WHITE PAPER

commercetools Security White Paper 2025

What's inside

Introduction

From emerging start-ups to global enterprises, businesses rely on the commercetools commerce platform to power their operations. Our platform enables companies to manage rich product data, manage shopping carts and seamlessly handle order and customer information in a unified system. Given its critical role in our merchants' success, ensuring the continuous availability and security of the commercetools platform — particularly its API infrastructure — is paramount.

However, reliability alone is not enough. commercetools is committed to adhering to industry-leading security standards and maintaining compliance with global privacy regulations to provide businesses with a secure and trustworthy environment.

Transparency is a cornerstone of our security approach. Our customers need to know who can access their data, when and what safeguards are in place to prevent unauthorized access. This white paper offers an in-depth look at our security frameworks, protocols and controls, demonstrating how commercetools safeguards businesses and their customers worldwide.

What is commercetools

commercetools has redefined the future of commerce by empowering businesses to break free from legacy constraints and embrace a truly composable approach. As the pioneers of headless commerce in 2012 — long before “composable commerce” became an industry standard — we have continuously pushed the boundaries of innovation.

Today, commercetools provides businesses with the essential building blocks of modern commerce, delivering unparalleled flexibility, scalability and performance. More than just a technology provider, we are a trusted partner, ensuring our customers operate with resilience, security and confidence in an ever-evolving digital landscape.

What security means to commercetools

At commercetools, security is not just a feature; it's a fundamental pillar of our platform. As a SaaS provider entrusted with powering businesses worldwide, we recognize that our customers must have absolute confidence in our security model. That's why we adhere to **Secure by Design** principles, embedding security into every layer of our infrastructure, development lifecycle and operational processes.

Our comprehensive security framework is built on industry-leading standards, regulatory compliance and a proactive approach to risk management. We have established a robust Governance, Risk and Compliance (GRC) program that aligns with modern security controls to address evolving threats, ensuring our platform remains resilient against cyber risks. From encryption and access controls to continuous monitoring and threat detection, we integrate best practices that safeguard customer data and ensure business continuity.

Security is woven into the fabric of our corporate strategy, enabling our customers and partners to operate with trust and confidence. By continuously evolving our security posture and staying ahead of emerging threats, commercetools empowers businesses to focus on growth — without compromising on security.

Shared security model

The shared security responsibility model is a widely adopted framework used by leading cloud providers, including Amazon AWS, Microsoft and Salesforce, to define the distinct security obligations of the provider and the customer. In a composable SaaS environment like commercetools, this model is essential to maintaining a secure and resilient ecosystem.

As the SaaS provider, commercetools ensures the security of the platform, infrastructure, APIs and compliance with industry standards and data protection regulations. We implement robust security controls, including encryption, access management and continuous monitoring, to safeguard the foundation on which businesses operate.

However, customers also play a crucial role in securing their commerce solutions. Since commercetools provides an extensible and API-driven platform, customers develop their own business logic, integrations and custom extensions that interact with our system. This means they must adhere to secure coding practices, enforce access controls and proactively manage vulnerabilities in their custom implementations.

By embracing this shared responsibility, commercetools and its customers collectively ensure that security is maintained end-to-end, enabling a scalable, flexible and trusted commerce experience.

Security culture

At commercetools, we recognize that data ownership remains solely with our customers, and we are committed to maintaining their data confidentiality, integrity and security at all times. Our Data Processing Agreement (DPA) explicitly defines our obligations in accordance with applicable data protection laws, ensuring that commercetools will process customer data only for the purposes necessary to fulfill contractual obligations. commercetools will never use data for unauthorized purposes.

Furthermore, commercetools provides customers with full control over their data, including the ability to request deletion of their information at any time. This extends to backup, log, and monitoring data, which will be securely erased upon request in compliance with regulatory requirements.

To uphold data portability rights, commercetools enables customers to retrieve and migrate their data at their discretion without incurring penalties or additional costs. This ensures that businesses retain complete autonomy over their data, even if they choose to discontinue our services. Our commitment to data privacy, security and compliance reinforces the trust that businesses place in commercetools as their commerce technology provider.

commercetools' security controls

commercetools take proactive measures to protect our employees, customers, and partners from risks related to information security. To achieve this, we have implemented a comprehensive Information Security Management System (ISMS) based on industry best practices. This system ensures that sensitive information is securely handled, stored, and processed across our organization.

