



S E C U R I T Y S T A T E M E N T

Cye Platform Security and Privacy Statement

Date: May 24, 2026

Table of Contents

1. General	3
2. Product Design and Assessment	3
3. Cye Platform Cloud Deployment and Regions.....	4
4. Cye Platform Security.....	4
4.1. Authentication and authorization of Cye Platform users.....	4
4.2. Environment security and protection	4
4.3. Vulnerability management and response	5
5. Compliance.....	5
6. Privacy and Data Policy	5
6.1. Data Collected.....	5
6.2. Data Security	6
6.3. Encryption	7
6.4. Access control.....	7
6.5. Security logs	7
6.6. Data Retention and Deletion	7
7. Backup	8
8. Disaster recovery and business continuity.....	8
9. Artificial Intelligence Security	9

1. General

This document describes how C/E protects customers' sensitive data and other information during interaction with C/e Platform, which is C/E's cloud-based cybersecurity optimization platform. This document also describes privacy policy and what data is collected; how that data is used along with all the security aspects pertaining to the protection of that data. C/E is committed to the security and privacy of our customers' data. C/E has created and follows security processes and procedures that provide comprehensive protection to C/e Platform.

The following topics that pertain to security and privacy are covered:

- C/e Platform Cloud Deployment and Regions
- C/e Platform Security
- Compliance
- Privacy and Data Policy
- Backup
- Disaster Recovery

2. Product Design and Assessment

Product security at C/E is very important, which is reflected in our policies, procedures, and operations. C/E operates according to Secure by Design principles which are employed at all stages of the SDLC. Software changes are subject to rigorous verification and validation to ensure that the platform complies with the highest standards of safety and performance. As part of this process the C/e Platform and the corresponding infrastructure are proactively and continuously pen-tested to identify potential security weaknesses and to mitigate them. This activity is being performed by the C/E Red-Team experts.

3. Cye Platform Cloud Deployment and Regions

Cye Platform is deployed in a multi-cloud configuration AWS environment on a dedicated account. The geographical regions in which the compute instances operate, and the data is stored are described in the following table:

Cloud Provider	Region
AWS	Germany, Frankfurt US, North Virginia

- For more information about AWS data protection and privacy, click [AWS](#).

4. Cye Platform Security

4.1. Authentication and authorization of Cye Platform users

User management is done through Cye Platform. Password complexity is configured to provide maximum security (Minimum of 12 characters, with requirement for upper/lower case characters, special characters, and numbers).

To increase security, customers are encouraged to enforce login by using Two-factor authentication with any multi-factor authentication application such as Google authenticator, or Microsoft authenticator).

4.2. Environment security and protection

All Cye Platform servers use hardened operating systems to meet business needs and use technical controls such as a CNAPP tool to track and monitor all activities in the environment.

4.3. Vulnerability management and response

CYE continuously monitors and mitigates newly published security vulnerabilities on an ongoing basis, including those identified by third-party software and operating system vendors. In addition, CYE performs continuous Red Team activities to verify the Cye Platform resilience and security.

5. Compliance

CYE uses independent third-party auditors to assess CYE’s regulatory compliance, and certifications:

Standard	Description
ISO 27001 - 2022	ISO 27001 is specification for an information security management system (ISMS), which is a framework for an organization's information risk management processes. Updated February 2026
SOC 2 type II	SOC 2 is a compliance standard for service organizations. It captures how a company safeguards customer data and how well those controls are operating. Updated October 2025

6. Privacy and Data Policy

6.1. Data Collected

Cye Platform provides customers with visibility to their organization’s security posture through detecting vulnerabilities and misconfigurations, by gathering relevant data that is used to identify, understand, and respond to events in a timely manner.

Cye Platform collects the following information for the purpose of providing services to its customers and improving those services. The following list includes data which may not be collected in every case. As CYE enhances the Cye Platform product's capabilities, the specified data collected may vary:

- IPs (single or a range), users, groups, computer names, domains, email addresses, services, roles, cloud services, cloud resources and cloud assets.
- The Cye Platform also manages user's data for authentication and authorization purposes. The information only contains email addresses and job titles. This information is highly secured by Cye Platform and can be deleted on demand upon official request.
- All data items collected by CYE, may be used by CYE in an aggregated and anonymized manner. The data is used to do performance testing, compile statistical information related to the provision and operation of the Cye Platform services, and to improve these services.

6.2. Data Security

Cye Platform is a multi-tenant SaaS platform that keeps customer's data logically and securely segregated. CYE implements multiple controls at many levels across different components.

To ensure that the actions of one customer cannot compromise the data of other customers.

