ONTIC

Information Security and Data Privacy Overview

How Ontic ensures your information stays secure, private, and compliant

Table of Contents

Security and privacy you can depend on

Global enterprises trust us for our unwavering commitment to security, reliability, and data protection. Our platform and products are designed with security and privacy at the forefront, and we adhere to rigorous standards across jurisdictions to maintain comprehensive compliance and protect your data.

Our promise to you

At Ontic, trust is the foundation of everything we do. We understand that security professionals rely on us to safeguard their most sensitive data, and we take that responsibility seriously.

Protect your data: We recognize your information as your most valuable asset and are dedicated to safeguarding its confidentiality, integrity, and availability. Our platform employs robust, industry-leading security measures to prevent unauthorized access, modification, or deletion.

Privacy as a fundamental principle: We view data privacy as far more than a regulatory obligation; it is a foundational value that informs every aspect of our platform. From the earliest design stages, we employ privacy-by-design principles and rigorously align with leading global standards to ensure robust protection for all data.

Commitment to transparency: We believe you have the right to understand precisely how your data is handled. That's why we openly communicate our security measures, data usage policies, and compliance practices — ensuring you can trust our platform to protect your information.

Maintain resilience and reliability: Your business depends on uninterrupted access to critical information. We build our systems for high availability and resilience, utilizing availability zones, ensuring you have the tools you need when you need them.

Continuously evolve and improve: The security landscape is always changing, and so are we. We proactively enhance our security posture, update our policies, and invest in the latest technologies to keep your data safe.

The experts behind our commitment

Security, privacy, and compliance require more than just policies and technology — they require people who are dedicated to upholding them. At Ontic, we have a team of experts who work every day to ensure your data is protected and our security standards remain best-in-class.

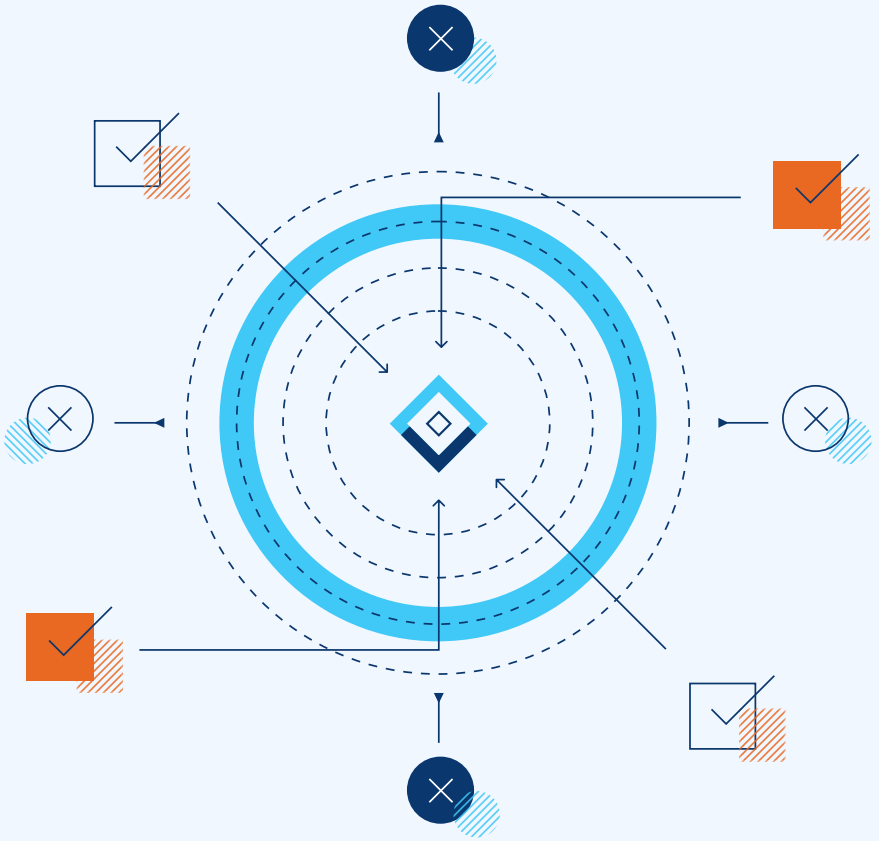
- **Chief Legal Officer:** Ensuring compliance with global privacy regulations and legal standards.
- **Information Security Officer:** Leading our security strategy and safeguarding our systems.
- **Data Protection Officer:** Overseeing data handling, safeguarding personal data, and ensuring compliance with privacy regulations.
- **Cybersecurity Analysts:** Monitoring, detecting, and preventing security threats.
- **Security Compliance Analysts:** Maintaining our security certifications, and adherence to security frameworks and best practices.

