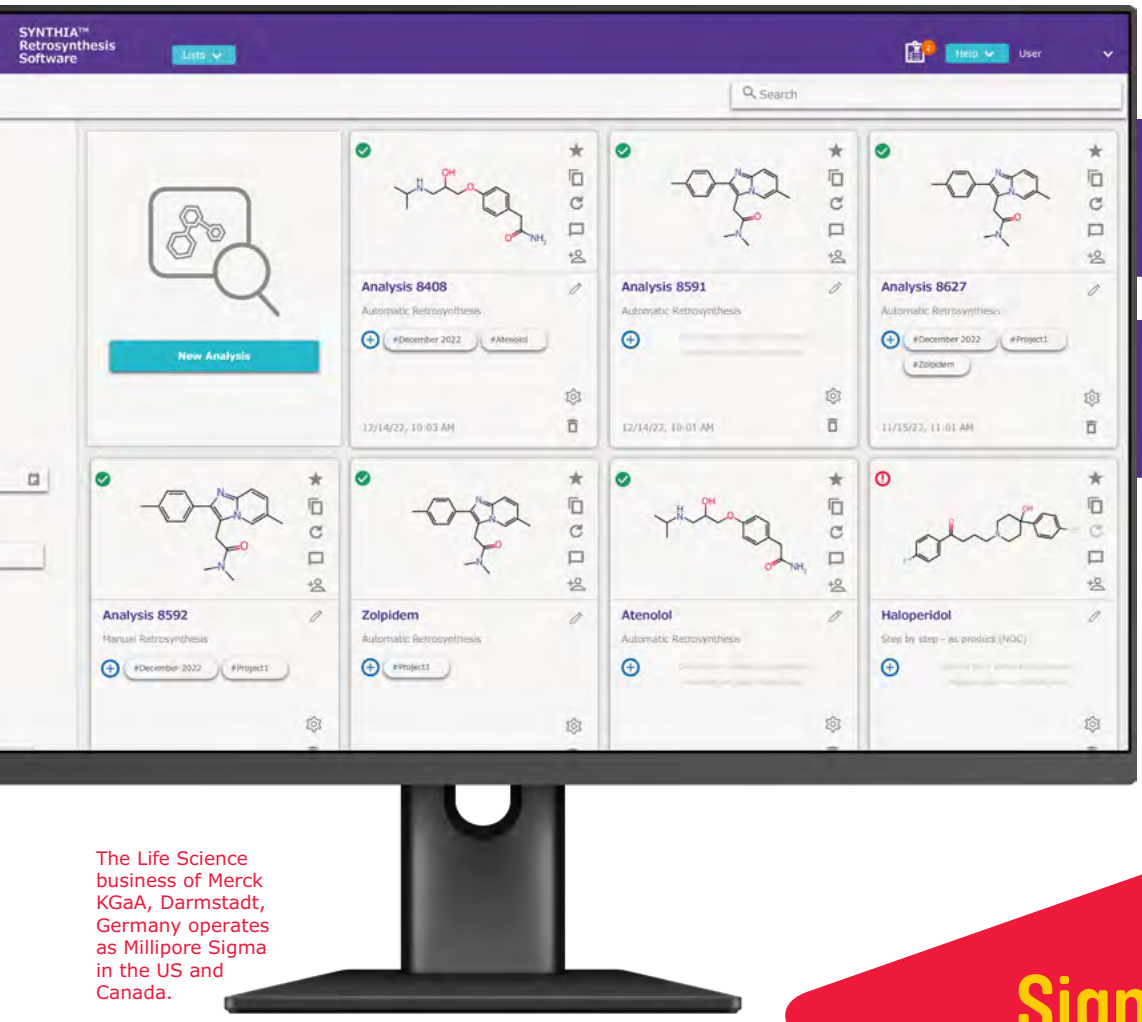
SYNTHIA® Retrosynthesis Software

Security Brief

SYNTHIA® is a cloud-based retrosynthesis software solution developed and commercialized by Merck KGaA, Darmstadt, Germany, and its affiliates. The platform is designed to enable chemists to efficiently plan synthetic routes for both novel and published molecules. Security and data protection are foundational to SYNTHIA®, as evidenced by its ISO 27001:2022 certification and top-tier cybersecurity ratings.

This document provides a factual overview of the security measures, certifications, and practices in place for SYNTHIA®, referencing only the attached and officially published sources.



