Cyber Quant

Overview

Cyber Quant provides a centralized strategic cyber risk dashboard of your organization through its contextual risk assessment and technology integration capabilities.

Cyber Quant helps answer critical business questions

- Do you know which security gaps pose the greatest risk to your business?
- What is the financial impact of security breaches on your organization?
- How can my organization's unique cyber threat landscape be incorporated into risk assessments?
- How do your business and security leaders determine where to invest?

Cyber Quant utilizes a 4-step approach

Threat Landscape

Evaluate demographic information about your organization to personalize threat landscape impact for your business based on location, industry, and organization size

Questionnaires

Analyze responses to customized, dynamic questionnaires to identify depth of risk, alignment to security standards and fit within other key industry frameworks

Technical Analysis

Validate your system's security settings alignment to your policies and industry best practices by securely evaluating 60+ technologies covering operating systems, cloud platforms, firewalls, security applications and more

Evaluate & Act

- ✓ Automatically converge the information above to create role-based dashboards and reports
- ✓ Calculate cyber risk score and financial impact of potential cyber events for your organization
- ✓ Simulate scenarios to identify priority business and technical actions based on ROI from financial impact and risk reduction perspectives

Cyber Quant's Value Proposition for Key Stakeholders

CISO

- ✓ Develop strategy to address security gaps and organization's risk posture over time
- ✓ Adjust IT and security roadmaps based on tangible gaps & maturity evaluations
- ✓ Justify budgetary needs with quantified ROI and "what-if" analyses
- ✓ Utilize quantified risk analytics to evaluate cyber insurance coverage

The Board and CEO

- ✓ Oversee quantified automated reporting and cyber risk data in real-time via dashboards
- ✓ Easily conduct ROI and "what-if" analyses before any activity involving cyber risk

Compliance Officer

- ✓ Pre-assess qualification for industry-standard certifications
- ✓ Leverage Cyber Quant assessment's track record to highlight the organization's focus on cybersecurity and risk management

CRO

- ✓ Communicate cyber risk in terms that are easily understood across the business
- ✓ Maintain visibility of cyber risk with granularity by business asset, division, and technology stack levels

CFO

- ✓ Quickly assess the cyber risks of divestitures and M&A activities
- ✓ Provide budget prioritization guidance driven by quantified risk insights

Cyber Quant

Assessment Types

Cyber Quant gives you flexibility to utilize various elements to conduct five different assessment types ranging from a quick check in less than one hour to an in-depth assessment spanning a few weeks. Multiple assessments can be aggregated to understand the risk across different departments or across a portfolio of companies. Periodic assessments enable you to track trends in your cyber posture to assess continued investments in cyber threat protection and the dynamic threat landscape. Cyber Quant effectively provides you a centralized strategic cyber risk dashboard of your organization.

Questionnaires

Based on the Cyber Quant Security Framework (CQSF) with 47 control categories, the *platform gives you flexibility in the depth of assessment suitable for your business needs.*

	CQ One	CQ Two	CQ Three	CQ Four	CQ Five
Depth of Questionnaire	15 Questions	24 Questions	47 Questions	188 Questions	544 Questions
Threat Landscape Analysis (Cyber Insights)	Medium	Medium	Medium	High	High
Technical Analysis (CyMA)	CQ Essentials Technology Checks		Both	CQ Essentials Technology Checks	
Assessment for Industry Frameworks	Not Enabled		Available	Available	Available
Financial Impact & Risk	Yes	Yes	Yes	Yes	Yes
Simulation & What-if Analyses	Not Enabled		Enabled	Enabled	Enabled
Remediation Action Recommendations	Basic	Basic	Both	Detailed	Detailed
Level of Confidence	Initial	Low	Medium	Moderately High	High

Cyber Quant assessments using Cyber Quant Essentials Questionnaires can be further improved with auxiliary questionnaires to augment assessment of various frameworks and standards such as:

- ✓ NIST CSF 1.1
- ✓ ISO 27002:2022
- ✓ PCI-DSS 4.0
- ✓ CIS Controls 7-8
- ✓ HIPAA
- ✓ CQSF

Threat Landscape

All Cyber Quant users will have personalized threat landscape information based on the organization's environment automatically factored into their assessments. Based on assessment type, the personalized threat landscape information is defined in the following manner:

Cyber Quant Lite: Environments are created with a *series of questions*. These questions determine the business assets, technologies that store them, and the industry and location specific to the environment.

