

Managed Detection and Response (MDR) for Cloud Apps Shadow IT

Overview

Cynode's MDR for Cloud Apps Shadow IT is an innovative service designed to (1) prevent data exfiltration and unauthorised access of cloud apps (shadow IT) to business data, (2) detect and respond to unusual activities, misconfigurations, suspicious behaviour and malware activity on our customer's own SaaS applications such as Google Workspace, Microsoft Office 365, Salesforce.

Given the difficulty in limiting the use of SaaS applications and the immediate business benefits they offer, their adoption has surged. Threat actors exploit this trend by employing various attack techniques, starting from initial access, privilege escalation, and lateral movement, all the way to exfiltration and impact across the SaaS exposure of corporations.

Utilising our customers' Cloud Access Security Broker (CASB) infrastructures, this service:

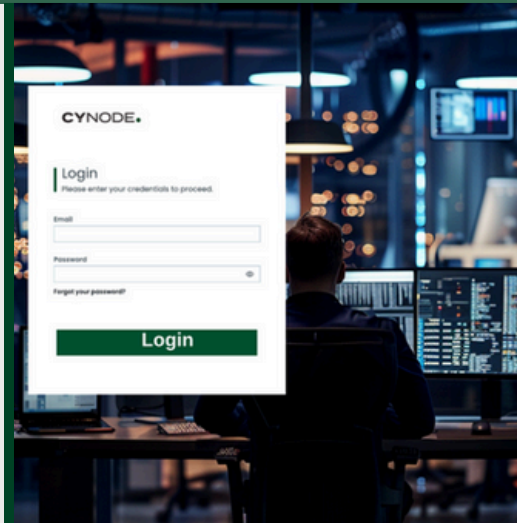
- helps determine whether to approve, sanction, or deny user requests for SaaS applications
- detects and responds to unauthorised SaaS application usage on a 24/7 basis
- detects and responds to potentially malicious activities within collaborative SaaS applications such as Microsoft 365, Google Workspace, Salesforce, Box, Slack on a 24/7 basis
- analyses and continually improves security policies.

Problems Cynode's MDR for Cloud Apps Shadow IT Service Solves

- Controlling cloud app usage is extremely demanding, encompassing CASB, identity management, and internet access traffic analysis. It involves policy compliance monitoring, application usage analysis, access rights review, and auditing data access by users and devices across the entire network estate and thousands of SaaS applications. This heavy load often results in high operational costs or underutilisation of the CASB investment.
- Traditional security measures (such as restricting local admin rights, network access control and application control) struggle to provide visibility into shadow IT activities, which introduces security blind spots, increases risks of data leakage, and often violates data protection regulations and compliance standards, exposing organisations to fines, legal liabilities, and damage to your reputation.
- Users in general casually grant permissions to third-party apps (to achieve their business goals), allow access to their account information and data in other cloud apps.
- External collaboration, file sharing, massive data reviews, downloads, or unusual activities on cloud applications may indicate organisation level security breaches or attack preparations. A lack of this visibility leaves organisations vulnerable.

Supported CASB Platforms

- Microsoft Defender for Cloud Apps
- Proofpoint Cloud App Security Broker
- Netskope CASB
- Skyhigh Security
- Palo Alto Networks Next-Gen CASB
- Zscaler CASB



Key Facts

- SaaS apps such as CRM, email marketing, digital design, collaboration tools and many others are easily accessible over the Internet either with free or monthly subscription options. These applications offer immediate business solutions and significantly enhance business efficiency.
- Various public statistics available on the internet indicate that the average number of SaaS applications used per user exceeds 20 in small enterprises and is significantly higher in larger companies. The average number of SaaS applications used per company is over 250.
- Broad consent policies of SaaS vendors, users' neglect of security concerns, hacker-developed tools for access and impersonation, and the use of unapproved SaaS (shadow IT) necessitate strict control over SaaS usage.