Rated Platinum 2025 by cybervadis

ISO 27001 CERTIFIED by schellman

Sigma-Aldrich®
Lab & Production Materials

Security Framework Overview

An outline of core security domains and practices across governance, infrastructure, compliance, and risk management.

Information Security Governance

ISO 27001 Certification

SYNTHIA® is certified to the ISO/IEC 27001:2022 standard for Information Security Management Systems (ISMS). This certification covers the development and commercialization of SYNTHIA® and other digital solutions, ensuring a systematic approach to managing sensitive information and mitigating risks. The certification is attached.

CyberVadis Platinum Rating

In 2025, Merck received a Platinum medal from CyberVadis for outstanding cybersecurity performance, reflecting mature and comprehensive security controls across data privacy, data protection, business continuity, and third-party management.

Data Privacy and Compliance

A formal data protection policy is in place, and the Data Protection Function is responsible for the protection of personal data (PII).

Retention periods for personal data are identified, and procedures for deletion, modification, and portability are formalized.

All processing of personal data is lawful, and necessary data privacy clauses are included in contracts.

The organization complies with GDPR and other applicable data privacy regulations and has processes for notifying individuals and regulators in the event of a data breach.

Application and Infrastructure Security

Secure Development Lifecycle

SYNTHIA® follows a secure software development lifecycle (SSDLC), including static and dynamic application security testing (SAST/DAST), vulnerability management, and code reviews.

Penetration testing and vulnerability analysis are conducted at least annually, with continuous integration of security testing in the development pipeline.

Threat modeling and architecture reviews are performed regularly.

Encryption

Data is encrypted in transit using HTTPS (TLS v2) and at rest using cloud-managed encryption. Encryption keys are managed via a key management system (KMS).

All passwords are stored in salted and hashed form.

Access Control

Role-based access control (RBAC) is enforced, with multi-factor authentication (MFA) for user login.

Access rights are periodically reviewed, and the principle of least privilege is implemented for all users.

Segregation of duties and separate accounts for administrative tasks are in place.

Logging, Monitoring, and Incident Response

Security events and incidents are managed according to a formalized process, with logs protected from tampering and unauthorized access.

Network and Endpoint Security

SYNTHIA® is protected by Web Application Firewalls (WAF), intrusion detection/prevention systems (IDS/IPS), and data loss prevention (DLP) mechanisms.

Distributed Denial of Service (DDoS) protection is implemented at the infrastructure level.

Workstations and corporate storage media are encrypted, patched regularly, and protected against unauthorized access and malware

Cloud Infrastructure

SYNTHIA® is hosted on Amazon Web Services (AWS), which is regularly audited for ISO 9001, 27001, 27018, and SOC2 compliance.

The platform follows AWS Well-Architected Framework best practices, including private subnetting, key management, and continuous monitoring.

Secure configuration, firewall, and malware protection are implemented at both application and infrastructure levels.

Business Continuity and Disaster Recovery

Business continuity management and disaster recovery plans are formalized and periodically tested.

Data backups are encrypted and performed daily.

Third-Party and Supply Chain Security

Third-party access is restricted to specific systems and is governed by contracts that include security requirements, NDAs, and audit rights.

Third-party risk assessments are conducted, and cloud providers must provide evidence of business continuity and incident response plans, as well as official security certifications.

Compliance and Regulatory Alignment

SYNTHIA® is compliant with ISO 27001:2022 and GDPR.

Local compliance requirements are tracked and adopted as needed.

The platform does not process payment data and is not subject to PCI DSS requirements.

Security Awareness and Training

Information security and data privacy awareness programs are in place for all staff, including social engineering training and a clear desk policy.

New hires, contractors, and temporary workers are required to sign a code of ethics or NDA, and background checks are conducted.