To maintain the effectiveness and reliability of our security framework, our Security Team conducts regular internal and external audits, along with annual penetration testing, to identify and mitigate potential vulnerabilities.

Dimensions of security controls

Security at commercetools is not a singular function: It is a foundational principle embedded across every aspect of our platform, operations and ecosystem. Our approach to security is comprehensive, addressing risks across multiple dimensions to ensure the confidentiality, integrity, and availability of customer data and services.

To achieve this, we measure security across the following key dimensions:

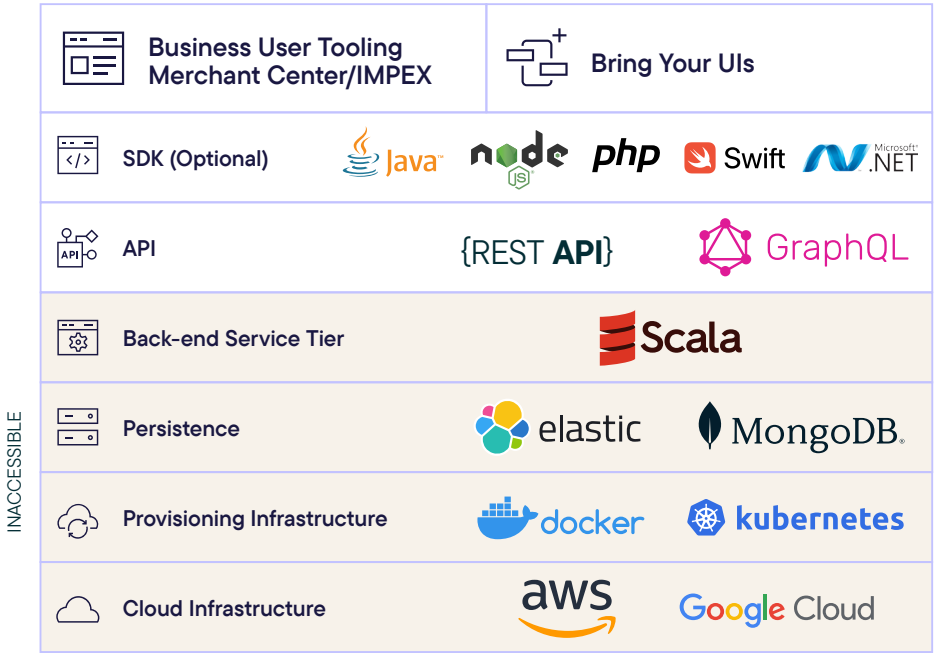
- Infrastructure security
- Operational security
- Data security
- Product security
- Business continuity and disaster recovery
- Compliance and governance

Infrastructure security

System overview

commercetools is a next-generation commerce platform designed to give businesses unparalleled agility, flexibility and versatility over their commerce operations. At the core of commercetools' composable commerce architecture are the MACH™ principles — Microservices-based, API-first, Cloud-Native and Headless—which enable businesses to build modular, scalable, and high-performing commerce solutions. The platform is designed for global scalability and is available on leading cloud providers, including Google Cloud and Amazon Web Services (AWS), ensuring resilience, security and performance at an enterprise level.

To further enhance reliability, commercetools leverages containerized deployments and auto-scaling capabilities, allowing the platform to dynamically adjust to traffic spikes and maintain high availability at all times. This ensures businesses can scale effortlessly, innovate faster and deliver exceptional commerce experiences without limitations.



API security

The commercetools platform secures API access through OAuth2-based authentication, requiring every request to include a valid, short-lived token issued by our dedicated OAuth2 service. These time-bound tokens minimize the risk of unauthorized access and reduce exposure in the event of credential compromise. Additionally, customers have the ability to create long-lived API keys for server-to-server integrations. While commercetools provides the infrastructure to manage these keys, it is the customer's responsibility to rotate them periodically and follow key management best practices to maintain a strong security posture.

