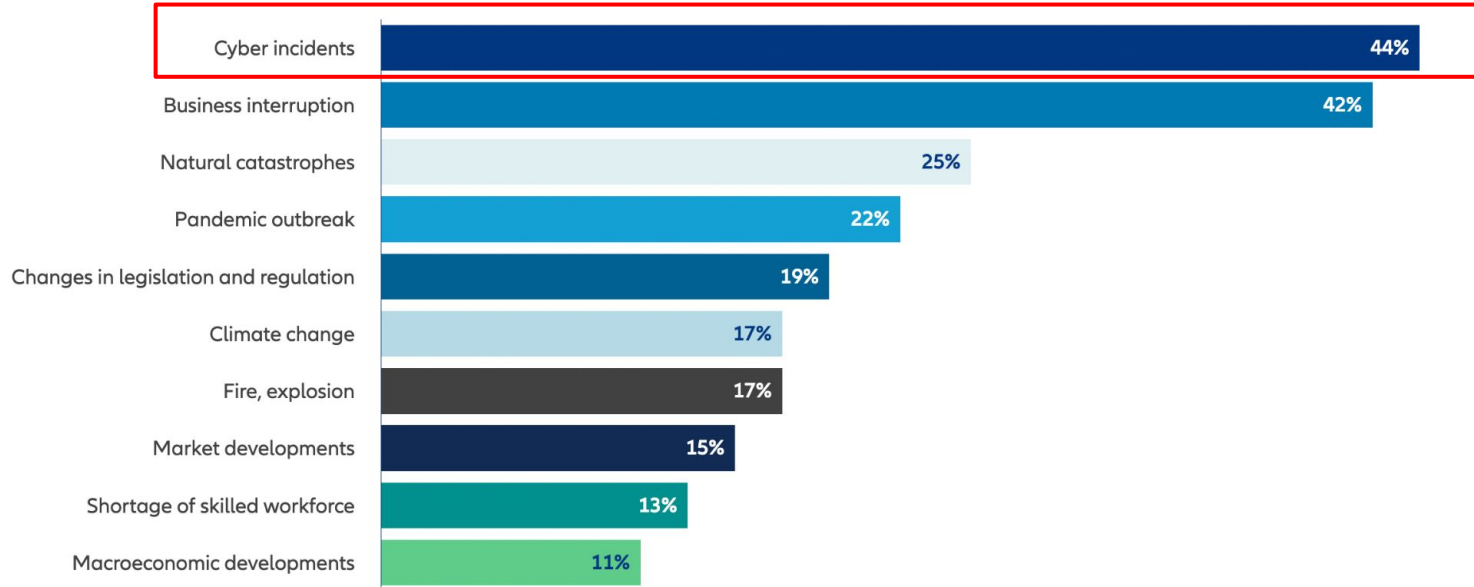


Financially Quantify & Manage Your Cyber Risks Platform

Access fast, on-demand insights into your cyber investment & strategy decisions with Kovrr Quantum.

The most important global business risks for 2022

Click on the bars in the chart for further details





Cyber Security is evolving Into Cyber Risk Management.

Copyright Kovrr, Inc 2023

Microsoft
Partner

Transforming the world's cyber security data into financially quantified cyber risk management decisions.

A scalable on-demand cyber risk management technology that connects and transforms a business's cyber data into:

Cyber Security Data



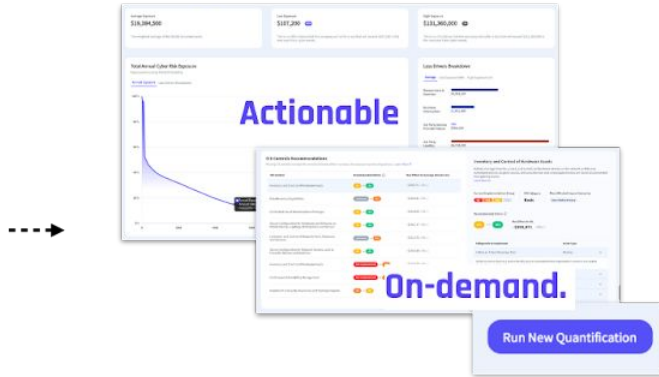
MICROSOFT 365 DEFENDER

DEFENDER for Cloud



Azure Sentinel

Financially Quantified



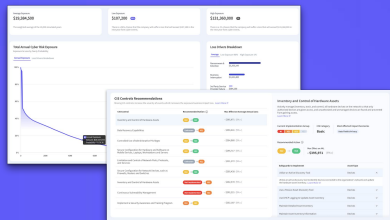
Cyber Decisions.

