Vendor Cyber-Risk Profile

Completed by:

Data Virtuality

Gartner®

Self-Report Risk Assessment

The Gartner Vendor Cyber-Risk Profile applies our best-practice research to provide CIOs, chief information security officers (CISOs) and their teams with a seamless way to identify and reduce risks related to the use of third-party vendors. Aligned to ISO, NIST 800-53 and NIST CSF, this standardized profile covers critical controls a vendor should employ to protect its customers' data and assets.

This profile characterizes the security posture of the following segment(s) of**:**

Business segment:	Data Virtuality
Website:	https://datavirtuality.com/en
Headquarters:	Leipzig, Germany
Public-facing security statements:	
Additional security information available at:	sales@datavirtuality.com
Short description of the service or products offered by the segment:	The Data Virtuality Platform is the sole advanced data virtualization solution in the market that brings the greatest flexibility to enable any modern data architectures incl. hybrid- and multi-cloud architecture, data fabric, and data mesh. By combining data virtualization with ETL/ELT, customers can always choose the best method for their specific requirements.

Gartner has not validated the information provided on this profile. The following person has certified that they are authorized to provide information regarding their company's security program and that all information is true and accurate to the best of their knowledge:

Name:	**Matthias Werner**
Title:	Head of Finance & Analytics
Date:	November 29th, 2022

Recent third-party audits, penetration tests and other artifacts that may have been included in the submission of this profile are not embedded.

Human Resources Security		
1. Do you train your employees regarding their specific role and the information security controls they must fulfill?	Yes	
2. Are all employees required to formally agree to apply information security in accordance with the established policies and procedures of the organization?	Yes	
3. Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	Yes	
4. Are all employees required to take recurring security awareness education and training, as relevant for their job function?	Yes	
5. Are employees subjected to disciplinary action in the event of noncompliance to security policies and procedures?	Yes	
6. Are contractors monitored and managed by an employee at your organization to ensure compliance with company policies and procedures?	Yes	
7. Are all personnel required to adhere to a Confidentiality Agreement or an Acceptable Use Policy to protect customer information?	Yes	
8. Are documented policies, procedures and guidelines in place to govern change in employment and/or termination including timely revocation of access and return of assets?	Yes	

Compliance and Privacy		
1. Do all practices that involve the creation, modification or storage of data comply with all legal, regulatory and contractual obligations?	Yes	
2. Are there procedures to ensure compliance of intellectual property with all legislative, regulatory and contractual requirements?	Yes	
3. Are there procedures in place regarding records retention to ensure records are protected from loss, destruction, falsification, unauthorized access and unauthorized release in accordance with legislative, regulatory and contractual requirements?	Yes	
4. Has the organization developed and maintained an approved and published external privacy notice?	Yes	
5. Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes	
6. Does your organization conduct regular privacy impact/maturity assessments?	Yes	
7. Do you perform, at a minimum, annual reviews to your privacy policies?	Yes	
8. Does your organization have cyber insurance (technical or professional errors and omissions insurance)?	Yes	
9. Do you have independent reviews and assessments performed at least annually, for example by Internal Audit or third-party providers, to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations?	Yes	

Identity and Access Management		
1. Is there a documented user access process that dictates requirements for requesting, approving, reviewing and removing access rights for all user types to all systems and services?	Yes	
2. Are access rights established and limited on the basis of specific business requirements (principle of least privilege)?	Yes	
3. Are access rights for all users reviewed at regular intervals?	Yes	
4. Are processes or controls put in place to ensure no single individual can access, modify or use critical assets without authorization or detection (i.e., a single individual should not be able to both authorize and then initiate an event that affects critical data)?	Yes	
5. Do you manage and store the identity of all personnel who have access to IT infrastructure, including their level of access?	Yes	
6. Where required by access control policy, are access to systems and applications password protected?	Yes	
7. Are passwords compliant with access management policies governing password complexity and password handling?	Yes	
8. Are controls in place to lockout users after a defined number of unsuccessful attempts to access their account?	Yes	
9. Do you require multifactor authentication (MFA) for all users?	Yes	MFA is required for all systems that support it.
10. Do all users have a unique ID to perform system functions? If shared IDs are used, please describe.	Yes	
11. Are inactive accounts disabled and/or removed after a set period of time (e.g., 90 days)?	No	All accounts are reviewed on a regular basis. In addition, inactive accounts are reviewed in an ad hoc manner. If there is no need for access anymore, the inactive account will be disabled after review.
12. For users that are authorized to access systems and data remotely, are access credentials required (VPN, MFA) to authenticate to the system?	Yes	

