CYE

Quantify and Manage

Your Cyber Exposure

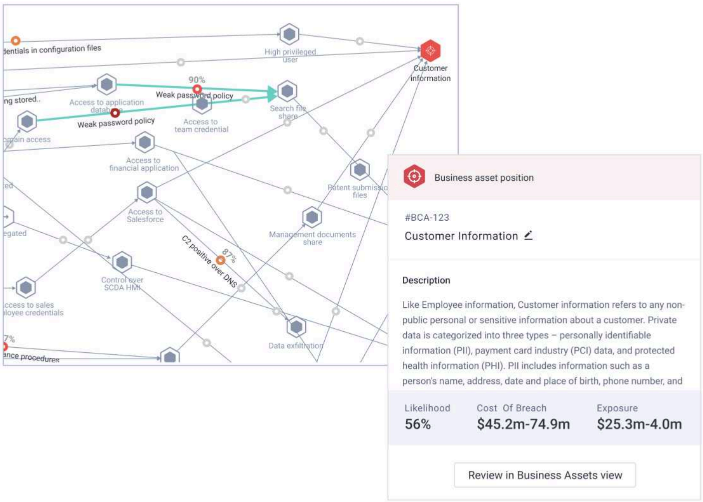
Continuously assess your cyber exposure in financial terms, drive mitigation based on attack route exploitability, and develop your cybersecurity maturity.

Quantify Mitigate Mature

Quantify

Gain clarity on your attack surface.

Hyver assesses your threat exposure and reveals your most likely exploitable attack vectors to your business assets across your organization, including cloud, IT, OT, and physical environments.



Business asset position

#BCA-123

Customer Information

Description

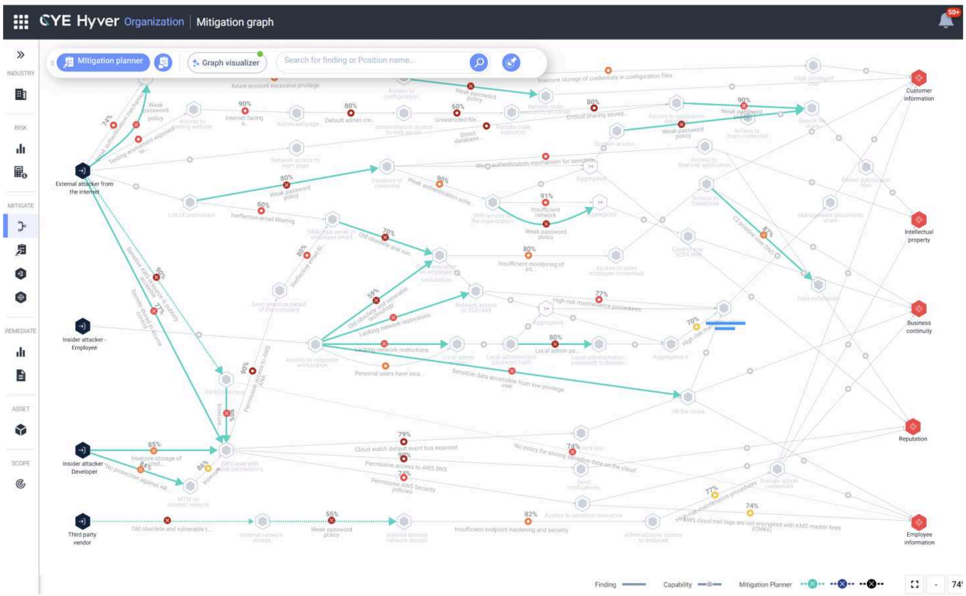
Like Employee information, Customer information refers to any non-public personal or sensitive information about a customer. Private data is categorized into three types – personally identifiable information (PII), payment card industry (PCI) data, and protected health information (PHI). PII includes information such as a person's name, address, date and place of birth, phone number, and

Likelihood	Cost Of Breach	Exposure
56%	$45.2m-74.9m	$25.3m-4.0m

Review in Business Assets view

Find out the likelihood that your cyber gaps will be exploited and their impact in financial terms.

