

Cloud and SaaS Security Posture Management (CSPM & SSPM)

Automatically identify, prioritize and fix security risks across cloud environments and SaaS applications

Cloud computing and SaaS Applications Open Companies to Risk

The proliferation of cloud environments and SaaS applications used across organizations has made it difficult for security teams to ensure that each is properly configured to reduce risks. Not only must each cloud service and SaaS application be configured correctly upon installation, but it must be continuously monitored and assessed to ensure that any routine changes do not inadvertently weaken the desired security posture.

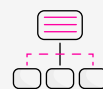
The Solution: Cloud Service and SaaS Application Security on Autopilot

Cynet CSPM/SSPM ensures that your cloud services and SaaS applications are properly configured to protect them from compromise and breaches. By continuously monitoring for variations between your stated policies and actual security posture, Cynet CSPM/SSPM lets you automatically find and fix security risks. Cynet 360 AutoXDR™ provides a single pane of glass to automatically identify, prioritize and track misconfigurations across all of your cloud services and SaaS applications.

Key Benefits



Continuous visibility into cloud service and SaaS app misconfigurations



Prioritize issues by risk severity



One-click to fix configuration errors



Track open and closed configuration issues



Reporting on configuration drifts

Automatically Track Cloud and SaaS Risks

Track security posture issues across all cloud services and SaaS platforms, prioritized by risk category, and closely tracked over time directly from your existing Cynet dashboard.



Analyze and Fix Issues with a Single Click

Drill down to the exact details and insights for each identified risk, see recommended remediation actions and fix issues with one click.

Severity	Service	Category	Subject	Current Value	Secure Value	Compliance	Actions
Medium	Dropbox	User Protection	Enable Two-Step Verification	False	True	HIPAA, ISO27001, PCI, CIS	Fix, Ignore, Mark as fixed, Export all issues to Excel, Export selected issues to Excel
High	Dropbox	Data Protection	Sharing with External People	Allow	Not Allow	HIPAA, ISO27001, PCI, CIS	
High	Dropbox	User Protection	Password Strength is moderate or higher	Minimal	Not minimal	HIPAA, ISO27001, PCI, CIS	
High	Dropbox	Data Protection	Harden Send Invite Policy	Everyone	Not Everyone	HIPAA, ISO27001, PCI, CIS	
Medium	Dropbox	User Protection	Web Session Length	More than 1 day	1 day	HIPAA, ISO27001, PCI, CIS	
High	Webex	Data Protection	Auto Lock Personal Room	Auto Lock Not Enabled	Auto Lock Enabled	HIPAA, ISO27001, PCI, CIS	
Medium	AWS	Data Protection	Ensure there are no EBS Volumes unenc...	eu-west-1: vol-0bfb4c...	Success	HIPAA, PCI, FFIEC, GDPR, APRA, MAS, NIST	

High | **Dropbox** | **User Protection** | **Password Strength is moderate or higher** | **Minimal** | **Not minimal** | **HIPAA ISO27001 PCI CIS NIST**

Description

Use a moderate or strong password. This means using a combination of upper and lower case letter, numbers and symbols while avoiding reusing the same combination of characters from other services. Dropbox suggests using "non-standard uPPercasing, creative spelling, personal slang, and non-obvious numbers and symbols (using \$ for s or o for o is too obvious!)." However trying to remember a lengthy and unique password is a challenge, particularly if you have a different one for every service. This is where password managers comes in. They will remember all your passwords for you and you will have to just remember a single password in order to access all your accounts.

Current Configuration

Current Status:
Password Strength: minimal_requirements

How to Fix Manually

To change the password strength policy go to → Admin Console → Settings → password control change to "ON" and change accordingly















Simplify Compliance

Automatically align critical cloud and SaaS security controls to meet regulatory and industry compliance requirements.

Severity	Service	Category	Subject	Current Value	Secure Value	Compliance / Standards
High	Office 365	Spam & Phishing Prevention	Limit Internal Recipients	[N/A]	800 or 1000	HIPAA
High	Office 365	Spam & Phishing Prevention	Limit Internal Recipients Strict	[N/A]	800	HIPAA
Medium	One Drive for business	Data Protection	Control access based on network locatio...	False	True	HIPAA ISO27001 PCI CIS
Medium	One Drive for business	Data Protection	Enable conditional access support in the ...	AadObjectId	empty list	HIPAA ISO27001 PCI CIS NIST
Medium	Google Workspace	User Protection	Require 2-Step Verification for users	False	True	HIPAA ISO27001 PCI NIST
Medium	AWS	User Protection	Ensure credentials unused for 90 days or ...	us-east-1: User sand...	Success	HIPAA PCI CIS FFIEC GDPR APRA MAS NIST
Medium	AWS	User Protection	Ensure access keys are rotated every 90 ...	us-east-1: anh-test-u...	Success	HIPAA PCI CIS FFIEC GDPR APRA MAS NIST
Medium	AWS	User Protection	Ensure IAM password policy requires at l...	us-east-1: Password ...	Success	HIPAA PCI CIS FFIEC GDPR APRA MAS NIST