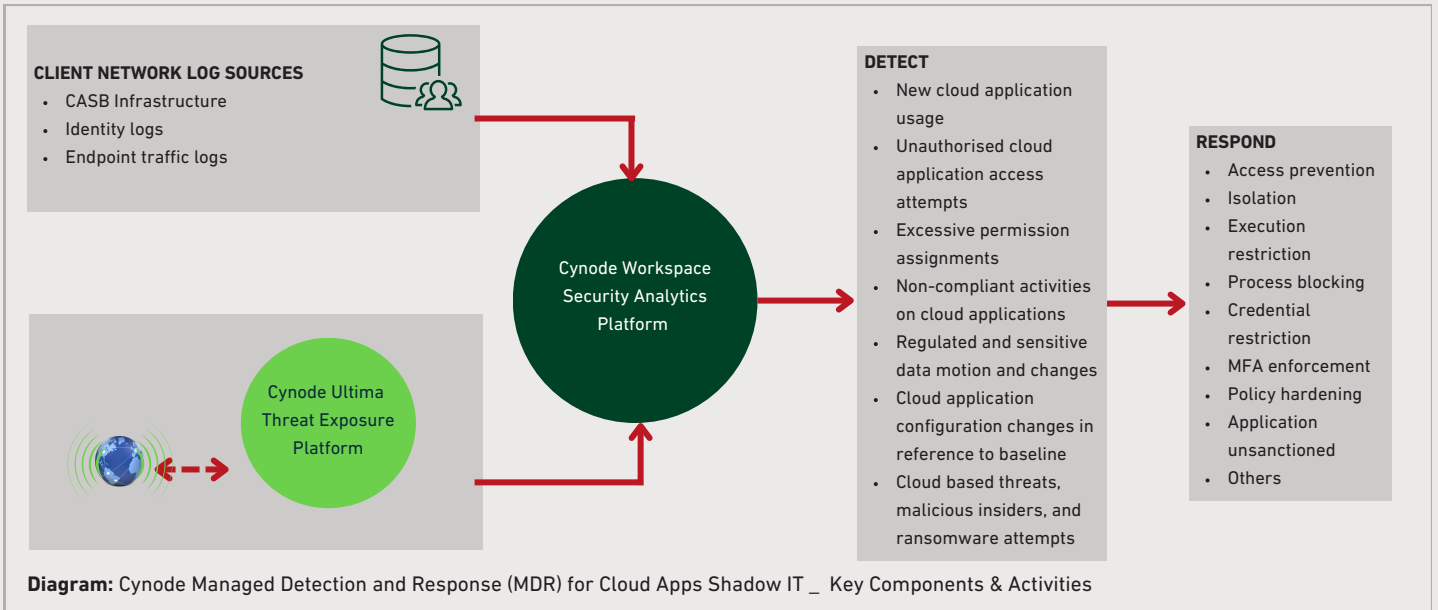
How It Works

Cynode leverages our customers' CASB infrastructures to continuously monitor user and file activities, usage of internal and external collaboration applications, information sharing, compliance, and authorisation policies on cloud applications. The service enhances the CASB solution application visibility by adding identity and network traffic context to detect rogue or non-compliant apps usage.

Cynode assesses and optimises the policies on CASB solutions integrated with customers' subscribed SaaS apps to detect misconfigurations, unusual activities, unauthorised access, and employees' casual actions.

Cynode's Workspace Security Analytics Platform aggregates alerts generated by governance and anomaly detection policies on CASB solutions and correlates these alerts into cases based on affected assets or cloud application entities. This approach helps identify malicious activities with similar patterns, lower the number of cases that to be handled and ensures timely response.

Onboarding Phase	<p>The service starts with prerequisite onboarding phase that includes posture analysis and policy hardening. The onboarding phase includes the following operations:</p> <ul style="list-style-type: none"> • users posture analysis • device posture analysis • discovery and assessment of cloud apps • limiting exposure to shared data • enforcing collaboration policies 	<ul style="list-style-type: none"> • discovering classified, labeled sensitive data stored in cloud apps • misconfiguration analysis • improving detection visibility on CASB <p>Onboarding phase provides visibility of assets, assesses policies and configurations, and identifies critical vulnerabilities and misconfigurations across our customers' CASB infrastructures. It also offers a comprehensive remediation plan.</p>
Detection Phase	<p>Cynode MDR for Cloud Apps Shadow IT service monitors user and file activities, external and internal collaborations, information sharing, compliance, and authorisation policies on cloud applications to detect:</p> <ul style="list-style-type: none"> • new cloud application usage • unauthorised cloud application access attempts • excessive permission assignments • non-compliant activities on cloud applications • regulated and sensitive data motion and changes • cloud application configuration changes in reference to baseline • cloud based threats, malicious insiders, and ransomware attempts <p>The service acquires alerts and incidents from the CASB infrastructure via an API collector, storing them on the Cynode Workspace Security Analytics Platform. These alerts and incident logs form the foundation for detection on the platform, consolidating alerts into cases while identifying affected assets and threat entities.</p> <p>Alerts are correlated based on affected assets, threats, or cloud application entities, and prioritised according to severity, impact, and relevance to the organisation's security posture. This phase of the service involves</p>	<p>applying the Workspace Platform's own rules, which are based on MITRE tactics and incorporate various techniques.</p> <p>The Workspace Platform provides a comprehensive narrative of unusual and non-compliant activities within the cases, encompassing all associated activities found in the alerts. The platform offers customer dashboards to report the detection of threat activities and displays the impact based on the affected assets.</p> <p>Additionally, Cynode analysts evaluate new cloud applications detected by the Workspace Platform to determine the app's risk level and compliance status relevant to our customers' cloud app governance policies.</p> <p>The risk level of the application is defined based on the following criteria to assist in making sanction or denial decisions:</p> <ul style="list-style-type: none"> • general app information • security posture • compliance status according to best practices and frameworks • legal liability



Response Phase

Cynode coordinates incident response efforts across IT, security teams to ensure a unified and timely response to the security attacks.

Cynode Workspace Platform provides response plan with customer negotiated automated actions that include the following Workspace playbooks:


- isolate the relevant user accounts.
- deny non-compliant and risky cloud applications.
- update the list of banned cloud applications.
- stop or block sensitive data sharing
- secure collaboration with external users


Cynode Workspace notifies the stakeholders with enhanced and verified content, providing guidance and support on list of mitigation actions.


Key Benefits

- Gain complete visibility into SaaS application usage by your users
- Assess the consent policies as per the security governance policies.
- Prevent Shadow IT
- Detect suspicious activities that takes place in collaboration tools such as Google Workspace, Salesforce, Slack, Microsoft Office 365 (including Onedrive, Sharepoint, Teams, etc.).


OTHER CYNODE MDR SERVICES


 Managed Detection and Response for Endpoint


 Managed Detection and Response for Microsoft Defender

 Managed WebApp Exposure Monitoring

 Managed Detection and Response for Cloud

 Managed Phishing Detection and Response

 Managed Detection and Response for Identity Protection

 Managed Business Email Compromise Detection and Response