Key Security Features

Comprehensive data privacy, protection, and compliance controls

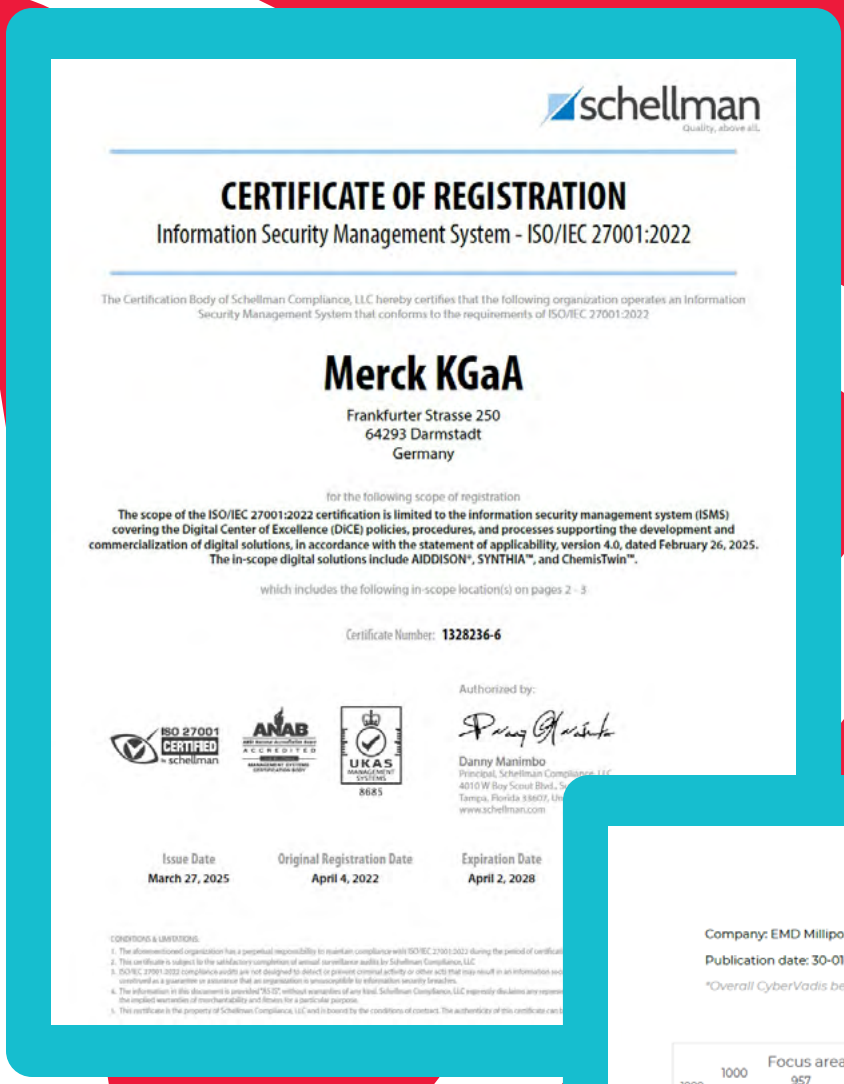
Business continuity, disaster recovery, and daily encrypted backups

Secure development lifecycle, regular penetration testing, and continuous vulnerability management

Secure AWS cloud infrastructure with regular audits and best-practice architecture

Encryption of data at rest and in transit, robust access control, and multi-factor authentication (MFA)

Strong third-party and supply chain security management



schellman
Quality, above all.

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2022

The Certification Body of Schellman Compliance, LLC hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2022

Merck KGaA

Frankfurter Strasse 250
64293 Darmstadt
Germany

for the following scope of registration

The scope of the ISO/IEC 27001:2022 certification is limited to the information security management system (ISMS) covering the Digital Center of Excellence (DiCE) policies, procedures, and processes supporting the development and commercialization of digital solutions, in accordance with the statement of applicability, version 4.0, dated February 26, 2025. The in-scope digital solutions include AIDDISON®, SYNTHIA™, and ChemisTwin™.

which includes the following in-scope location(s) on pages 2 - 3

Certificate Number: **1328236-6**

Authorized by:

Danny Manimbo
Principal, Schellman Compliance, LLC
4010 W Boy Scout Blvd., Ste. 600
Tampa, Florida 33607, United States of America
www.schellman.com