- Communicate cyber risk to your board
- Cybersecurity Investment optimization
- 3rd party vendors exposure analysis
- Governance & compliance
- Cyber Insurance & Risk Transfer
- Capital Management

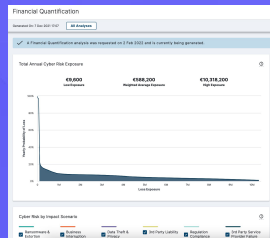


Cyber Decisions. Financially Quantified.

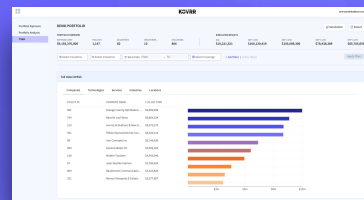
Cyber Decisions. Financially Quantified



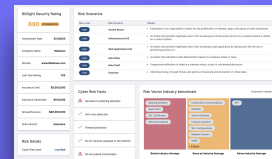
Quantum Platform



FQ-ECR



Exposure Management Platform



Cyber Underwriting

Enterprise
Market

Insurance & Reinsurance
Market

The Challenge

Enterprise Boards, CRO's and CISO's struggle to understand and communicate their business's exposure and resilience to cyber risk.

Unable to articulate their Cyber Exposure in financial terms

Unable to justify their cyber budget requests with an expected ROI

Unable to be confident they have the right level cyber insurance

Current Obstacles in financially quantifying cyber risk

Too Technical

Too Slow

Subjective Judgement

Manual Data Collection

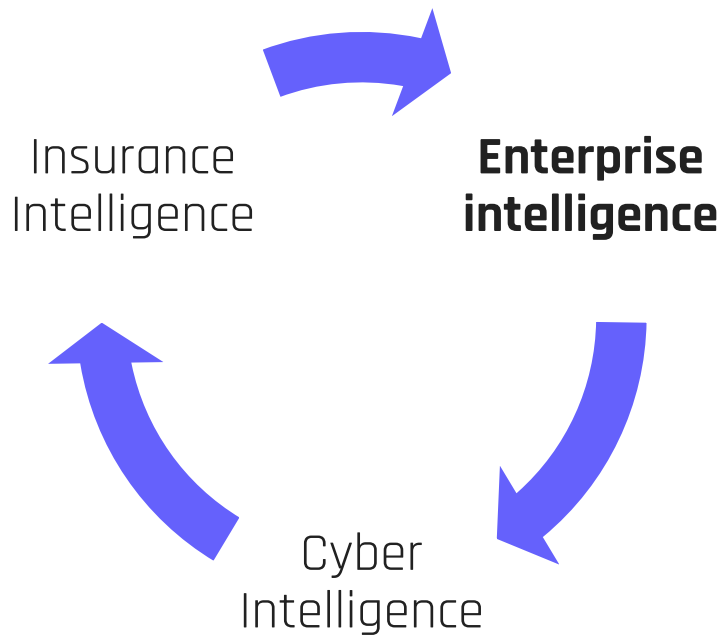
Abstract Ratings

Lack of market context

Lack of Actionability

Lack of Scalability

Analyze the Posture of Complex Enterprises At Any Level



**Group & Subsidiary
Company Structure**

Sensitive Records

Industry Benchmarks

Integrated External Attack Surface, Internal Telemetry and Threat Intelligence data