Cyber Quant Essentials: For each environment, *risk practitioners* define stored business assets, technologies that store and process these assets, as well as the specific industry and location of the environment.

.

Technical Analysis

Cyber Quant Lite: Risk practitioners performing Cyber Quant Lite assessments can count on the following integrations to augment and improve assessment results. These checks can be completed passively with minimal user interaction.

- ✓ APIVoid
- ✓ WhatIsMy Browser
- ✓ MyToolbox
- ✓ RiskRecon

Cyber Quant Essentials: Risk Practitioners performing Cyber Quant Essentials assessments can utilize the Cyber Maturity Analysis (CyMA) module to gain a deeper understanding of the maturity of your controls. In this module, it is possible to import technical configuration files from +60 technologies. Some notable examples include:

- ✓ AWS
- ✓ Azure
- ✓ Check Point
- ✓ Fortigate
- ✓ McAfee
- ✓ Microsoft Active Directory

Both assessment types have access to Cyber Front integration to validate and improve the control maturity ratings.

Evaluate & Act

Cyber Quant Lite: Holistic view of organization's cyber risk and the corresponding financial impact for the assessed organization or department.

Cyber Quant Essentials: An extensive and interactive dashboard is available for users who opt in. In addition, a simulation engine and multiple reports are available to articulate the risk and financial impact in various contexts.

Cyber Quant

The Cyber Quant platform empowers standards & frameworks maturity and cyber risk assessments to suit organizations large and small

	Maturity Assessment	*Cyber Risk Assessment*		
	Cyber Quant Assessor	**Cyber Quant Lite**	**Cyber Quant Essentials**	**Cyber Quant Ecosystem**
Depth of Questionnaires	• CQSF • NIST CSF • CIS • CRI • PCI DSS • ISO 27002 • GDPR • Brazil Privacy Framework • Others	• 15 / 24 / 47 questions	• 47 / 188 / 500+ questions • Combine with CQ Assessor	• Assess multiple organizations (businesses, departments, locations) • Combine multiple Essentials and Lite assessments into a singular view
Technical Analysis	• Passive checks [1] • Interactive / integrated checks [2]	• Passive checks	• Passive checks [1] • Interactive / integrated checks[2]	• Passive checks[1] • Interactive / integrated checks[2]
Threat Landscape Analysis (Cyber Insights [3])	• Pair up with Essentials version for threat landscape analysis	• Mastercard Cyber Insights based analysis on organization's threat landscape	• Mastercard Cyber Insights based analysis with additional attackers & attack methods analysis and reports	• Amalgamation of Cyber Insights across the ecosystem
Financial Impact & Risk Analysis	• Pair up with Essentials version for financial impact & risk analysis	• Included	• Included	• Included
ROI Simulation & What-if Analyses	• Pair up with Essentials version for ROI simulations	• Not included	• Included	• Included
Dashboards & Reports	• Mid-level	• Light-level	• Detail-level • Assess shared services	• Individual & Aggregated Dashboards • Prioritization amongst organizations
Implementation Guidance	• Advisory services available	• Advisory services for aggregated analyses for bulk purchases	• Advisory services available	• Advisory services available

1. Passive Checks run in the background checking security for OS, browser, mail server, and organization's website. These use light weight versions of Mastercard solutions like Risk Recon and Cyber Front, plus 3rd party solutions. Additional licensing may be required.
2. Interactive / integrated Checks on organization's infrastructure and application technologies. These are based on the platform's integrations with 60+ network, server, application, database, and security technologies. Additional licensing may be required for Risk Recon and Cyber Front.
3. Cyber Insights' threat landscape analysis for Cyber Quant cyber risk assessment is included. Additional license is required

Cyber Insights

Overview

Key stakeholders gain visibility into your organization's threat landscape enabling them to make proactive decisions on where to invest and what actions to prioritize.

