EPIPHANY | INTELLIGENCE PLATFORM

Security & Trust, Standard.

This document is for clients who are either intending to use, or are using Reveald's Epiphany Intelligence Platform. Its purpose is to help you understand how we protect the data the platform accesses and analyzes.

INTRODUCTION

The Epiphany Intelligence Platform's mission is to accelerate the ability for anyone to understand and act on cyber risks by differentiating between what is merely vulnerable to what is exploitable. We believe that time to context matters, and security should be consumable for any risk decision maker. Our goal is to provide actionable insights on where the most likely exploitable points of risks could occur in the daisy chain from an initial compromise to a material/significant event that could affect your organization and its stakeholders. Thus, we believe protecting your data is a sacred responsibility. We are committed to being transparent about our security practices and helping you understand our approach.

To be transparent we must first and foremost start with the actual risks that we as your solution provider could pose to your organization. We are not an active control so we could not be used as a weapon to directly shut down your business. We do not directly collect sensitive data from your organization; however, we do ingest data that could be sensitive in nature about your environment and turn those into actionable insights as to where you are most exploitable in ways that could cause material harm to your organization or your stakeholders. So, we pose a potential aggregation risk since the enriched data and attack path mapping we provide could in some cases be more sensitive than the independent data silos that already exist within your organization today.

This document is intended to explore the primary risks that could occur, the likely exploitable attack paths, and our approach to controlling for those risks. Some aspects for control to mitigate the potential risks with the use of the Epiphany Intelligence Platform will be our responsibility and some responsibility will be rest with our customers. Working together, focusing on the potential exploitable attack paths of where the Epiphany Intelligence Platform could be used to cause harm, we believe our risk as a 3rd party will be low.

PROGRAM DETAILS

The Epiphany Intelligence Platform is based on our belief that vulnerability does not equal exploitability. In our own internal efforts to secure our organization, as well as the capabilities we deliver, we are leading the way in the industry to change the risk equation that we have all used for decades.

The traditional approach: Risk = F (Threat, Vulnerability, Consequence)

The Epiphany Intelligence Platform way: Risk = F (Threat, EXPLOITABILITY, Consequence)

We believe that transforming how we contemplate, calculate, and ultimately focus our efforts to manage and mitigate risk should be changed from the historic norms that have been calcified in our industry over decades. While hygiene

efforts and vulnerability management will never go away, they have distracted our ability to focus and act on the fulcrum point(s) of risk that cause material harm – those points of exploitability that lead from compromise to catastrophe. The broad-based vulnerability distraction has contributed to rising costs, rising risks, and has caused security to continue to fall behind the exponential growth of our IT environments. Our approach to security looks not only on the breadth of our environment—the traditional attack surface perspective—but brings a vigilant focus on exploitability to gain an attack depth perspective that hones our control environment to minimize risks to the greatest extent possible.

Our security program is led by our Chief Information Security Officer (CISO) Ambassador as well as our Chief Technology Officer (CTO). Between them they are responsible for the implementation and management of our security program with a focus on security architecture, product security, security engineering and operations, detection and response, as well as overall risk and compliance.

PRIMARY RISKS

The primary risks that can be associated with the use of the Epiphany Intelligence Platform that could cause the potential for material harm to your organization are as follows in priority order:

- An attacker gains access to the Epiphany Intelligence Platform and uses it as a targeting system to accelerate a planned attack against your organization. Think of this as the "evil google maps scenario."
- A leak occurs and data on your attack paths and exploitability points is now in the public domain. This expands the "evil google maps scenario."
- A false positive/false negative occurs in our system causing inaccurate decisions on points of exploitable risks.
- The Epiphany Intelligence Platform is poisoned to alter the attack paths causing inaccurate decisions on points of exploitable risks.
- You transform how you calculate and manage risk towards a focus on exploitability and the Epiphany Intelligence Platform is offline which affects your ability to take action to mitigate your organizations points of exploitable risk.

OUR RESPONSABILITY TO YOU

As a software-as-a-service provider, we are the data processor of your information. As the data processor, our responsibility is to protect, secure, and safeguard your information as it is in transit or stored within our environment. We will make all efforts, in line with industry best practices, to secure each of the components within our processing pipeline and back-end systems. In the event an incident occurs that impacts the security of your data, we will promptly notify you as soon as we are reasonably able.

YOU RESPONSABILITY TO YOURSELF

As the data owner, you have a responsibility to safely access our platform and ensure adequate security safeguards are in place to secure the communications between the Epiphany Intelligence Platform and you. In the event of a potential security issue, you should notify Reveald as soon as reasonably possible so that a joint investigation can take place. We recommend that you, as the data owner, do at least the following:

- Appropriately safeguard devices used by the administrators of the Epiphany Platform and consider them as critical systems.

- Ensure your Epiphany Intelligence Platform user accounts are, at a minimum, using multi-factor authentication or an SSO portal.
- Access to the Epiphany Intelligence Platform is regularly reviewed by your security team.
- Old or unused accounts are removed from the Epiphany Intelligence Platform.
- Data extracted from the Epiphany Intelligence Platform is handled according to your internal data handling policies.