**Microsoft Defender
External Attack
Surface Management**

**Microsoft 365
Defender**

Microsoft Defender for Cloud

Microsoft Sentinel

**Microsoft Defender
Threat Intelligence**

Insurance
Intelligence

Enterprise
intelligence

**Cyber
Intelligence**

Ongoing validation from global insurance portfolios and Claims

Allianz 

AON

MS&AD
INSURANCE GROUP


LOCKTON
REINSURANCE

**Insurance
Intelligence**

Enterprise
intelligence

Cyber
Intelligence



Automatically integrate both External Attack Surface data & Internal Telemetry

The screenshot displays the Kovrr Quantum application interface. On the left, a permissions request dialog is open, titled "Permissions requested Review for your organization". It lists various permissions such as "Read incidents", "Read all security alerts", and "Perform user-impacting remote actions on Microsoft Intune devices". Below the list, there is a section for "If you accept, this app will get access to the specified resources for all users in your organization." and a link to "Report it here". At the bottom of the dialog are "Cancel" and "Accept" buttons.

On the right, a network diagram is displayed. The central node is "Acme Global". It is connected to several other nodes: "Employee Endpoints", "Cloud", "Infrastructure", "Production", and "Testing". The "Cloud" node is further connected to "Shared Env.". The "Infrastructure" node is connected to "USA", "FR", "JA", "BE", and "UK". The "Production" node is connected to "Shared Env.". The "Testing" node is connected to "Shared Env.". The diagram is set against a grid background.

Visualise your Enterprise's Exposure to Cyber Risk

Understand the Posture at as Asset Based level

KOVRR Quantum P

Acme IL Sphere **First Time Setup**

Asset Groups

- Employees Endpoints
- Infrastructure
- Cloud

Security Profiles

Damage Types

Security Controls

The following questions refer to your entity's security posture. These inputs will allow us to give you better recommendations regarding your cybersecurity investments. You can set specific settings to different asset groups.

[+ Add Security Profile](#)

Security Profile 1 All Asset Groups

What outage duration will cause a material impact on the company?

Hours

How long does it typically take to restore your critical business operations following a network interruption?

Hours

CIS Controls

Please select what implementation group your organization has obtained for each CIS control. Are you using a different framework? [Download Mappings](#)

Basic
CIS CONTROLS 1-6

CIS Control 1 - Inventory and Control of Hardware Assets

Not Implemented IG1 IG2 IG3 I Don't Know [Not sure?](#)

← Previous Step: Infrastructure

Next Step: Damage Types →

Financially Quantify the ROI of cyber security control investment decisions

CIS Controls Recommendations

Missing CIS controls increase the severity of events which increases the exposure business impact loss. [Learn More](#)

Using a different framework? [Download Mapping](#)

CIS Control	Recommended Action	Average effect ↑	Highest effect ↓
10. Data Recovery Capabilities	IG1 → IG2	-\$594,169 (1.52 % ↓)	-\$805,952 (0.18 % ↓)
6. Maintenance Monitoring And Analysis Of Audit Logs	IG1 → IG2	-\$541,566 (1.38 % ↓)	-\$811,469 (0.18 % ↓)
20. Penetration Tests And Red Team Exercises	IG1 → IG2	-\$347,911 (0.89 % ↓)	-\$546,725 (0.12 % ↓)
17. Implement A Security Awareness And Training Program	IG1 → IG2	-\$344,496 (0.88 % ↓)	-\$578,375 (0.13 % ↓)
14. Controlled Access Based On The Need To Know	IG2 → IG3	-\$294,247 (0.75 % ↓)	-\$529,221 (0.12 % ↓)
19. Incident Response And Management	IG2 → IG3	-\$291,174 (0.74 % ↓)	-\$456,644 (0.10 % ↓)
4. Controlled Use Of Administrative Privileges	IG2 → IG3	-\$251,162 (0.64 % ↓)	-\$450,757 (0.10 % ↓)
13. Data Protection	IG2 → IG3	-\$248,087 (0.63 % ↓)	-\$419,998 (0.09 % ↓)
8. Malware Defenses	IG2 → IG3	-\$245,067 (0.63 % ↓)	-\$381,161 (0.08 % ↓)
3. Continuous Vulnerability Management	IG2 → IG3	-\$189,877 (0.49 % ↓)	-\$303,458 (0.07 % ↓)

Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Current Implementation Group

NI IG1 IG2 IG3

CIS Category

Foundational

Recommended Action

IG1 → IG2

Most Affected Event type

Ransomware

Max Effect on High Exposure Year

-\$805,952 (0.18 % ↓)

Test ROI

Average Annual Loss ↓

How much will it cost the organization to complete the action?