Cyber risk assessments are traditionally perimeter-centric, ignoring the dynamic adversarial threat landscape facing the organization and affected by geo-political, economic, and technological factors. While ISO 27002 now requires organizations to collect and analyze cyber threat intelligence, only 30% include it as a critical component of their cybersecurity operating model. Evaluating the threat landscape provides full visibility into ongoing and future forecasted threats, enabling strategic decision-making and improved cybersecurity resilience.

Key Benefits of Cyber Insights

- Higher visibility into external threats and impacting factors
- Efficient resource utilization towards controls accurately aligned with threat landscape
- Reduced likelihood of an attack with mitigation strategy informed by actionable threat trend forecasts
- Evaluation of security resilience which identifies areas at risk from current and emerging threats

How Cyber Insights Works

Cyber Insights quickly provides strategic threat intelligence using thousands of qualified sources through the following 4 steps:

1

Data Collection

Mastercard integrates and manages thousands of clear, deep and dark web intelligence sources which are crawled and processed through the Cyber Insights system.

2

Data Processing

The system holds Mastercard's multilingual thesaurus consisting of tens of thousands of entities and synonyms. Each intelligence item is processed using a granular text analysis tool.

3

Statistical Analysis

The system combines and aggregates repetitions of the same permutation of entities, creating statistics for each one via the Cyber Insights platform.

4

Output

The query-based SaaS interface outputs:

- ✓ Cyber trends and threat landscape analysis
- ✓ Threat patterns and forecasts
- ✓ Customized intelligence reports

Competitive Advantage

Security as a Business Model

Mastercard has hands-on experience protecting petabytes of its own data with the Cyber Insights framework.

Personalized Insights

Mastercard analyzes risks taking into consideration the threat landscape tailored to a client organization.

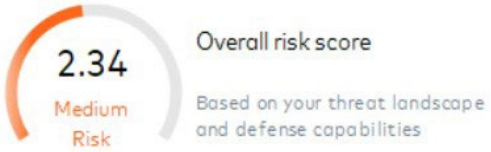
Dynamic Adjustments to New Threats

Our methodology makes it possible to account for the changing environment of cyber threats and dynamically respond to new attack vectors.

Cyber Quant

Risk and Financial Impact Quantification

Cyber Quant is a cyber risk quantification tool that leverages strategic threat intelligence coupled with accurate control maturity assessments to systematically identify, assess, and quantify the risks to an organization's business assets at multiple granularities. Two key outputs from the assessment are the Risk Score and the Financial Impact range amount for the organization from cyber security-related adverse events.



As you input demographic information, complete the questionnaire, and upload technical configuration files, the Cyber Quant platform employs a 9-step process to understand the organization, generate insights for remediation and calculate financial impact based on the organization's associated costs.

Step 1: Control Maturity Assessment

Controls maintain parameter-based adherence to best practices, policies, and procedures established by the organization, standards, or product vendor to protect business assets. Cyber Quant utilizes both human and machine inputs to achieve a high level of reliability when measuring the maturity of the security posture.