SUPLEMENTAL INFORMATION

While this document is not exhaustive, it does represent an overarching summary of the major areas of our security and trust program. Any specific questions about our program can be referred to *security@reveald.com*.

PROTECTING PRIVACY

Epiphany considers data privacy to be of paramount importance. Our privacy principles guide our focus and we have codified our privacy efforts accordingly. We define personal data as any information relating to an identified or identifiable natural person.

PRIVACY PRINCIPLES

+ **Accountability:** We strive to be a responsible steward of the personal data we manage on behalf of all individuals who share personal data with the Epiphany Intelligence Platform and to uphold these privacy principles. It is our goal to ensure personal data is always processed in a fair and lawful manner.
+ **Privacy by Design:** We seek to embed privacy into our business processes, products, and services by proactively identifying and addressing privacy risk early in the lifecycle of new projects in order to safeguard personal data entrusted to the Epiphany Intelligence Platform.
+ **Purpose and Use Limitation:** We will always attempt to limit our collection and use of personal data to the specific purposes that have been communicated. We will not use personal data in any way that is incompatible with the purpose for which it was collected.
+ **Transparency:** We will always try to provide clear descriptions of our policies and practices that collect, process, transfer, and disclose personal data.
+ **Choice:** Where possible, we will always describe the choices that are available and allow individuals to make informed decisions about the personal data they share with us.
+ **Data Minimization:** We will always strive to collect the minimal amount of personal data that is necessary for the purpose communicated.
+ **Security for Privacy:** We will always seek to protect personal data from unauthorized access throughout the data lifecycle with security safeguards that are appropriate for the sensitivity of the personal data.
+ **Integrity & Access:** Personal data should be accurate and kept up to date. Where feasible, we allow individuals to have access to their personal information to review and update.
+ **Transfer:** We only transfer personal data to authorized third- arties after informing users, and only for purposes that have been communicated or are compatible with the collection.
+ **Storage Limitation:** We endeavor to retain personal data for the minimum amount of time required to complete the purpose for which it was collected, or as required by law. After the purpose has been fulfilled, we will responsibly remove it in a timely manner.

SECURE BY DESIGN

The Epiphany Intelligence Platform's software, the platform it runs on, and the environment it runs within, is built with security as its core tenant. To help eliminate possible gaps in security, we have implemented redundant security controls within our environment and throughout our software. However, while we strive to catch all vulnerabilities in the due course of business, we realize that sometimes mistakes happen. We encourage our customers, industry experts, and partners to submit any bugs or security concerns to our security email at *security@reveald.com*.

DATA INGESTION, STORAGE AND PRIVACY

To protect our customers and their users from data compromise, the Epiphany Intelligence Platform takes every effort to ensure any personal identifying information (PII) collected is stored anonymized, obfuscated, hashed and/or encrypted. The Epiphany Intelligence Platform only collects data from systems our customers have either uploaded or where our customer has enabled data ingestion to the Epiphany Intelligence Platform via the use of an API.

Data at rest in the Epiphany Intelligence Platform's production network is encrypted using FIPS 140-2 compliant encryption standards, which applies to all types of data at rest within the Epiphany Intelligence Platform's relational databases, file stores, database backups, etc. All encryption keys are stored in a key management system with very limited access.

The Epiphany Intelligence Platform has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials. Each Epiphany Intelligence Platform customer's data is either hosted in our environment and is logically separated from any other customers' data or hosted in your own environment with a unique Epiphany Intelligence Platform instance. We use a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested.

The Epiphany Intelligence Platform service is hosted in data centers maintained by industry-leading service providers, offering state-of-the-art physical protection for the servers and infrastructure that comprise the Epiphany Intelligence Platform operating environment. Supplemental information on data usage within the Epiphany Intelligence Platform can be found in the Epiphany Intelligence Platform Data Usage Guide.

NETWORK SECURITY AND SERVER HARDENING

The Epiphany Intelligence Platform divides its systems into separate networks to better protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting the Epiphany Intelligence Platform's production infrastructure.

All servers within our production fleet are hardened (e.g., disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment. Network access to the Epiphany Intelligence Platform's production environment from open, public networks (the Internet) is restricted, with only a small number of production servers accessible from the Internet.

Only those network protocols essential for delivery of the Epiphany Intelligence Platform's service to its users

are open at our perimeter and there are mitigations against distributed denial of service (DDoS) attacks deployed at the network perimeter. Additionally, for host-based intrusion detection and prevention activities, the Epiphany Intelligence Platform logs, monitors, and audits all system calls and has alerting in place for system calls that indicate a potential intrusion.

ENDPOINT SECURITY

All workstations used by Reveald personnel are configured by the Epiphany Intelligence Platform to comply with our standards for security. These standards require all workstations to be properly configured, updated, tracked, and monitored. The Epiphany Intelligence Platform requires workstations to encrypt data at rest, use a modern endpoint protection, have strong passwords, and lock when idle.