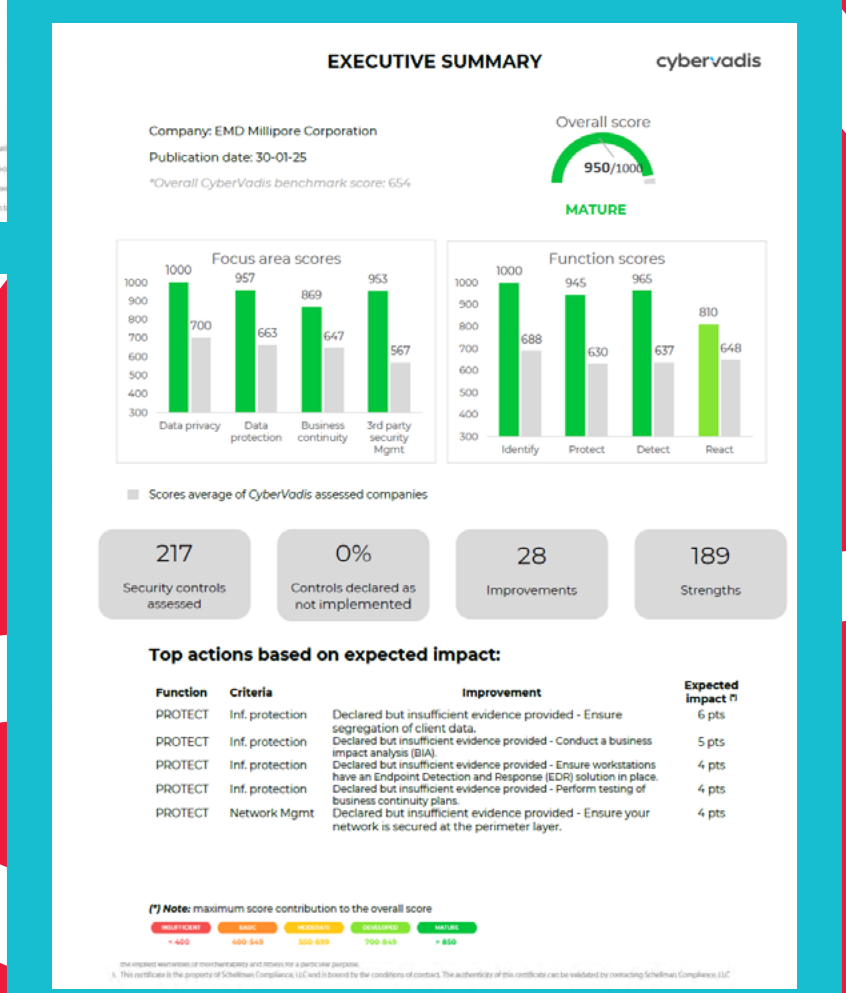
Issue Date	Original Registration Date	Expiration Date
March 27, 2025	April 4, 2022	April 2, 2028

8685

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO/IEC 27001:2022 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by Schellman Compliance, LLC.
3. ISO/IEC 27001:2022 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. ISO/IEC 27001:2022 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. Certification is not construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Schellman Compliance, LLC expressly disclaims any representation or warranty, express or implied, including the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of Schellman Compliance, LLC and is bound by the conditions of contract. The authenticity of this certificate can be validated by contacting Schellman Compliance, LLC.

ISO 27001 CERTIFIED by schellman



EXECUTIVE SUMMARY

cybervadis

Company: EMD Millipore Corporation
Publication date: 30-01-25
*Overall CyberVadis benchmark score: 654

Overall score
950/1000
MATURE

Focus area scores

	Data privacy	Data protection	Business continuity	3rd party security Mgmt
	1000	957	869	953
	700	663	647	567

Function scores

	Identify	Protect	Detect	React
	1000	945	965	810
	688	630	637	648

Scores average of *CyberVadis* assessed companies

217	0%	28	189
Security controls assessed	Controls declared as not implemented	Improvements	Strengths

Top actions based on expected impact:

Function	Criteria	Improvement	Expected impact
PROTECT	Inf. protection	Declared but insufficient evidence provided - Ensure segregation of client data.	6 pts
PROTECT	Inf. protection	Declared but insufficient evidence provided - Conduct a business impact analysis (BIA).	5 pts
PROTECT	Inf. protection	Declared but insufficient evidence provided - Ensure workstations have an Endpoint Detection and Response (EDR) solution in place.	4 pts
PROTECT	Inf. protection	Declared but insufficient evidence provided - Perform testing of business continuity plans.	4 pts
PROTECT	Network Mgmt	Declared but insufficient evidence provided - Ensure your network is secured at the perimeter layer.	4 pts

(*) **Note:** maximum score contribution to the overall score

INSUFFICIENT	BASIC	MODERATE	DEVELOPED	MATURE
< 400	400-549	550-699	700-849	> 850

the implied warranties of merchantability and fitness for a particular purpose.

5. This certificate is the property of Schellman Compliance, LLC and is bound by the conditions of contract. The authenticity of this certificate can be validated by contacting Schellman Compliance, LLC

Rated Platinum 2025 by cybervadis

MK_DS15005EN Ver. 1.0 11/2025