150000 USD Test

Mitigation Cost

\$150,000

Expected Savings

\$594,169

Net ROI

\$444,169

Safeguards to Implement

Ensure Regular Automated BackUps

Perform Complete System Backups

Asset Type

Data

Data

Test ROI

Average Annual Loss ↓

How much will it cost the organization to complete the action?

150000 USD Test

Mitigation Cost

\$150,000

Expected Savings

\$594,169

Net ROI

\$444,169

ROI Ratio

296%

Transparency into the the data sources & how they were used

ID	Name	Tags	Criticality	Risk Score	AG Type	AG Name	OS	Technologies	Integration
beba076c-ed0-4ff2-82ec-8d536d2ed3b3	dna-redash.i10ji4jpkietgq31hypk2hggg.zx.internal.cloudapp.net		MEDIUM	0	Cloud	IP Segment: 10.0.1.0/24	Ubuntu		Azure Sentinel
bddb6a6b-4f86-4c87-ac4c-b19b936bf6e7	oasis-lmf1i10ji4jpkietgq31hypk2hggg.zx.internal.cloudapp.net		MEDIUM	0	Cloud	IP Segment: 10.0.1.0/24	Ubuntu		Azure Sentinel
4e807b90-6c5a-4f32-9e3e-48d2bc5e968a	analytics-redash.i10ji4jpkietgq31hypk2hggg.zx.internal.cloudapp.net		MEDIUM	0	Cloud	IP Segment: 10.0.1.0/24	Ubuntu		Azure Sentinel
6f38abd9-57ef-44c8-80e0-da5b0eb4fd7e	redash		MEDIUM	0	Cloud	IP Segment: 172.17.0.0/24	Ubuntu		Azure Sentinel
3c02a9bc-19f1-4671-8af1-1fac7331d774	windows1		MEDIUM	2	Cloud	IP Segment: 10.1.0.0/24	Windows10	6 technologies	Azure Sentinel
672f1c7f-6ba6-4de1-8e5e-876e0d1efe53	linux-test1.tf1k4scsafozuih42n2clojd5e.bx.internal.cloudapp.net		MEDIUM	0	Cloud	IP Segment: 10.1.0.0/24	Ubuntu		Azure Sentinel
ca39d87f-c46b-4091-8520-c56e0cfaecf	LAPTOP-GQMIK24U		LOW	0	Cloud	Unidentified IP Segment	Windows		Azure Sentinel
92283895-4405-40cd-8001-e01ea0ca7388	windows2		LOW	0	Cloud	Unidentified IP Segment	Windows		Azure Sentinel