ACCESS CONTROL PROVISIONING

To minimize the risk of data exposure, the Epiphany Intelligence Platform adheres to the principles of least privilege and role-based permissions when provisioning access. Workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly by our security team.

AUTHENTICATION

To further reduce the risk of unauthorized access to data, the Epiphany Intelligence Platform employs multi-factor authentication for all access to systems with highly sensitive data, including our production environment, which houses our customer data. Where possible and appropriate, the Epiphany Intelligence Platform uses private keys for authentication, in addition to the previously mentioned multi-factor authentication on a separate device.

PASSWORD MANAGEMENT

The Epiphany Intelligence Platform leverages a password management system, where possible, to ensure enhanced credential management and monitor passwords for uniqueness, complexity, reuse, dark web compromise, and other password-related risks. In cases where this is not possible, the Epiphany Intelligence Platform ensures those systems have proper controls in place and are monitored.

SYSTEM MONITORING, LOGGING, AND ALERTING

The Epiphany Intelligence Platform monitors servers, workstations, and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in the Epiphany Intelligence Platform's production network are logged and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. All production logs are stored in a separate network that is restricted to only the relevant security personnel.

DATA RETENTION AND DISPOSAL

We will store your usage data until such time when you withdraw your consent for us to do so. All other data as specified above will be retained for as long as is necessary for the purposes for which we originally collected it. We may also retain information as required by law. Customer data is removed immediately upon deletion by the

end user or upon expiration of message retention as configured by the administrator.

Upon termination of your production subscription the Epiphany Intelligence Platform will encrypt a current state backup of your information and retain it for 15 days should you wish to re-activate your subscription. If you wish this not be done, please notify us at *security@reveald.com*.

The Epiphany Intelligence Platform hard deletes all information from currently running production systems and backups are destroyed the day after the temporary retention period. The Epiphany Intelligence Platform's hosting providers, including customers that host the Epiphany Intelligence Platform or Epiphany Intelligence Platform images on premises, are responsible for ensuring removal of data from disks is performed in a responsible manner before they are re-purposed.

DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

The Epiphany Intelligence Platform utilizes services deployed by its hosting provider to distribute production operations across multiple AWS regions within the continental United States. These AWS regions are within separate geographic regions and protect the Epiphany Intelligence Platform's service from loss of connectivity, power infrastructure, and other common location-specific failures.

Production transactions are replicated among these discrete operating environments to protect the availability of the Epiphany Intelligence Platform's service in the event of a location-specific catastrophic event. The Epiphany Intelligence Platform also retains a full back-up copy of production data in a remote location significantly distant from the location of the primary operating environment. Full backups are saved to this remote location at least once per day and transactions are saved continuously. The Epiphany Intelligence Platform tests backups at least quarterly to ensure they can be successfully restored.

RESPONDING TO SECURITY INCIDENTS

The Epiphany Intelligence Platform has established policies and procedures for responding to potential security incidents. All security incidents are managed by the Epiphany Intelligence Platform's dedicated Detection and Response Team (DART). We have defined the types of events that must be managed via the incident response process and classify them based on severity. In the event of an incident, affected customers will be informed via email from our customer experience team. Incident response procedures are tested and updated at least annually. To initiate an investigation for a security-related concern, you can reach out to your customer service representative with the details or email security@reveald.com.

VENDOR MANAGEMENT

To run efficiently, the Epiphany Intelligence Platform relies on a select number of trusted external service providers. These service providers are carefully selected and meet high data protection and security standards. We only share information with them that is required for the services offered and we contractually bind them to keep any information we share with them as confidential and to process personal data only according to our instructions. Where those service providers may impact the security of the Epiphany Intelligence Platform's production environment, we take appropriate steps to ensure our security posture is maintained by establishing agreements that require service organizations to adhere to confidentiality commitments we have made to

users. The Epiphany Intelligence Platform monitors the effective operation of the organization's safeguards by conducting reviews of all service organizations' controls before use and at least annually.

EXTERNAL VALIDATION

- **Security Compliance Audits.** The Epiphany Intelligence Platform is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and the Epiphany Intelligence Platform's internal risk and compliance team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.management and all findings are tracked to resolution in a timely manner.
- **Penetration Testing.** In addition to our compliance audits, the Epiphany Intelligence Platform engages independent entities to conduct application-level and infrastructure-level penetration tests at least annually. Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner. Customers may receive executive summaries of these activities by requesting them from their account executive.
- **Customer Driven Audits and Penetration Tests.** Our customers are welcome to perform either security controls assessments or penetration testing on the Epiphany Intelligence Platform's environment during our annual Epiphany "Bright Idea" hack-a-thon. Please contact your account executive to express your desire to participate in these types of activities.

CONCLUSION

We have an existential interest in protecting your data. Every person, team, and organization deserve and should expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we will always work hard to maintain that trust.

Please contact your account executive if you have any questions or concerns or email us at *security@revealdata.com*.

MALCOM HARKINS
CISO Ambassador
Reveald

ROB BATHURST
Chief Technology Officer
Reveald