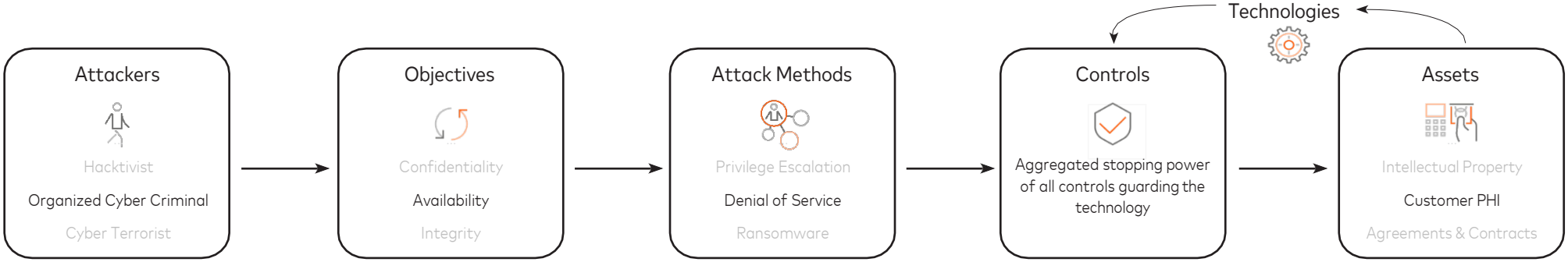
Step 2: Threat Activity Level

The cybersecurity threat landscape is understood through a strategic threat intelligence model that is tailored to the organization's location and industry. Threat actors' methods, capabilities and preferred targets are examined and assessed using intelligence from around the world coupled with Mastercard proprietary intelligence.

Step 3: Probability of Success (PoS) of Attack Methods

Once the internal and external context of the organization is understood with the Control Maturity and Threat Activity Level insights, the Probability of Success (PoS) of each attack method is calculated. PoS is the probability that an attack method will succeed based on how it compares to a defensive vector of controls and their defensive power.

Attack methods are selected based on the skills and objective of the attacker. To reach the asset, the attack method must overcome the controls guarding it. Controls guarding the asset depend on which technologies the asset is stored in. For each possible attack scenario, a PoS is calculated. This metric is used to understand which assets are most at risk, which attackers or attack methods pose the greatest risk and which controls need improvement.



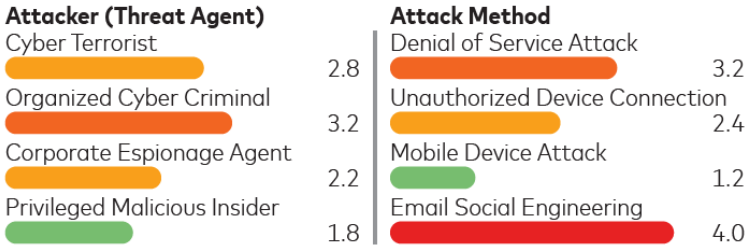
Cyber Quant

Risk and Financial Impact Quantification

1 Control Maturity Assessment | 2 Threat Activity Level | 3 PoS of Attack Methods | **4 Attacker/Attack Threat Levels** | **5 Business Assets Risk Level** | **6 Environment Risk Level** | **7 Organization's Risk Level** | **8 Remediation Priorities** | **9 Financial Impact Calculation**

Step 4: Attacker/Attack Threat Levels

After understanding the PoS for each attack method on a single asset, it is possible to aggregate this information for each asset to calculate the risk of a single attack method. Similarly, the PoS for all attack methods used by an attacker can be aggregated to calculate the risk of a single attacker.



Step 5: Business Assets Risk Level

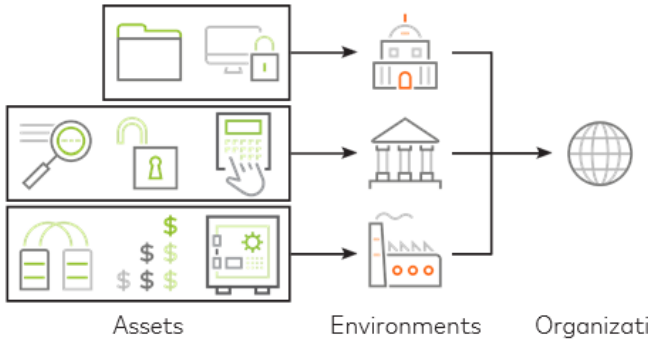
To understand the attacks on a single business asset, the Cyber Quant platform aggregates all risks associated with said asset. This can be further broken down by the objective of the attacker to understand the risk to the confidentiality, integrity and availability of the asset.