Asset Management and Data Protection		
1. Do you maintain a complete inventory of all of your assets that includes ownership of the asset and asset details?	Yes	
2. Is the asset inventory updated on a periodic basis for the addition and removal of assets?	Yes	
3. Do you have a formal information classification policy?	Yes	
4. Are there appropriate procedures in place to ensure all data is correctly labeled and handled in accordance with its classification level and corresponding policy guidelines?	Yes	
5. Do you store data from multiple clients on properly segregated databases, networks and/or other storage capacities?	N/A	
6. Will all devices and removable-media storing or processing client data have full encryption?	Yes	
7. Do you encrypt client data in transit?	N/A	
8. Do you encrypt client data at rest?	N/A	
9. Do you have a key management policy within your organization that addresses management and monitoring of keys?	Yes	
10. Is a key management system used to store the keys, and is the use of keys by personnel logged?	Yes	
11. Do you prohibit the use of removable media in your organization?	Yes	
12. If so, do you have a policy governing the permissible use of removable media?	Yes	
13. Do you prevent client data from being accessed, modified, or stored on remote desktops or laptops?	Yes	
14. Do you have a documented data disposal process in place (record management and retention policy)?	Yes	
15. Are all items of equipment containing storage media verified to ensure that any sensitive data and/or licensed software have been removed or securely overwritten prior to disposal or reuse?	Yes	

Logging and Monitoring		
1. Do you log data such as access, exceptions, faults, security events, etc.?	Yes	
2. Are audit logs protected against modification, deletion and/or inappropriate access (including system administrators and operators)?	Yes	
3. Do you employ monitoring solutions on the audit logs with alerting capabilities for suspicious activity?	Yes	
4. Are audit logs maintained per retention policies?	Yes	
5. Do you employ intrusion detection tools to facilitate timely detection, investigation and response to security incidents?	N/A	
6. Do you monitor the network, including firewall and IDS/IPS, for security events on a 24x7x365 basis?	Yes	
7. Do you have a staffed SOC 24x7x365 or an on-call process that supplements staffed coverage for full 24x7x365 coverage?	Yes	
8. Do you have a defined incident response and management process/plan to manage and respond to information privacy and security incidents within an agreed timeline?	Yes	
9. Do you test your Incident Response Program at least annually?	Yes	
10. Do you have a defined process and plan to notify relevant clients in the event of information breaches and/or incidents?	Yes	
11. Do you attest that your organization has not experienced an information security breach in the past three years?	Yes	
12. In the event of an incident, do you have processes and procedures for forensic analysis and chain of custody?	Yes	

Physical and Environmental Security		
1. Does your organization have a formal documented physical and environmental security policy that is periodically reviewed and updated?	Yes	
2. Are all physical premises and/or processing facilities protected to ensure that only authorized personnel are allowed access?	Yes	
3. Do your physical premises and/or processing facilities have environmental controls to protect client data?	Yes	
4. Do you have a documented visitor policy that ensures that visitors are escorted at all times?	Yes	

Threats and Vulnerabilities		
1. Do you have antimalware programs installed on all of your IT infrastructure network and system components?	Yes	
2. Do you have antivirus (AV) or host-based intrusion prevention systems (HIPS) in all resources that will be storing or processing client data?	Yes	
3. Do you regularly scan your external/internal infrastructure for vulnerabilities?	Yes	
4. Do you have an established process to patch vulnerabilities across all of your computing devices, applications and systems in a timely matter?	Yes	
5. Do you employ a risk-based prioritization approach to patching all servers, databases and applications (e.g., critical within seven days, high within 10 days)?	Yes	
6. Do you use system hardening configurations to ensure only necessary features and services are provided?	No	
7. Are there restrictions on the installation of software on operational systems?	Yes	
8. Does the organization have a threat intelligence program and/or use external resources to stay up to date and monitor threats to your environment?	N/A	
9. Do you conduct network and application penetration tests of your environment on at least an annual basis?	Yes	