- Customer data in Cye Platform is encrypted in transit over public networks using TLS to protect it from unauthorized disclosure or modification.
- Data gathered in Cye Platform is protected using multiple guardrails and controls including data segregation, encryption at-rest and in-transit, access control policies and procedures. For more information about AWS security measures, click [AWS data security](#).

6.3. Encryption

Cye Platform user passwords are hashed using a salted PBKDF2-SHA256 algorithm and stored in a secure database. Passwords are subject to complexity and history validation rules that prevent reuse of previous passwords.

Data at rest is encrypted using Amazon Aurora with AWS KMS-managed keys (AES-256). AWS KMS uses FIPS 140-2 validated HSMs to protect the keys.

All connections to Cye Platform services are encrypted in transit using TLS. The platform enforces TLS 1.2 as the minimum protocol version with Forward Secrecy cipher suites via AWS ALB security policy ELBSecurityPolicy-FS-1-2-Res-2020-10. Plain HTTP connections are automatically redirected to HTTPS.

6.4. Access control

Access to Cye Platform services, networks and systems is managed in accordance with CYE's access policy and is granted only to individuals who are responsible for operating and supporting the Services. Third party contractors are not permitted to connect to Cye Platform SaaS production systems.

6.5. Security logs

All logins to Cye Platform services and servers, and actions performed are audited and monitored.

6.6. Data Retention and Deletion

Customers can extract data at any time by using Cye Platform s' built-in export capabilities.

- Data deletion for customers - Customers have permission to delete manually created data items.
- Data deletion by CYE - Data can be deleted upon official request by a customer from Cye Platform production environment.

7. Backup

The Cye Platform employs a multi-tier automated backup strategy for all production databases.

Continuous Point-in-Time Recovery (PITR). Production Aurora PostgreSQL clusters are configured with automated backup retention window, enabling point-in-time recovery to any second within the backup retention window period.

Long-term Monthly Backups. Every month, a full Aurora cluster snapshot is taken and stored in a dedicated AWS Backup vault with a retention period of 13 months (396 days).

Mid-month Operational Backups. An additional snapshot is taken mid-month and retained for 47 days.

Cross-Region Replication. Long-term monthly backups are automatically replicated to a secondary AWS region (EU production > eu-north-1; US production → us-west-2), providing geographic redundancy in the event of a regional outage.

Immutability and Encryption. All backup vaults are protected by AWS Backup Vault Lock, preventing accidental or unauthorized deletion. Backups are encrypted at rest using dedicated customer-managed AWS KMS keys with automatic annual key rotation enabled.

Access Control. Access to backup vaults and restore operations is governed by a dedicated IAM role with least-privilege policies scoped exclusively to AWS Backup service operations.

8. Disaster recovery and business continuity

CYE maintains disaster recovery and business continuity plan for Cye Platform and has set Return time Objective for Cye Platform to 4 hours, while the Return Point Objective is set to 24 hours. CYE periodically tests restoring data from backups to ensure CYE is prepared for different failure scenarios.

9. Artificial Intelligence Security

CYE's AI features run exclusively on **Amazon Bedrock** within CYE's own AWS accounts. No customer data is sent to third-party AI APIs or public model endpoints. AI inference runs in the same region as the customer's tenant: EU customers' data is processed only in the EU (eu-west-1), and US customers' data is processed only in the US. Customer data does not cross regions for AI processing.

No customer data leaves CYE's infrastructure. The AI service is stateless — no conversation history or customer context is retained between requests. Customer data is scoped on the application layer before reaching Bedrock.

Prompt injections are blocked at the infrastructure level. Every AI request passes through an AWS Bedrock Guardrail with PROMPT_ATTACK detection set to HIGH. Blocked requests receive a generic refusal with no internal context exposed.

Model access is least-privilege. Bedrock agents operate under a dedicated IAM role with permissions scoped strictly to model invocation. S3 and KMS access are opt-in per agent, not granted by default.

All AI resources are encrypted with customer-managed AWS KMS keys. Data in transit to Bedrock uses TLS within AWS's private network.

AWS does not train in customer data. Amazon Bedrock's terms explicitly prohibit using customer inputs or outputs to train foundation models.

Quality monitoring. Cyec captures AI prompts and outputs for quality-control monitoring, and this data is used only for that purpose. It is stored in Cyec's production environment as part of the tenant's data, under the same controls as all other tenant data [retention period; who can access it]. This monitoring copy is not sent to Amazon Bedrock or to any model provider.

End of Document — Cyesecc Ltd. — Confidential

About Cye

Cye combines an AI-native exposure management platform with world-class cyber expertise to help organizations know the financial impact of their cyber exposure, prioritize risk mitigation and automate remediation. Cye's customers gain the clarity to make smart, defensible decisions that reduce their risk exploitability and improve their resilience to the dynamic threat landscape.

Visit us at cyesecc.com.