Utilizing graph theory and MITRE ATT&CK based threat modeling, Hyver reveals attacker TTPs and movement across your attack surface. Hyver's mathematical model estimates your vulnerabilities' likelihood to be exploited by considering cyber threat intelligence data, industry data, and your organization's external and internal attack surface.

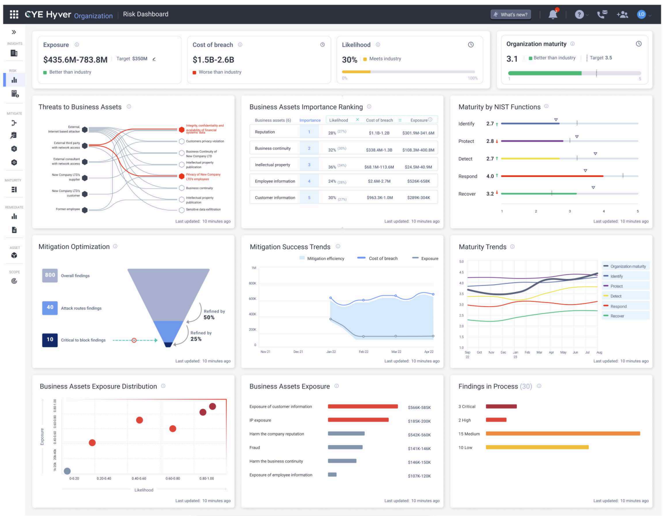


CYE Hyver
Organization
Mitigation graph
50+
Mitigation planner
Graph visualizer
Search for finding or Position name...
INDUSTRY
RISK
MITIGATE
REMEDIATE
ASSET
SCOPE
External attacker from the internet
Insider attacker - Employee
Insider attacker - Developer
Third party vendor
Azure account excessive privilege
Weak password policy
90%
Internet facing a...
80%
Default admin cre...
60%
Unrestricted file...
Direct database...
Insecure storage of credentials in configuration files
80%
Critical sharing stored...
90%
Weak password policy
Weak password policy
Customer information
Weak authentication mechanism for sensitive...
80%
Weak password policy
60%
Ineffective email filtering
90%
Weak authentication sche...
91%
Insufficient network
Weak password policy
70%
Old obsolete and vun...
80%
Insufficient monitoring of int...
Intellectual property
C2 positive over DNS
87%
59%
Old obsolete and venerable technology
Lacking network restrictions
Lacking network restrictions
Personal users have loca...
77%
High risk maintenance procedures
80%
Local admin pa...
70%
Sensitive data accessible from low privilege user
Business continuity
90%
77%
Sensitive AWS resource is publicly accessible
Secrets stored in source control
Permission access to AWS ANA
85%
Insecure storage of cred...
84%
No protection against AR...
86%
79%
Cloud watch default event bus exposed
90%
Permissive access to AWS SNS
74%
Permissive AWS Security policies
74%
No policy for storing sensitive data on the cloud
Reputation
55%
Old obsolete and vulnerable t...
Weak password policy
82%
Insufficient endpoint hardening and security
77%
High risk maintenance procedures
74%
AWS cloud trail logs are not encrypted with KMS master keys (CMKs)
Employee information
Finding
Capability
Mitigation Planner
74

Quantify your organization's threat exposure.

Exposure represents the expected financial loss an organization faces due to a potential security breach. It quantifies risk in monetary terms by combining:

- Likelihood of Breach (LoB):
  The chance that a breach will occur within a year.
- Cost of Breach (CoB):
  The financial impact if a breach happens.