Each token is assigned a specific scope, defining what data and functionalities can be accessed or modified. Scopes ensure that API interactions are contextually restricted, meaning a token generated for managing product catalogs will have different access rights than one issued for processing orders or handling customer data. This scoped approach provides fine-grained control over API access, ensuring that each integration or user receives only the necessary permissions to perform their designated operations.

Payment API

The commercetools platform is architected to avoid storing or processing sensitive payment information directly. Instead, our Payment API enables businesses to reference key payment transaction details—such as transaction IDs or statuses—without handling actual payment data. These references can be associated with orders and passed to external systems like ERPs for secure downstream processing.

Any actual payment processing, including the capture of card or banking information, must occur outside of the commercetools platform, within an environment managed by the customer or a certified payment service provider (PSP). This ensures a clear separation of concerns and significantly reduces PCI compliance scope for merchants using commercetools.

For frontend implementations, especially at checkout, it is strongly recommended to build solutions that comply with PCI DSS SAQ-A level requirements, which apply to setups where no payment data passes through or is stored on merchant systems. This model helps businesses maintain a high level of security while streamlining compliance efforts.

Access controls

At commercetools, access to systems and data is governed by the principles of “need to know” and least privilege, ensuring that individuals only have access to the resources required for their specific responsibilities. This is enforced through a robust Identity and Access Management (IAM) system, which centrally manages and monitors all user roles and permissions.

Roles and access rights are defined by the asset owner or system administrator, based on the functional requirements of the role, and must be formally approved by the team lead. Whenever an employee’s role changes or they leave the organization, access rights are promptly reviewed and updated to prevent unauthorized access.

To maintain the integrity of this process, regular access reviews are conducted to validate that permissions remain appropriate over time. This structured and transparent approach ensures tight access control, reduces security risk and supports compliance with internal governance and external regulatory requirements.

Environment segregation

commercetools maintains a strict separation between production and non-production environments. Customer data is not used in development or testing environments, which are strictly limited to non-production purposes.

As a multi-tenant platform, we ensure complete data isolation by storing each customer's project data in a logically separated database, accessible only by the project owner. This architecture guarantees strong segregation of persistent data, which is continuously monitored and validated to uphold the highest standards of data privacy and security.

Data security and privacy

Data security and privacy are critical to maintaining customer trust and regulatory compliance. At commercetools, we protect all customer data through strong encryption, strict access controls and compliance with global data protection standards, ensuring it is handled securely and used only for its intended purpose.

Data isolation

A core focus of commercetools' security strategy is to consistently protect customer data. As a multi-tenant platform, we enforce strict data separation by storing each project's data in a logically separated database, accessible only by the owning customer. This ensures full isolation and segregation, which is regularly verified to maintain the highest levels of security and privacy.

Data in-transit

The commercetools platform is built on a carefully selected software stack, designed from the ground up with security in mind. Following the principle of defense in depth, we leverage leading cloud providers with secure, modern infrastructure that surpasses traditional IT environments in both protection and manageability.

All communication with the platform is strictly enforced over HTTPS, secured by TLS 1.2 or higher. Non-TLS connections are redirected, ensuring that data in transit is always encrypted and protected from unauthorized access.

Data at rest

All data at rest is encrypted using AES-256, with encryption managed by each cloud provider's central key management service. Data is encrypted, with automatic key rotation and comprehensive audit logging. User passwords are securely salted and hashed using modern cryptographic algorithms and are never stored in plain text.

Operational security

Operational security at commercetools is a core part of our risk management strategy. It is focused on preventing unauthorized access to sensitive information and is seamlessly integrated into our day-to-day operations to ensure continuous protection.

Network security

commercetools employs a multi-layered, cloud-native network security architecture across AWS and GCP to ensure secure, scalable, and resilient operations in a multi-tenant SaaS environment. All traffic is encrypted using TLS 1.2 or higher, securing internal service communication. A combination of perimeter network controls and cloud-native tools provides DDoS, high availability, and application-level protection.

Vulnerability management

To maintain a strong security posture, commercetools performs regular vulnerability scans across its office networks to detect and remediate potential weaknesses. We also actively monitor threat intelligence feeds and security alerts to stay ahead of emerging risks.

Our platform undergoes continuous scanning for exposed ports, misconfigurations and weak SSL/TLS certificates, ensuring adherence to the latest security standards. In addition, we conduct annual penetration tests through independent third-party security firms, providing an objective assessment of our platform's defenses and helping us identify and address vulnerabilities proactively.

