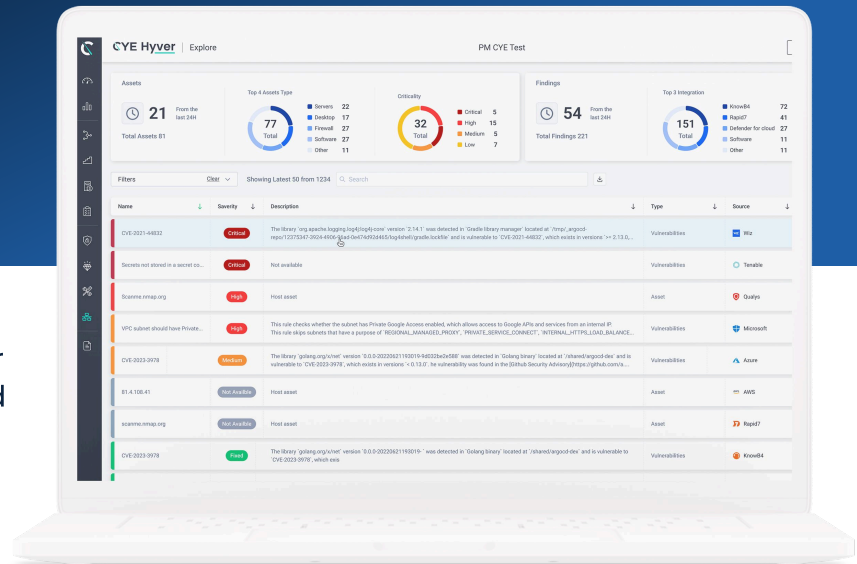# Hyver Integrations Hub

Integrate security and IT data to continuously monitor your cyber exposure, correlate findings, and remediate faster.



## Correlate findings. Create tasks. Remediate faster.

Hyver integrates the telemetry from your existing tools to correlate data into a central page with prioritization of the findings to be addressed. Hyver's mathematical model analyzes the telemetry and eliminates duplicates, to determine the finding's contribution to the overall cyber exposure. This allows organizations to prioritize remediation actions based on their value to reduce cyber exposure.

## Key Benefits

✅ **Correlate & Deduplicate Findings:**
Eliminate redundant alerts by integrating telemetry from your cybersecurity stack, including VM, cloud, AppSec, IAM, EDR, and awareness tools.

✅ **Prioritize Based on Exploitation Likelihood and Impact:**
Use Likelihood of Breach (LoB) and Cost of Breach (CoB) to surface the most critical exposures in your attack surface.

✅ **Single, Central View in Context:**
Centralize findings from all sources into a single, contextualized page.

✅ **Remediate Fast:**
Push remediation actions to the relevant teams across the organization via SecOps and enterprise solutions such as your SIEM, Jira, and ServiceNow.

✅ **Scale with Automated Workflows:**
Connect with 1,000+ tools, including custom and non-standard platforms, using Workato to expand remediation execution across your specific enterprise tools and processes.

## How the integration works

| Integrate data (tools and reports) | ▶ | See your maturity, risk, and exposure metrics | ▶ | Create and execute mitigation plans (ITSM / workflows) |

## Integrations Hub

Hyver connects with 100+ tools across your environment, some of which are mentioned in the table below, representing the more common tools as reference.

| Cloud | Microsoft | Wiz | Azure | AWS | GCP | Orca | Cisco | Palo Alto | |
|---|---|---|---|---|---|---|---|---|---|
| Proactive Cyber Risk Management (including IAM, ASM, EASM) | Qualys | Tenable | Rapid7 | Crowdstrike | CyberArk | Panorays | Axonius | Armis | GitHub |
| Endpoint Detection & Response / Threat Intelligence | Microsoft | SentinalOne | Crowdstrike | Datadog | Cisco | Palo Alto | Recorded | | |
| Business Applications | Servicenow | Workato | Atlassian | Slack | Microsoft | Zendesk | Asana | | |
| Cyber Awareness | KnowBe4 | | | | | | | | |

## The Hyver Advantage

Gain clarity from the data in your cybersecurity tools by

☑ Automatically **correlating** and **mapping findings** on your organizational attack graph with likelihood of vulnerabilities' exploitability

☑ Determining your **cyber exposure in financial terms** to drive outcome-driven priorities

☑ Identifying the findings that are more critical to block to **reduce your exposure**

☑ **Dispatching remediation** tasks across your organization

☑ Monitoring and tracking your mitigation outcomes with a **continuous feedback loop from your cybersecurity stack**

## Start Managing Cyber Exposure To Enable Your Business Growth

Discover how Hyver enables you to continuously reduce your cyber exposure, prioritize remediation, and improve your cyber resilience over time.

### Schedule a demo

## 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.