Supported Cloud Services and SaaS Applications

The applications below are supported by Cynet CSPM/SSPM. The list of applications continues to expand; please contact your sales rep or visit <https://help.cynet.com/en/articles/73-cloud-saas-security-posture-management> for the most up-to-date list.

-  **AWS** (requires privileges of AWS_ConfigRole policy)
-  **Azure Active Directory**
-  **Cynet Port Scanner**
-  **Dropbox**
-  **Google Workspace*** (including GDrive, Gmail, and all other G Suite applications)
-  **Microsoft 365**
-  **Microsoft Teams**
-  **OneDrive**
-  **Salesforce**
-  **SharePoint**
-  **Slack**
-  **Slack Enterprise**
-  **WebEx**
-  **Zoom**

*Comments for Google Workspace:

- When prompted to approve scopes, select all the available checkboxes.
- You can safely dismiss the warning regarding Cynet certification.

Remediate Open Ports

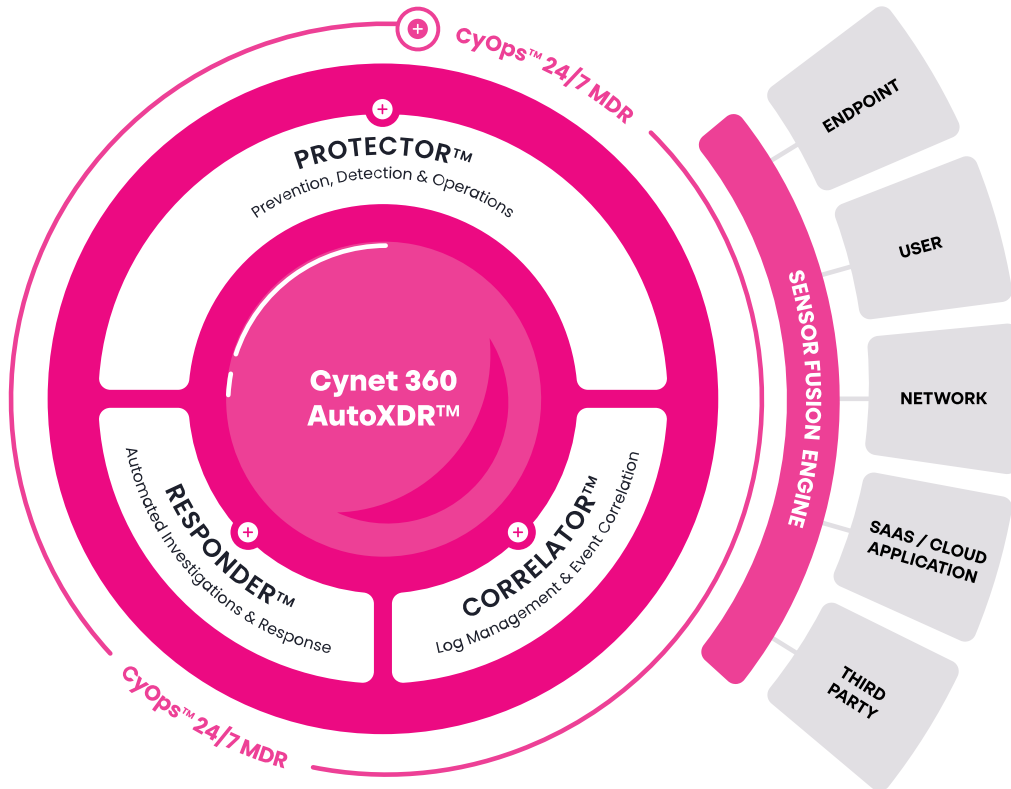
Cynet Port Scanner gives you visibility into risky ports and subdomains that are exposed to the public internet. Available as a connected SaaS application, the service identifies ports associated with your domains and IP addresses, along with each port's status, all within the Cynet dashboard.



About us

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.



Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.

[Learn more](#)