Step 6: Environment Risk Level

Similar to business asset risk, the Cyber Quant platform aggregates all risks associated with all assets in an environment to calculate to the environment risk level.

Step 7: Organization Risk Level

For a higher-level view, the Cyber Quant platform aggregates all risks associated with all environments in an organization to yield the organization risk level. This can be illustrated in the following chart.



Step 8: Remediate Priorities

Based on data produced from all previous steps, Cyber Quant calculates a metric called control importance, which measures how the improvement of a specific control would affect the environment risk level. This metric determines prioritization of control improvements to remediate risks.

Step 9: Financial Impact Calculation

The financial impact of these risks is calculated using statistical methods along with historical data. This data can be used to articulate cyber risk to leadership or other personnel who are not necessarily information security professionals.

Cyber Quant

Cyber Maturity Analysis - CyMA

Cyber Maturity Analysis (CyMA) is a component of Cyber Quant that allows you to validate and augment your Cyber Quant Assessments. At its core, CyMA is a tool to help you collect and analyze:

- ✓ Design effectiveness data from questionnaires conducted by information security professionals
- ✓ Operating effectiveness data from analyzing configuration files of various technologies

CyMA Workflow

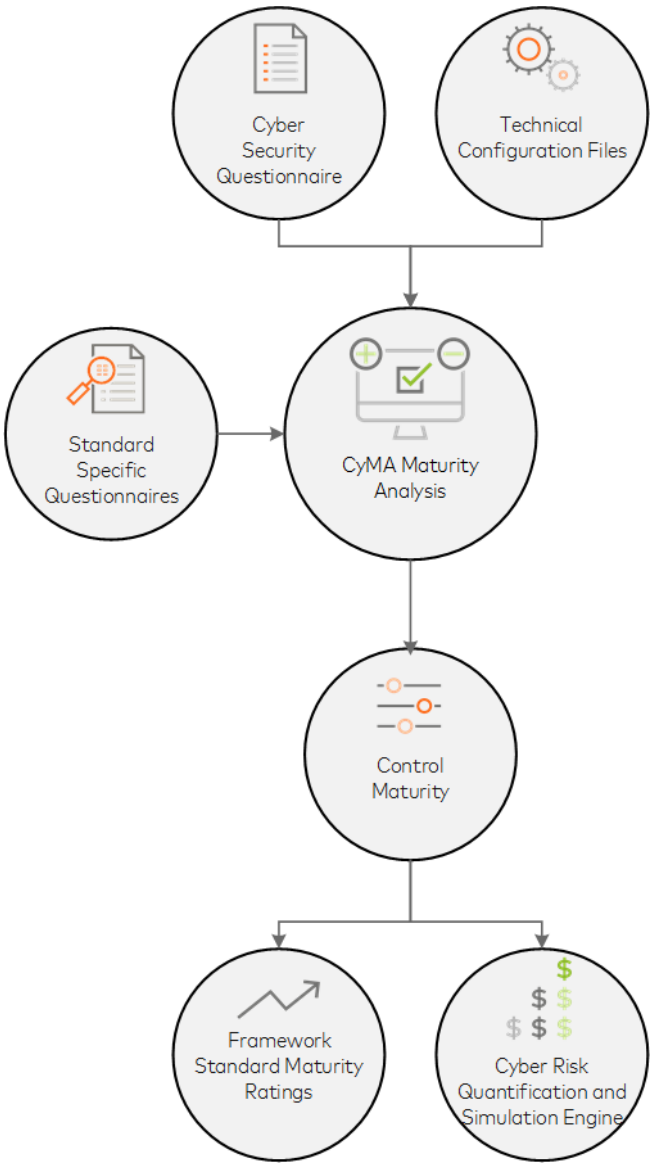
To evaluate the maturity of an environment, by default, Cyber Quant employs a list of 47 controls. The exact amount may change when doing maturity analysis. The controls are grouped based on selected standard or framework.