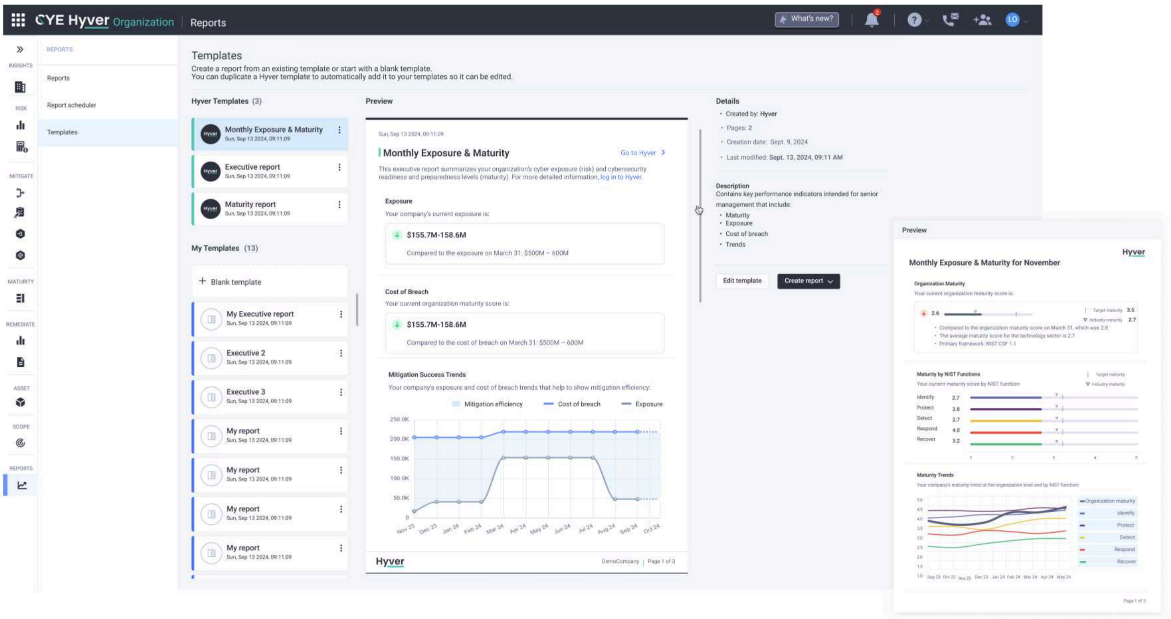


Hyver quantifies exposure by first identifying the financial impact of an attacker reaching your critical business assets, such as IP and customer data. It then considers cybersecurity findings from your security tools and internal assessments, such as penetration tests and risk registers, to determine the likelihood of a breach. Hyver uses sophisticated algorithms, prediction tools, and machine learning to estimate your organization's risk exposure.

Generate executive and operational reports.

Hyver empowers you to generate customized reporting with board-level metrics and operational actions. This drives executive-level decision making and operational mitigation plans tailored to your organization, while considering the time and team effort required to remediate your vulnerabilities. With these reports, you can also track your progress reducing exposure over time, as well as the cost of remediation to continuously improve your cybersecurity program's effectiveness.

This financial clarity enables you to provide explicit guidance to management and security teams on acceptable levels of risk, helping you communicate the value and impact of security programs for your business.



Templates

Create a report from an existing template or start with a blank template.
You can duplicate a Hyver template to automatically add it to your templates so it can be edited.

Monthly Exposure & Maturity

This executive report summarizes your organization's cyber exposure (risk) and cybersecurity readiness and preparedness levels (maturity). For more detailed information, log in to Hyver.

Exposure

Your company's current exposure is:

$155.7M-158.6M

Compared to the exposure on March 31: $500M – 600M

Cost of Breach

Your current organization maturity score is:

$155.7M-158.6M

Compared to the cost of breach on March 31: $500M – 600M

Mitigation Success Trends

Your company's exposure and cost of breach trends that help to show mitigation efficiency:

Details

- Created by: Hyver
- Pages: 2
- Creation date: Sept. 9, 2024
- Last modified: Sept. 13, 2024, 09:11 AM

Description

Contains key performance indicators intended for senior management that include:

- Maturity
- Exposure
- Cost of breach
- Trends

Monthly Exposure & Maturity for November

Organization Maturity

Your current organization maturity score is:

- Compared to the organization maturity score on March 31, which was 2.8
- The average maturity score for the technology sector is 2.7
- Primary framework: NIST CSF 1.1