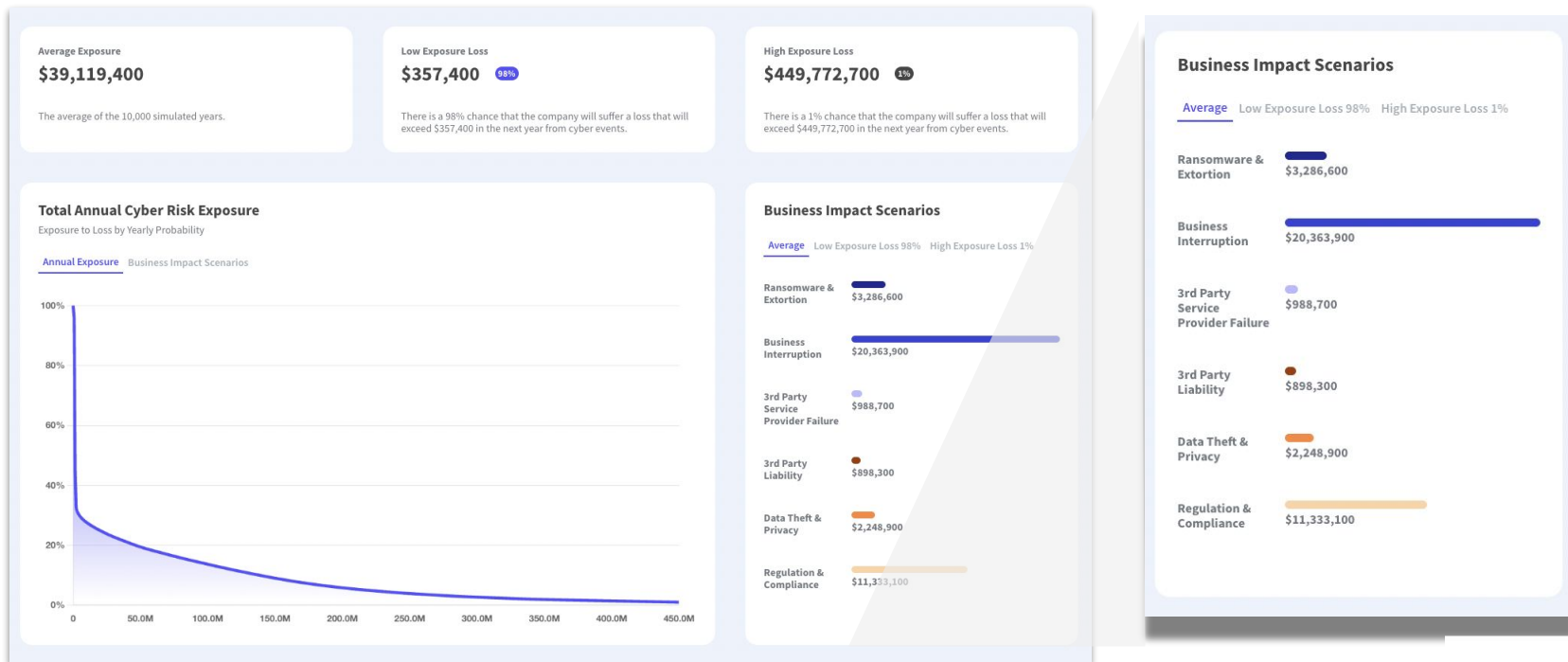
View entries per page

Results: 1 - 8 of 8 < 1 >

MEDIUM

Azure
Sentinel

Communicate overall exposure and the main drivers of financial loss