Additionally, each control comprises indicators of maturity gathered from technical assessments of security products and systems as well as questionnaires providing a comprehensive assessment of the control. Incorporating maturity data from security standards and framework enriches the control maturity assessment even further.

During this assessment, multiple samples from endpoints and servers may be required. CyMA is equipped to process technical configuration files from multiple endpoints to present a baseline for the entirety of the environment.

Unlike the rest of the Cyber Quant platform, CyMA is installed on-premises. This is part of our data minimization strategy. CyMA does not upload your technical configuration files to the Cyber Quant platform on cloud and only uploads control maturity ratings.

As long as the host system is connected to the internet, CyMA will function in Online Mode and continue to send maturity ratings of the controls to the Cyber Quant dashboard, enabling the risk dashboard to update and continually adjust environment risk. Changes in maturity ratings will affect the enterprise-wide risk rating and the calculated financial impact of cyber risk on the organization depending on the current security posture.



Cyber Quant

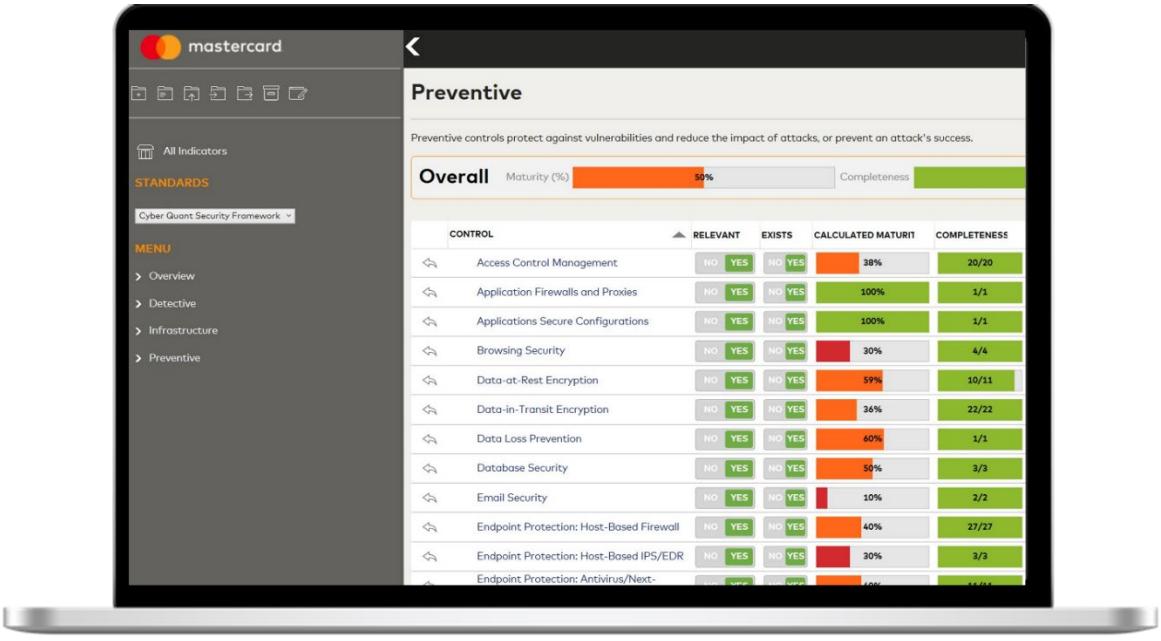
Cyber Maturity Analysis – CyMA

Standard Compatibility

By default, the Cyber Quant platform uses a proprietary standard called **Cyber Quant Security Framework**. This framework is based on various standards and frameworks that form the industry security standards and frameworks such as IS 27002, NIST CSF, and more.