Maturity by NIST Functions

Your current maturity score by NIST function:

Maturity Trends

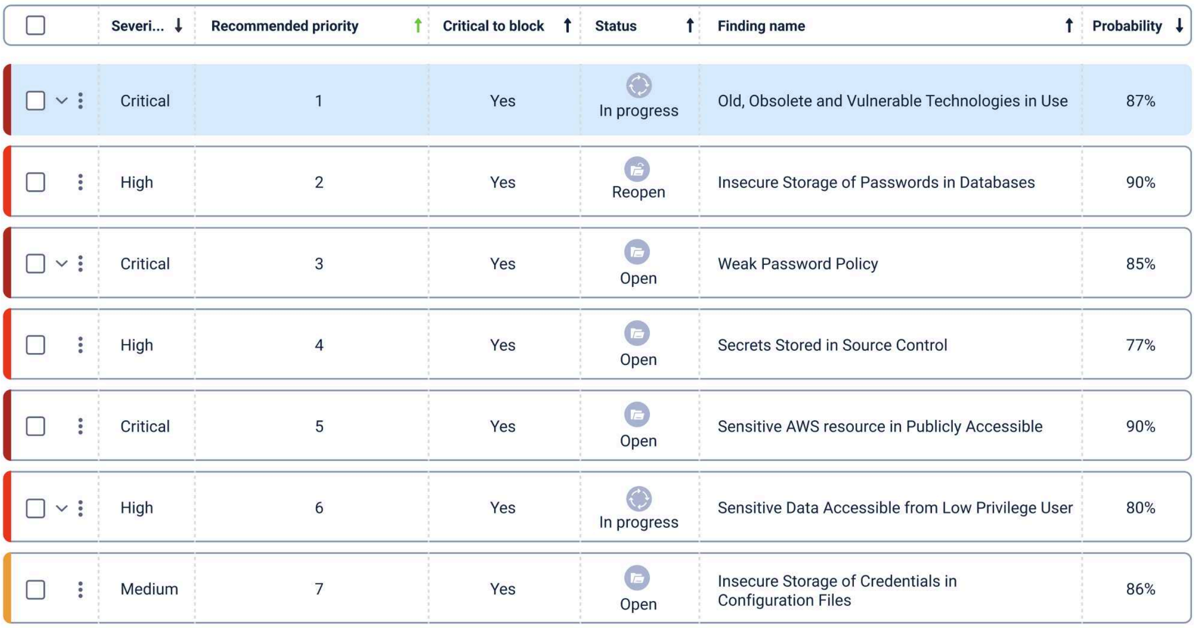
Your company's maturity trend at the organization level and by NIST function:

Mitigate

Tailor your mitigation planning.

Prioritize your remediation strategy according to your threat exposure.

A thorough understanding of which critical assets are specifically at risk—as well as the attack routes, breach, and mitigation costs—help your organization plan and prioritize mitigation based on exposure reduction.



□	Severi... ↓	Recommended priority ↑	Critical to block ↑	Status ↑	Finding name ↑	Probability ↓
□	Critical	1	Yes	In progress	Old, Obsolete and Vulnerable Technologies in Use	87%
□	High	2	Yes	Reopen	Insecure Storage of Passwords in Databases	90%
□	Critical	3	Yes	Open	Weak Password Policy	85%
□	High	4	Yes	Open	Secrets Stored in Source Control	77%
□	Critical	5	Yes	Open	Sensitive AWS resource in Publicly Accessible	90%
□	High	6	Yes	In progress	Sensitive Data Accessible from Low Privilege User	80%
□	Medium	7	Yes	Open	Insecure Storage of Credentials in Configuration Files	86%

Hyver creates four mitigation plans to help you understand the ramifications of mitigation: critical to block, most probable route, lowest cost level, and lowest effort level.

Each one simulates the problems to be fixed, along with their cost and effort. Integrating with workflow and ticketing systems such as ServiceNow and Jira enables you to operationalize these mitigation plans across the organization.