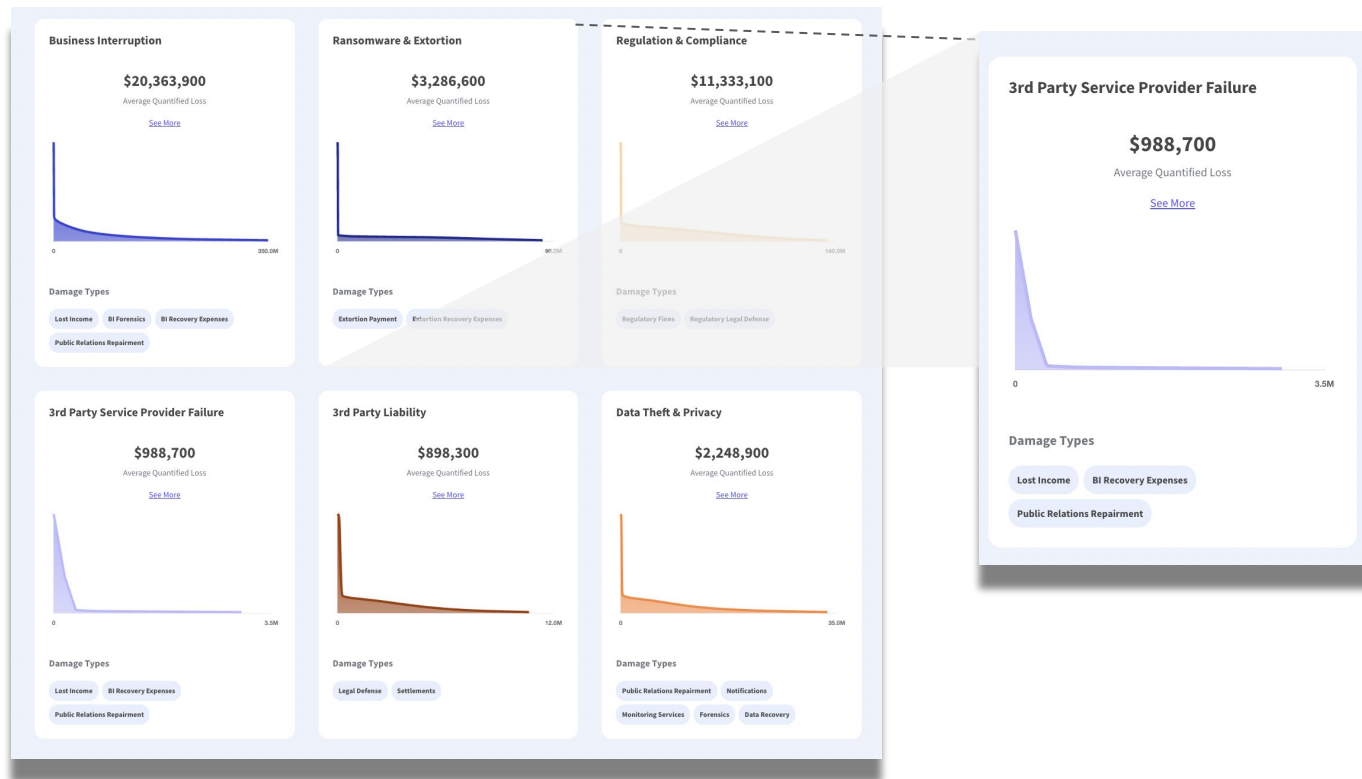


Business Impact Scenarios

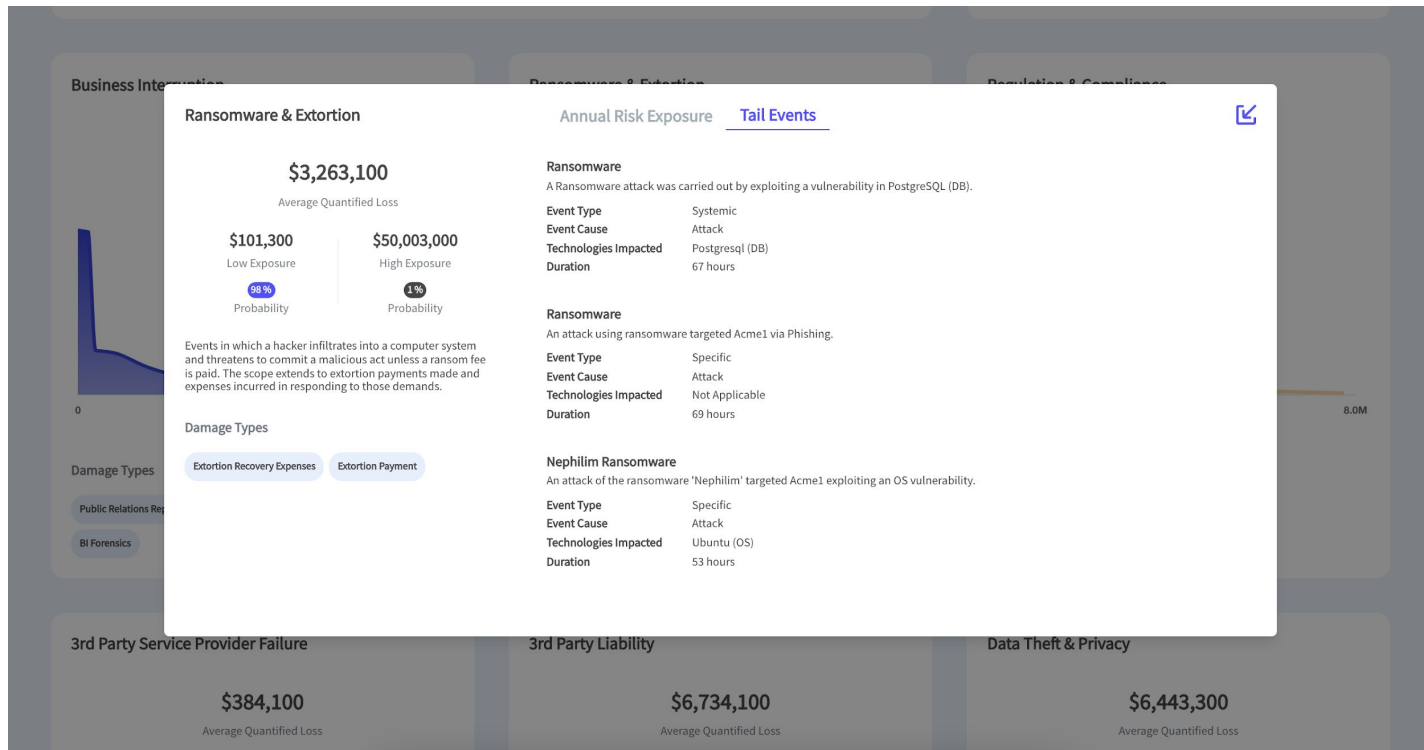
Average Low Exposure Loss 98% High Exposure Loss 1%