Cyber Quant enables clients to conduct maturity assessments of various standards and frameworks. CyMA deploys secondary questionnaires to Cyber Quant to manage that, allowing standard-specific indicators to be added to the computation. The system is highly customizable, and different standards can be added to fit your organization's specific needs. CyMA allows maturity analysis against standards such as:

NIST CSF 1.1 | **ISO 27002:2022** | **PCI-DSS 4.0** | **CIS Controls 7-8** | **HIPAA**



Technology Integrations

Validation is achieved by importing technical configuration files from +60 technologies, comparing them against maturity indicators based on environment and industry best practices. To ensure the security of your organization's data, these processing activities are done on premise.

To ensure greater visibility into information technologies, CIS-CAT Pro Assessor has been incorporated into CyMA with licensure for use. CyMA leverages CIS-CAT Pro reports to scan any system in the network against various CIS benchmarks.

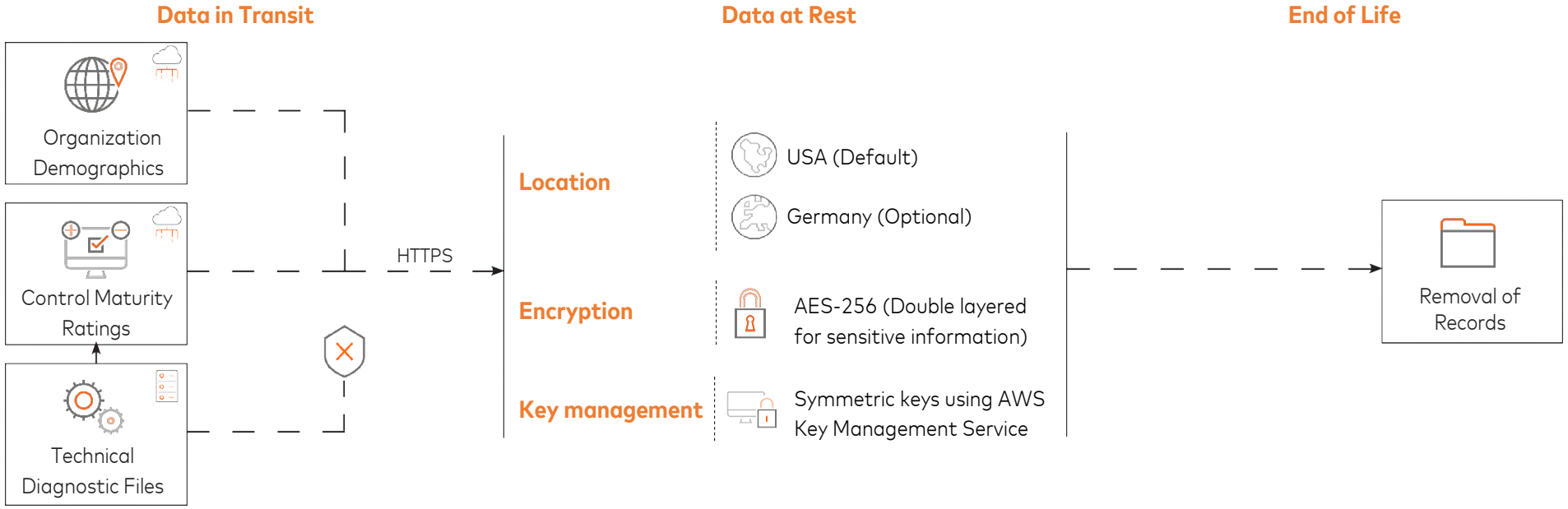
Notable examples include:

- ✓ AWS
- ✓ Microsoft Cloud Security
- ✓ Check Point
- ✓ Crowdstrike
- ✓ Fortigate
- ✓ McAfee
- ✓ Palo Alto
- ✓ Okta
- ✓ Symantec
- ✓ Windows Enterprise
- ✓ Windows Server
- ✓ CentOS Linux
- ✓ Cisco IOS
- ✓ Google Chrome
- ✓ Microsoft Edge
- ✓ Microsoft Exchange
- ✓ Oracle MySQL Enterprise Edition
- ✓ Google Kubernetes Engine
- ✓ Amazon Elastic Kubernetes Service
- ✓ Kubernetes
- ✓ VMWare
- ✓ Palo Alto Firewall

Cyber Quant

Data Handling

Data protection and privacy is embedded into the design and creation of all Mastercard products and services. Extensive procedures and processes are in place to ensure that only necessary data is processed. Before any data is considered for collection, an extensive review and approval process is executed by Mastercard's Information Security and Privacy teams to minimize collection, protect access, and manage retention.



With your security needs in mind, Cyber Quant does not process any of your technical diagnostic files in the cloud and keeps those files strictly on premises.

Only necessary data is retained to manage the functioning of Cyber Quant. This data is kept on an Amazon Relational Database, which ensures Cyber Quant users are in compliance with all security standards upheld by AWS.

To ensure data is transmitted securely to Cyber Quant, all access to the database is granted through HTTPS. AWS Key Management Service is used to encrypt data in all stages of processing.

Clients are onboarded to an availability zone in USA by default. If any client prefers to host their information in Europe due to reasons such as regulatory requirements, it is possible to host information in an availability zone in Germany.

According to Mastercard's policies, different categories of data have different retention requirements. The total retention period from the first statement of work to deletion of the project documentation is 84 months.

Upon request, Mastercard will remove customer information from all devices or storage media unless retention is required to comply with applicable regulations or procedures.

When all retention requirements are satisfied, Mastercard will certify that customer information has been removed, physically destroyed, securely erased, or returned to customer using an industry accepted technique to render customer information irretrievable from all devices or storage media.

Cyber Quant

Reporting Capabilities

Cyber Quant comes with an interactive dashboard, through which you can monitor risk and cyber posture.

Cyber Quant also offers a range of reports that can be generated on demand, which provide information needed to understand, articulate and remediate risk both at the enterprise level and for constituent parts of the organization.

9 Comprehensive Report Types

1. Mastercard Detailed Technical Report

An assessment based on the Cyber Quant Security Framework (CQSF) with 47 control categories The platform gives you flexibility to choose the depth of assessment suitable for your business needs

2. Full Report

A detailed view of the control maturity, risk, financial impact, threat landscape and remediation priorities through multiple assessments at an environment level

3. CQ Lite Report

A holistic view of an organization's cyber risk and the corresponding financial impact for the entire enterprise as well as for each business asset

4. Management Report

A visualization of the risk score, control importance, financial impact and threat landscape of the entire enterprise encompassing multiple assessments

5. Technical Diagnostics versus Questionnaire

A comparison between controls maturity levels as perceived by the organization and controls maturity levels calculated through technical configurations

6. Standards and Frameworks Maturity Report

Detailed information regarding the maturity of controls, broken down on a per-indicator basis for each standard

7. Control Maturity Breakdown

Control maturity data gathered from questionnaires and technical analysis of a single environment

8. Sources Breakdown by Control

This report contains all indicators gathered per control from all available sources

9. Instances Report

Raw and calculated maturity data gathered from questionnaires and technical analyses

Use Case Legend

Intended for Leadership | Intended for Technical Staff | Financial Impact Information | Standard Specific Information | Control Maturity

Thank you

For more information on Cyber Quant, please visit us at https://cyberquant.zendesk.com/hc/en-us

Alternatively, you can contact our Cyber Quant team at support@cyberquant.com

Intellectual property
Please note that the contents of this document are for demonstration, comparison, and review. Individual images may belong to third parties and may not be reproduced in any way.

Confidentiality
The contents of this document are strictly confidential and may not be shared with any other parties without Mastercard's permission.