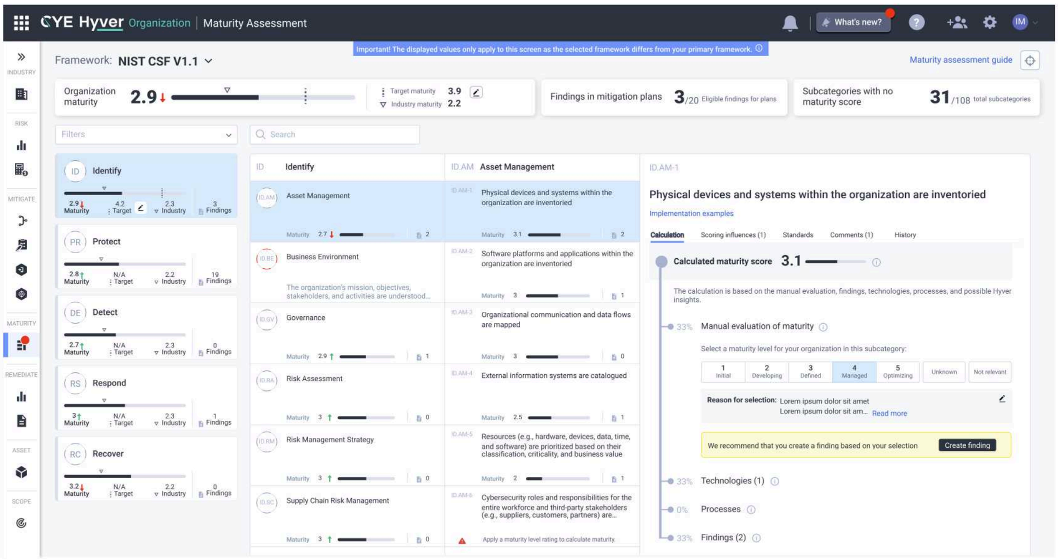
Mature

Develop your cybersecurity maturity.

Leveraging your existing organizational assessments, compliance audits, risk registers, and data from your security tools, Hyver automatically maps and calculates your organization's cybersecurity maturity according to NIST CSF 1.1 and 2.0 models.

The outcome is reflected in an organization's overall maturity score, as well as scoring for each function across the NIST framework. This allows you to identify the areas of improvement required to improve your security posture over time. Furthermore, each finding is mapped to the relevant NIST subcategory so that you can create mitigation plans.

Your organization's maturity is also a key consideration in Hyver's assessment of the financial cost of a potential breach, as it directly influences Time to Detect (TTD), Time to Respond (TTR), and recovery efforts—all of which affect business continuity and the risk of customer and employee PII loss.



Important! The displayed values only apply to this screen as the selected framework differs from your primary framework.

Framework: NIST CSF V1.1

Organization maturity 2.9 — Target maturity 3.9 — Industry maturity 2.2

Findings in mitigation plans 3/20 Eligible findings for plans

Subcategories with no maturity score 31/108 total subcategories

ID	Function	Maturity	Target	Industry	Findings
ID	Identify	2.9	4.2	2.3	3
PR	Protect	2.8	N/A	2.2	19
DE	Detect	2.7	N/A	2.3	0
RS	Respond	3	N/A	2.3	1
RC	Recover	3.2	N/A	2.2	0

ID	Identify	Maturity	Findings
ID.AM	Asset Management	2.7	2
ID.BE	Business Environment The organization's mission, objectives, stakeholders, and activities are understood...		
ID.GV	Governance	2.9	1
ID.RA	Risk Assessment	3	0
ID.RM	Risk Management Strategy	3	0
ID.SC	Supply Chain Risk Management	3	0

ID.AM	Asset Management	Maturity	Findings
ID.AM-1	Physical devices and systems within the organization are inventoried	3.1	2
ID.AM-2	Software platforms and applications within the organization are inventoried	3	1
ID.AM-3	Organizational communication and data flows are mapped	3	0
ID.AM-4	External information systems are catalogued	2.5	1
ID.AM-5	Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	2	1
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are... Apply a maturity level rating to calculate maturity.		

