

Hyver for MSPs

Hyver for MSP is CYE's exposure management offering for Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) to quantify their clients' risk exposure in financial terms, assess maturity, and manage cybersecurity posture.

The MSP enables a customer's access to the Hyver platform and configures it to build a cybersecurity program. These activities are built around exposure management and the establishment of cybersecurity maturity. MSPs manage customers' Hyver instances from the multi-client dashboard.

Multi-Client Dashboard

The multi-client dashboard is designed for MSPs and MSSPs with one or more clients using Hyver.



It allows the MSP to manage and monitor essential cybersecurity risk performance data for multiple clients in a centralized location. Furthermore, it consolidates exposure and cybersecurity maturity scores for the entire client base.

Customer Risk Dashboard

Customers can view their risk dashboard in Hyver to display these risk indicators.

- Cost of Breach
- Likelihood
- Exposure
- Organizational maturity

These risk indicator metrics represent the data that is input in Hyver from vulnerabilities to maturity data.



Cybersecurity Maturity in Hyver

Hyver's maturity assessment is the cornerstone for evaluating, enhancing, and sustaining an organization's cybersecurity ecosystem's robustness and resilience. Hyver's cybersecurity maturity assessment enables you to evaluate an organization's cybersecurity posture.

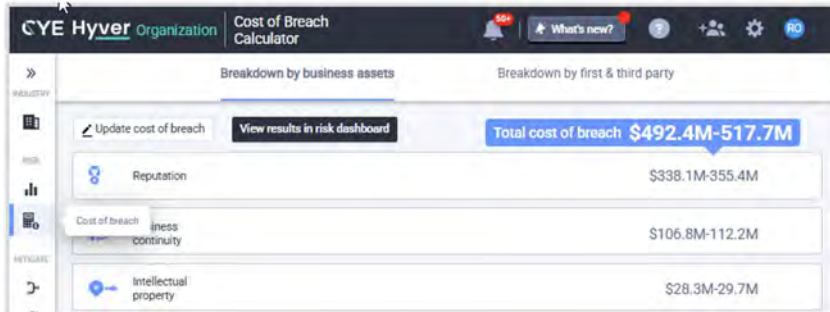
- Easy to assess and maintain
- Evaluated using NIST CSF with mappings to other frameworks, such as ISO 27201:2022
- A maturity level can be determined relatively quickly



The Hyver cybersecurity maturity assessment offers valuable insights into your organization's security posture. The platform enables a thorough evaluation of your organization's cybersecurity maturity.

Cost of Breach

Calculate the estimated monetary loss incurred in the event of a cybersecurity breach.



CoB is particularly relevant at the board level and valuable for CISOs to effectively convey their security posture and requirements to stakeholders. Hyver's Cost of Breach feature provides a detailed view of an organization's cyber risk, its likelihood, and the financial impact of a breach. The calculator estimates the potential monetary loss from a data breach, helping organizations allocate resources more effectively to prevent and mitigate such incidents.

Exposure Management

Hyver for MSPs enables you to manage your organization's vulnerabilities in Hyver and see the outcome in your cyber risk metrics. Maturity is a key feature in Hyver for assessing risk and it contributes to the calculation of exposure, cost of breach, and the likelihood of breach.

Exposure represents an organization's expected financial loss due to a potential cybersecurity breach. Hyver quantifies your organization's exposure in monetary terms based on:

- **Cost of Breach (CoB):** Financial impact of a data breach event
- **Likelihood of Breach (LoB):** The chance that a breach will occur within a year

Hyver calculates exposure by multiplying the estimated financial impact of a breach event (Cost of Breach), such as a customer data breach, by the Likelihood of Breach (LoB). Likelihood of breach is determined through input from various elements, such as vulnerabilities (findings), maturity, and internal (proprietary) attack route data to estimate a breach's likelihood (LoB).

Risk Dashboards

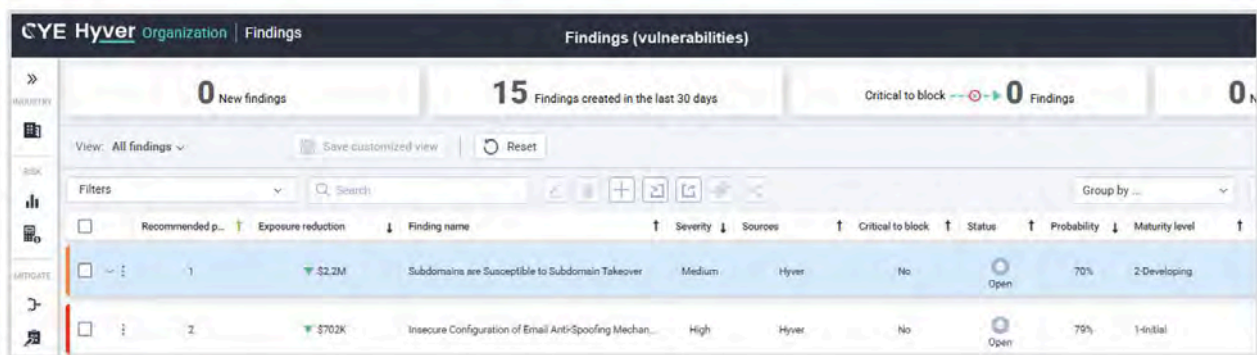
The Hyver security risk dashboard offers a comprehensive, centralized overview of an organization's cybersecurity posture.



Findings in Hyver

Hyver integrates with Azure to automate findings and asset ingestion. The finding import feature allows you to import findings from disparate sources.

Manage your vulnerabilities from the findings screen, where you can add, import, share, prioritize, and fix findings. These contribute to the various risk metrics on the dashboards. You can prioritize your remediation strategy according to your threat exposure. Hyver calculates an exposure reduction value for each finding to represent the exposure reduction when the finding is fixed.



Assets in Hyver

You can manage your organization's assets on the assets screen. Assets are an organization's potential access points, such as specific servers, routers, IP addresses, etc.

Findings Dashboard

Monitor and track your organization's security posture using the findings dashboard which provides a continuous, at-a-glance view of various aspects of vulnerabilities (findings) in your organization, such as trends for creating and fixing findings or distribution per severity and status.

**Contact your account manager for more information
or refer to the Knowledge Center in Hyver.**

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.