Ransomware & Extortion	\$3,286,600
Business Interruption	\$20,363,900
3rd Party Service Provider Failure	\$988,700
3rd Party Liability	\$898,300
Data Theft & Privacy	\$2,248,900
Regulation & Compliance	\$11,333,100

Understand the Impact of Cyber Attacks and 3rd Party Service Provider Failures



Detailed Insights into multiple cyber events types that could cause severe losses



Insights into Third Party Service Provider Risk

Quantification for CloudComms Inc.

Quantification Date: 13 Nov 2022

Export

Run New Quantification

Risk Overview Financial Exposure Recommendations Risk Transfer **Third Party Risk** Quantification Explained

Third Party Risk Report Third Party Service Providers

Third Party Risk: Annual Financial Exposure

\$0
LOW EXPOSURE LOSS ⓘ

\$74,900
AVERAGE ANNUAL LOSS ⓘ

\$3,250,100
HIGH EXPOSURE LOSS ⓘ

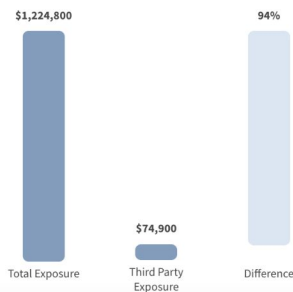
Top Third Party Service Providers

Based on Average Yearly Loss



Third Party Exposure vs. Overall Exposure

Based on Average Annual Loss



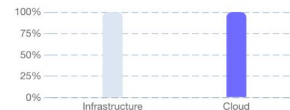
How are these results calculated?

The company's third party risk is calculated by taking into account events solely involving third party service providers. This includes events occurring in the company caused by an exploitation of a provider weakness as well as events affecting the provider that can impact the company. Attritional events are excluded from this calculation.

How my input affects the results?

Assets Criticality

Your input shows that the criticality of your cloud asset groups is equal compared to infrastructure asset groups. The severity of events associated with third party service providers may therefore be as high as other types of events.