ID.AM-1

Physical devices and systems within the organization are inventoried

Implementation examples

Calculation | Scoring influences (1) | Standards | Comments (1) | History

Calculated maturity score 3.1

The calculation is based on the manual evaluation, findings, technologies, processes, and possible Hyver insights.

33% Manual evaluation of maturity

Select a maturity level for your organization in this subcategory:

1 Initial | 2 Developing | 3 Defined | [✓ 4 Managed] | 5 Optimizing | Unknown | Not relevant

Reason for selection: Lorem ipsum dolor sit amet
Lorem ipsum dolor sit am... Read more

We recommend that you create a finding based on your selection — Create finding

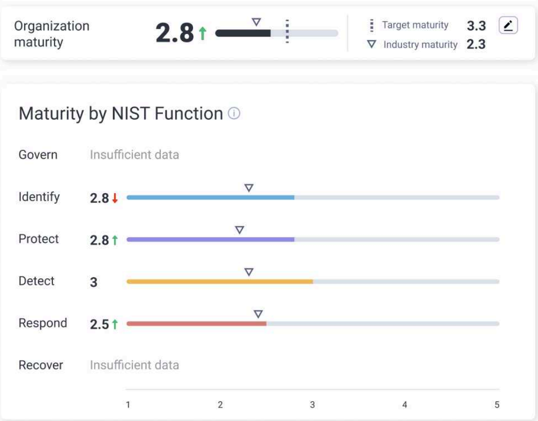
33% Technologies (1)

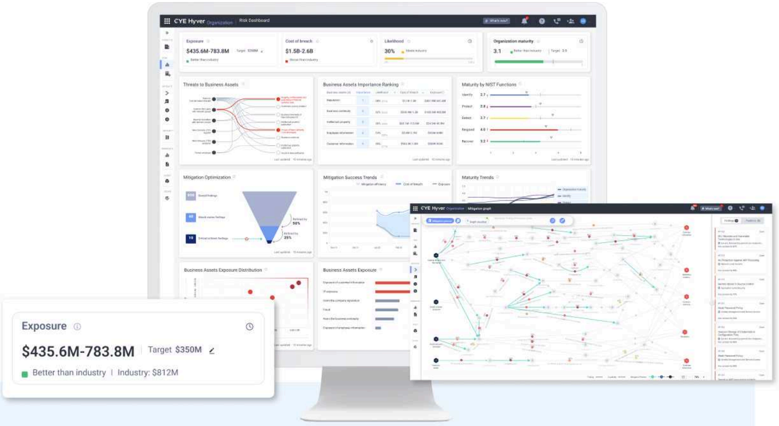
0% Processes

33% Findings (2)

Benchmark against industry peers.

Hyver provides you with comparable industry data on cybersecurity maturity levels, cost of breach, and threat exposure in financial terms. This benchmarking enables you to determine your relative security posture, identify weaknesses compared to your peers, and define targets to improve your cybersecurity maturity.





Exposure

$435.6M-783.8M Target $350M

🟩 Better than industry | Industry: $812M

Hyver Benefits

Scalability

☑ Multi-Region ☑ Multi-Company ☑ No Geographical Limitations ☑ Multi-Vertical

Deployment

☑ Agentless ☑ Non-Disruptive ☑ Rapid

Immediate ROI

☑ Data-Led Operational Effectiveness ☑ Reduced Costs ☑ Improved Security Posture

Tech integrations

WIZ aws

Trusted by industry leaders around the globe

intel. Harrods PHILIPS GENERALI WARBURG PINCUS AutoStore Hoffmann Group

Schindler SHL GROUP ALSO RedSail TECHNOLOGIES Anticimex reckitt KIK CONSUMER PRODUCTS

About CYE

CYE's exposure management platform 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.

www.cyesec.com | info@cyesec.com
1000 North West Street, Suite 1410, Wilmington DE 19801, United States
1 Ballards Lane, London N3 1LQ, UK | Abba Eban 10, Herzliya 4615200, Israel

CYE