matter where it's stored or who it's shared with.

Prisma Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. By integrating with existing security infrastructure and leveraging ML and crowdsourced intelligence from the global community, Next-Generation CASB is able to automatically discover and control all SaaS and data risks across all users from every location, whether the corporate office or remote.

Use Cases for Integration with Azure Information Protection:

Use Case 1:

Increase visibility of labeled document flow through your network beyond M365 applications

Challenge: Enterprises want to identify and protect sensitive and confidential data. Not having full context of changes in access levels or file transfers can result in missing out on important changes which could've helped admins take preventative actions.

Solution: Prisma Access can help enhance visibility into AIP labeled documents beyond just the Microsoft 365 applications. This will enable the customer to have increased context of the movement of the document and can accordingly take remedial action like removing access, if necessary.

Example: If a "confidential" file is moved from One Drive to Box, Prisma Access will be able to provide that visibility through the logs.

Use Case 2:

Enforce data loss prevention policies by leveraging AIP labels

Challenge: With the rise of digital assets, the need to track, monitor and be proactive about access of these assets (files, documents or emails) is becoming more pertinent. Customers are leveraging tools to enable labeling and classification of assets which can help enhance data protection. However, manually keeping track and preventing data loss or exfiltration is becoming increasingly challenging.

Solution: Prisma Access Next-Gen CASB can help in keeping track of sensitive assets and data movement and can also help enforce preventative policies to mitigate risk and auto remediation.

a) **Data in motion:** With synced labels and label IDs, Prisma Access DLP policies could alert/ block uploading actions based on tags from AIP. Customers can also check for pre-configured DLP patterns to find sensitive information like Credit Card number and SSN etc in the AIP labeled documents for the supported applications.

b) **Data at rest:** Prisma Access can take already synced DLP profile(s) and use it in a data at rest policy where if someone shared a sensitive file publicly on a supported Saas application like OneDrive, our SaaS API could detect that, detect the AIP tag, and a policy could auto remediate this issue by removing the public link.

Use Case 3:

More granular inspection and querying for data at rest

This integration will also enable the customer to view and query the data based on data patterns combined from DLP and AIP.

Example: The customer can see a list of all confidential files (AIP tag) that also have credit card details (DLP pattern) in the document

About Microsoft

Microsoft Corporation is a multinational computer technology corporation that develops, manufactures, licenses, and supports a wide range of software products for computing devices. For more information, visit www.microsoft.com

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com