Patch management

At commercetools, all services are continuously reviewed for security-relevant aspects to ensure they meet evolving threat and compliance requirements. This includes regular assessments of configurations, dependencies and services.

Wherever possible, we automate security checks and monitoring to detect issues early and respond quickly. Security patches and updates are applied on a regular schedule or immediately in the case of high-severity vulnerabilities, ensuring that our platform remains protected against known threats at all times.

Malware prevention

icommercetools maintains formalized security policies that strictly prohibit the use of unauthorized software and define clear guidelines for the acceptable use of systems, data and network resources. These policies are designed to reduce risk, prevent the introduction of unvetted or malicious applications and ensure that all employees follow consistent and secure practices when accessing company systems.

Additionally, our incident response procedures are well-documented and regularly communicated, so that employees know exactly how to report suspicious activity or security incidents, enabling a fast and coordinated response.

To protect endpoint devices, all commercetools-managed laptops and workstations are equipped with centrally managed anti-virus and anti-malware solutions, which are automatically updated to defend against the latest threats. This combination of policy enforcement and technical protection helps maintain a secure and compliant IT environment across the organization.

Security monitoring

commercetools' IT systems are continuously monitored across all layers — from physical infrastructure to platform components and the office network — using automated processes. We combine internal system metrics with external behavior and availability to ensure end-to-end visibility. This proactive approach helps us detect and resolve issues early, minimizing the risk of business-critical outages and ensuring platform reliability.

Incident management

The commercetools operations team provides 24/7/365 monitoring and incident response, following standardized diagnostic procedures to quickly detect, assess and resolve any business-impacting events. To ensure data resilience, we perform regular backups, enabling reliable data recovery even in the event of unexpected disruptions, protecting customer data and ensuring continuity of service.

Product security

Secure personnel practice and culture

At commercetools, we recognize that employees are central to our security posture and that technical controls are most effective when reinforced by a strong security culture. We foster this culture throughout the entire employee lifecycle — from onboarding to daily operations — by actively engaging employees and contractors in security awareness and best practices. This includes:

Before hiring: At commercetools, we take proactive steps to ensure that all employees and contractors meet our high standards of trust and integrity. Prior to hiring — and where legally permitted — all candidates undergo comprehensive background checks, which include a review of criminal records and financial history. For roles involving sensitive financial responsibilities, such as senior finance positions, we also conduct credit checks.

These screening procedures are a critical part of our security and risk management framework, helping to safeguard our operations and customer data from insider threats. The effectiveness of our background check policies is independently verified as part of our SOC 2 Type II audit, which is available for review under NDA upon request.

Upon hiring: All employees and contractors complete a structured onboarding process that includes:

- Signing a Proprietary Information and Inventions Agreement (PIIA) outlining their confidentiality obligations.
- Completing employment onboarding and security awareness training.

This training ensures all new hires clearly understand their security responsibilities from day one.

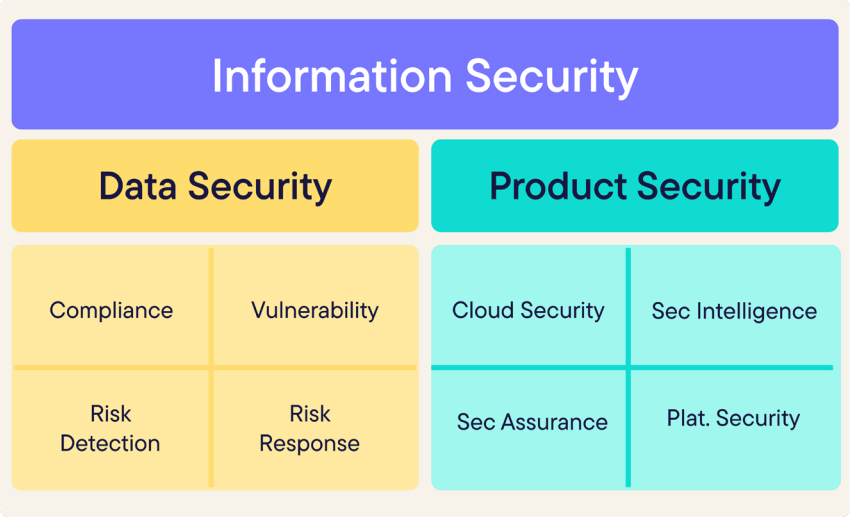
While working: Throughout their time at commercetools, employees and contractors receive continuous security awareness training to reinforce their data protection responsibilities. The security team also conducts regular social engineering tests and awareness campaigns to strengthen the security culture across the organization.