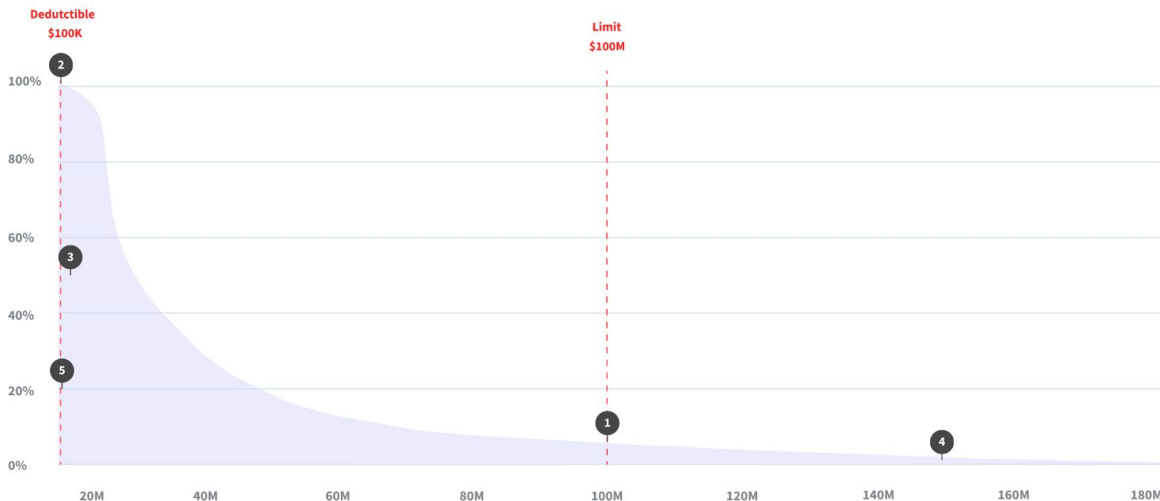
Number of Data Records

Your input shows that 98% less data records are stored in your cloud asset groups compared to infrastructure asset groups. This may lead to a decrease in severity of events associated with third party service providers.

Financially quantify cyber insurance & risk transfer options

Insurance Terms Stress Testing

Annual Exposure Loss Drivers Breakdown



Highlights

- 1 There is a 5% probability that annual losses will exceed the aggregate Limit.
- 2 There is an 98% probability that annual losses will exceed the deductible.
- 3 Average annual risk loss is falling above the deductible.
- 4 The current limit is under the estimated 1% high exposure (\$153,000,000).
- 5 The current deductible is under the estimated 98% low exposure (\$371,000).

Prioritize Insurance coverages based on potential impact

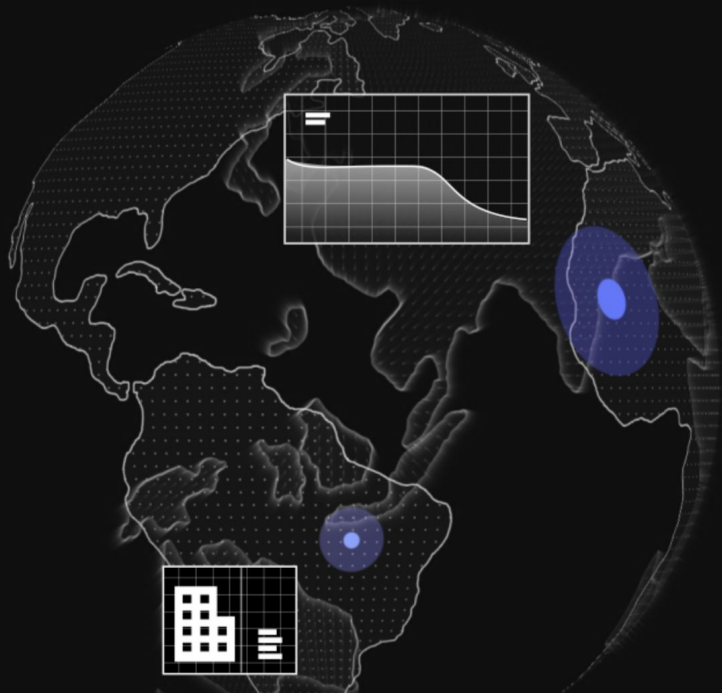
Insurance Terms Stress Testing

Annual Exposure Business Impact Scenarios



Highlights

- 1 There is a 18% probability of Business Impact events breaching the event insured limit
- 2 There is a 40% probability of Business Impact events exceeding the event deductible
- 3 There is a 2% probability of Contingent Business Impact events exceeding the event deductible
- 4 There is a 4% probability of Extortion events breaching the event insured limit
- 5 There is a 5% probability of Extortion events exceeding the event deductible
- 6 There is a 1% probability of Liability events breaching the event insured limit
- 7 There is a 16% probability of Liability events exceeding the event deductible



Thank You

Tom Boltman, VP Strategic Initiatives

tom@kovrr.com

+44 7 52 54 56 168