Development Security and Change Management		
1. Are there documented Change Management and Software Development Life Cycle Management policies and procedures in place?	Yes	
2. Are the development, testing and operational environments separate to reduce the risks of unauthorized access or changes to the operational environment?	Yes	
3. Are changes to information systems, operating platforms and applications made during development appropriately reviewed and tested to ensure there is no adverse impact on the organization's operations or security?	Yes	
4. Do you prevent the use of production data in lower environments?	Yes	
5. Do you have a process in place to detect security defects in code prior to deployment through mechanisms such as DAST and SAST?	Yes	
6. Are changes approved prior to migration to production through appropriate IT owners and/or a Change Control Board?	Yes	

Network Security		
1. Are all networks being used to transfer information formally identified and documented by IT?	Yes	
2. Are messaging systems (including email, instant messaging, chat services, etc.) appropriately protected so the confidentiality and integrity of information is protected in transit?	Yes	
3. Is sensitive information passing over public networks protected from fraudulent activity, contract dispute, unauthorized disclosure and modification, mis-routing and incomplete transmission?	Yes	
4. Are firewall rules reviewed and updated on a frequent basis?	Yes	
5. Does the organization maintain system and network topology and architecture diagrams that are reviewed and updated when changes occur?	Yes	
6. Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes	

Business Continuity and Disaster Recovery		
1. Does your organization have a defined and implemented Business Continuity/Disaster Recovery Policy or an equivalent document for the continuity of offered services?	Yes	
2. Do you test your Business Continuity/Disaster Recovery plan periodically, with critical business functions tested at least annually?	Yes	
3. Are there frequent backups of information, software and system images in compliance with data management policy?	Yes	
4. Do you have an off-site backup storage facility or provider?	Yes	
5. Do you encrypt your backups?	Yes	

Third-Party Risk		
1. Has your organization defined and implemented a formal process (that includes due diligence) for managing any third parties that may require access to client information?	Yes	
2. Does your organization have defined contractual agreements with third parties that process customer information?	Yes	
3. Do you perform information security reviews and/or audits of your third-party providers to ensure that all agreed-upon security requirements are met periodically on the basis of risk?	Yes	
4. Do you ensure that services or products that are being provided to the end client are not subcontracted out to a fourth party without client notification?	Yes	

Methodology and Terms

This profile was generated based on a vendor's profile for the Gartner Third-Party Cyber-Risk Management Solution for CIOs and CISOs.

CIOs and CISOs are under increased pressure from their boards to measure third-party cyber risk, resulting in thousands of hours of redundant surveys being sent to your organization.

The Gartner Third-Party Cyber-Risk Management solution will provide CIOs, CISOs and vendors with a seamless way to request, respond to and interpret third-party risk assessments, all from a single profile for your organization.

The Gartner profile applies our best practice research to provide CIOs, CISOs and their teams with a seamless way to identify and reduce risks related to the use of third-party vendors. Aligned to ISO, NIST 800-53 and NIST CSF, this standardized profile covers critical controls a vendor should employ to protect its customers' data and assets. It may not be comprehensive for every organization's needs.

Gartner does not validate information provided by vendors on their profiles.

This Gartner template may be distributed to your customers or prospects in accordance with the Gartner Content Compliance Policy.

Permission is hereby granted to use this Gartner template with vendor responses, but it must not be altered or changed in any way. The only permitted edit is the inclusion of information that would otherwise be confidential or require an NDA.

This template may not be hosted in the public domain or otherwise shared with external parties that are not customers or prospects. It may not be replicated or used for any purpose other than the transmission of risk information between vendors and buyers/potential buyers.

The template may be used for the earlier of (a) one year from date of attestation, or (b) when responses are no longer representative of your security posture. Other than information requiring NDA, information on this sheet must represent those in the Gartner third-party risk platform.

For additional details on the Gartner Content Compliance Policy, please see: https://www.gartner.com/en/about/policies/content-compliance

For additional details about the services Gartner offers to CIOs, CISOs and other IT roles, please see: https://www.gartner.com/en/information-technology/role

If you are a vendor looking to complete another assessment or seeking more information, please see: https://surveys.gartner.com/s.aspx?s=d6b95701-0a81-40a9-901d-e1d2fa048d01