Departing: commercetools employees and contractors in this phase are reminded of their confidentiality obligations, and their accounts, credentials, devices and access badges are promptly revoked within a defined timeframe to ensure security continuity.

This proactive approach ensures that **security is everyone's responsibility**, embedded into our daily operations and decision-making.

Security team

At commercetools, our security investments are closely aligned with our product strategy and organizational culture, enabling us to deliver a strong, resilient platform. We go beyond simply adopting best practices: We have built a dedicated security and compliance team focused on maintaining, enhancing and embedding secure development and compliance practices across the entire product lifecycle. This strategic integration ensures that security is not an afterthought but a core component of how we build, innovate and grow.



Development practice

commercetools follows a comprehensive CI/CD (Continuous integration and continuous delivery/deployment) model within an agile development framework, allowing teams to deliver high-quality software quickly and efficiently. Developers work in short, iterative cycles, ensuring that new features, updates and fixes can be safely released at any time.

All development and testing take place in isolated, non-production environments, reducing the risk of unintended impact on live systems. Before any code reaches production, it goes through testing, peer reviews and multi-step approval workflows, ensuring that only fully vetted and stable code is deployed. This approach enables commercetools to maintain rapid innovation while upholding the highest standards of reliability, security and performance.

- **Secure development training:** Educates developers on secure coding practices to prevent vulnerabilities early in the SDLC.
- **Security consideration in design:** Embeds security principles during architecture and design to mitigate risks from the outset.
- **Secure code assurance:** Ensures code meets security standards through validation and best practice enforcement.
- **Security assessment:** Comprehensive evaluation of systems to identify security weaknesses and areas of improvement.

Performance management and scalability

The goal of performance management at commercetools is to ensure the infrastructure, platform services and supporting operations are continuously optimized to deliver high availability, reliability and cost-efficiency. This approach supports our customers in meeting their business objectives — whether they are experiencing steady growth or sudden traffic spikes.

Our platform is built on a distributed, cloud-native and asynchronous architecture, which allows for intelligent auto-scaling based on real-time demand. As customer usage and transaction volumes increase, the platform can automatically allocate additional resources across multiple services and components with minimal manual intervention. This ensures that performance remains consistent, even during peak periods such as product launches or seasonal events.

To validate these capabilities, commercetools conducts internal load simulations and stress tests under varied scenarios, ensuring the system can handle large-scale operations while maintaining low latency and high throughput. Performance metrics are continuously monitored and system adjustments are made proactively to avoid bottlenecks.

This scalable and resilient architecture enables commercetools to offer a future-proof commerce platform, capable of adapting to customer needs without compromising on performance or stability — regardless of market dynamics or business scale.

commercetools live Status - https://status.commercetools.com/

Business continuity and disaster recovery

commercetools has a comprehensive business continuity plan designed to identify and mitigate risks from internal and external threats, ensuring operations continue during adverse events such as natural disasters, cyberattacks or human error.

Redundancy and high availability architecture

commercetools' cloud infrastructure is designed for maximum uptime and fault tolerance, ensuring our platform remains reliable even in the face of disruptions. We deploy our services across multiple physical availability zones within each cloud region, creating built-in redundancy and failover capabilities.

Our database clusters are also distributed across these zones, so if one availability zone experiences an outage due to hardware failure, natural disaster or other incidents,data remains intact and services continue running without interruption. This architecture ensures that our customers can rely on commercetools for consistent performance, even under adverse conditions.

Data backup and recovery objectives

commercetools maintains a robust data backup and recovery strategy to ensure data integrity and availability in the event of a disruption. Our backups are designed with a small to medium recovery time objective (RTO), meaning we can restore services within a reasonable timeframe depending on the nature and scale of the incident. Additionally, we maintain a small recovery point objective (RPO), which minimizes the amount of data that could be lost by ensuring backups are taken frequently.

Depending on the impact and scope of the data loss, commercetools can perform either a partial restore (targeting specific datasets) or a full restore (recovering the entire system). This flexible approach allows us to respond effectively to various failure scenarios while maintaining continuity of service and protecting customer data.

Supplier relationship

Before onboarding any new suppliers, commercetools conducts a thorough security and compliance assessment to ensure they meet the same level of protection we uphold internally. This includes verifying their technical and organizational measures (TOMs), which are formally documented in a TOM inspection report and reviewed regularly to ensure continued compliance.

If a supplier is required to process personal data, a data processing agreement (DPA) is established to define responsibilities and data protection obligations. When customer data is involved, the supplier is formally designated as a sub-processor in our master DPA, ensuring full transparency and alignment with privacy regulations such as GDPR. This structured process helps us maintain a secure and compliant supply chain, safeguarding both our operations and customer trust.

Compliance, governance and industry regulations

commercetools also continuously undergoes independent verification of platform security, privacy and compliance controls. Our strong and growing focus on standard conformance and compliance will help you meet your regulatory and policy objectives.

commercetools service certifications

ISO 27001

ISO 27001 is an international standard, developed by the International Organization for Standardization (ISO), that sets rigorous requirements for managing information and ensuring its confidentiality, integrity and availability. TÜV Rheinland, an independent auditor, has verified that our Information Security Management System (ISMS) meets or exceeds the requirements of ISO 27001.

SOC II

commercetools meets SOC II standards, demonstrating our commitment to a secure, reliable and compliant service environment. A SOC II (System and Organization Controls) report addresses relevant controls for operational compliance, based on AICPA's Trust Services Criteria (TSC). Verified by independent auditors, our compliance with this renowned US standard highlights our dedication to protecting client information and privacy within our cloud-native infrastructure. Our continuous monitoring and robust control measures ensure uninterrupted availability, processing integrity and confidentiality.

TISAX

For commercetools, the TISAX assessment was conducted by TUEV SUED on Jan 27, 2025 for the scope items
“Data Protection according to EU-GDPR Art. 28 (“Processor”)”
“High Availability”
“Confidential”with assessment level AL2.
The result is available to authorized participants via the ENX portal

GDPR

We are GDPR-compliant, verified by external audits. The General Data Protection Regulation (GDPR) aims to strengthen personal data protection in Europe and affects the way we all do business. Compliance with GDPR is a top priority for commercetools and our customers.

HIPAA Compliant

commercetools implements all the necessary safeguards as a Business Associate to allow organizations that are Covered Entities to process protected health information (PHI) through the composable commerce platform. Our HIPAA compliance is affirmed by third-party security risk assessments, adoption of industry standards and established frameworks, direct alignment with the guidance set by the US Department of Health & Human Services, technical, administrative and physical controls, as well as continuous internal training.

commercetools is committed to powering secure and exceptional commerce and patient experiences for all types of healthcare and life sciences customers.

HDS (Hébergeur de Données de Santé)

As an IT-managed service provider, commercetools holds the HDS certification for the scope of personal health data management, which is a requirement by the French Public Health Code for handling personal health information (Hébergeur de Données de Santé). This certification underscores our commitment to securely managing health data and affirms our meticulous approach to data protection.

Cyber Essentials

commercetools complies with the requirements of the Cyber Essentials Scheme. The scheme, backed by the UK Government, is intended to help protect organizations of all sizes against a wide range of the most common cyber attacks.

About commercetools

commercetools is the leading enterprise commerce platform built to power innovation and versatility for the world's leading brands. Our composable, cloud-native technology provides the flexibility to design tailored, scalable commerce experiences across any channel, at any scale — whether in stores, on social media, through connected devices, or in augmented reality. By removing the constraints of legacy systems, commercetools enables companies to innovate freely, personalize at scale, and quickly launch new channels to meet the evolving demands of their customers.

As trusted partners to brands like Audi, Danone, Eurail, NBCUniversal, and Sephora, commercetools helps its customers set the pace of innovation, deliver exceptional experiences, and achieve sustainable growth. With commercetools, businesses don't just adapt to change — they lead it.

More information at commercetools.com.