This dedicated team operates globally, providing around-the-clock vigilance to keep your data safe.

Robust data privacy controls that empower clients

Ontic's data privacy practices align with recognized frameworks, giving clients granular authority over data ingestion, storage, and access within our platform. We design our services with privacy by design and default, supporting least-privileged and role-based access models that extend robust control to our clients.

- Clients select which data sources to connect, maintaining full visibility into where, when, and why each source is used. This ensures data minimization and transparent data flows.
- Client administrators retain exclusive oversight of data and processes, including fine-grained permissions that dictate who can access specific information and what data is permitted to remain in the platform.
- Comprehensive audit trails document user and system actions within Ontic, granting detailed oversight that surpasses standard security operations.
- All client data is securely and permanently deleted 30 days after contract termination.
- Ontic operates as a "data processor" or "service provider," adhering to all applicable data protection laws. You can review our commitments in our Data Processing Addendum.
- Neither Ontic nor its third-party data providers hold a direct relationship with data subjects. However, in line with legal requirements, we provide mechanisms for data subjects to exercise their privacy rights, as outlined in our Privacy Policy.

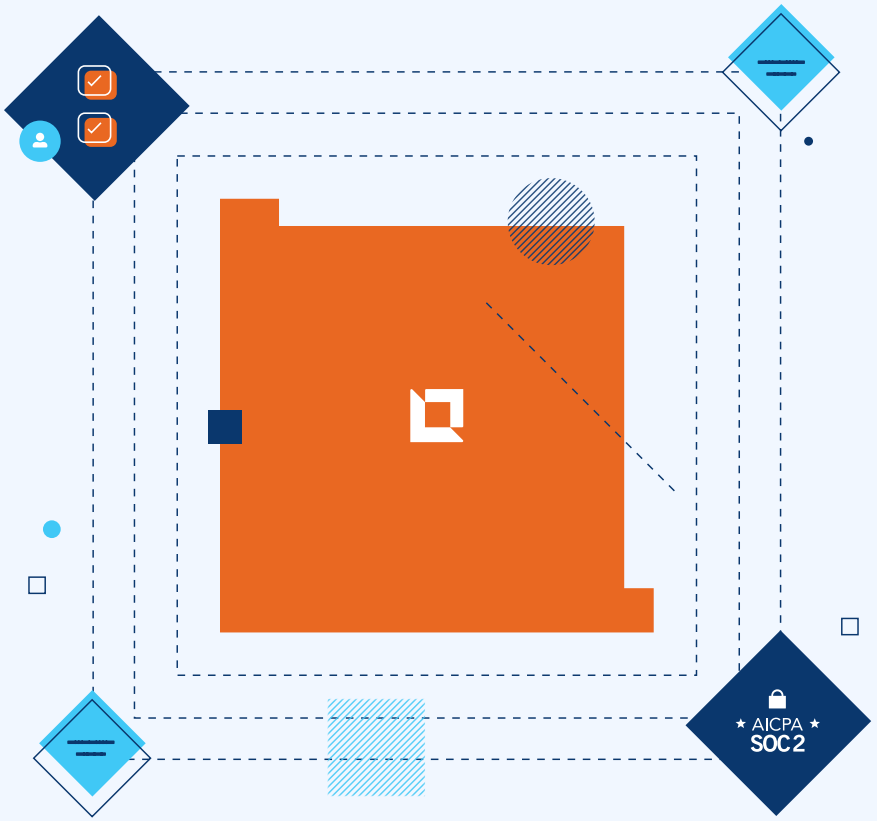


Security built to support global enterprises

Our platform and related products are designed from the ground up to provide robust data protection and application security. We work with the largest organizations in the world with demanding security requirements. We employ data security best practices, including:

- Each client has a dedicated database in the cloud accessible only to its designated users.
- All data accessed or stored in the Ontic Platform is encrypted both in transit and at rest.
- We undergo a SOC 2 audit every year and make a summary of that report available to clients.
- Cybervadis has assessed Ontic as “mature” and awarded us a Gold Medal.
- Ontic is CSA Star Level One Certified.
- All Ontic employees undergo background checks and are required to complete annual Data Security and Data Privacy Awareness Training.

Interested in some more detail, like what encryption levels we use? Visit our Security Details page.



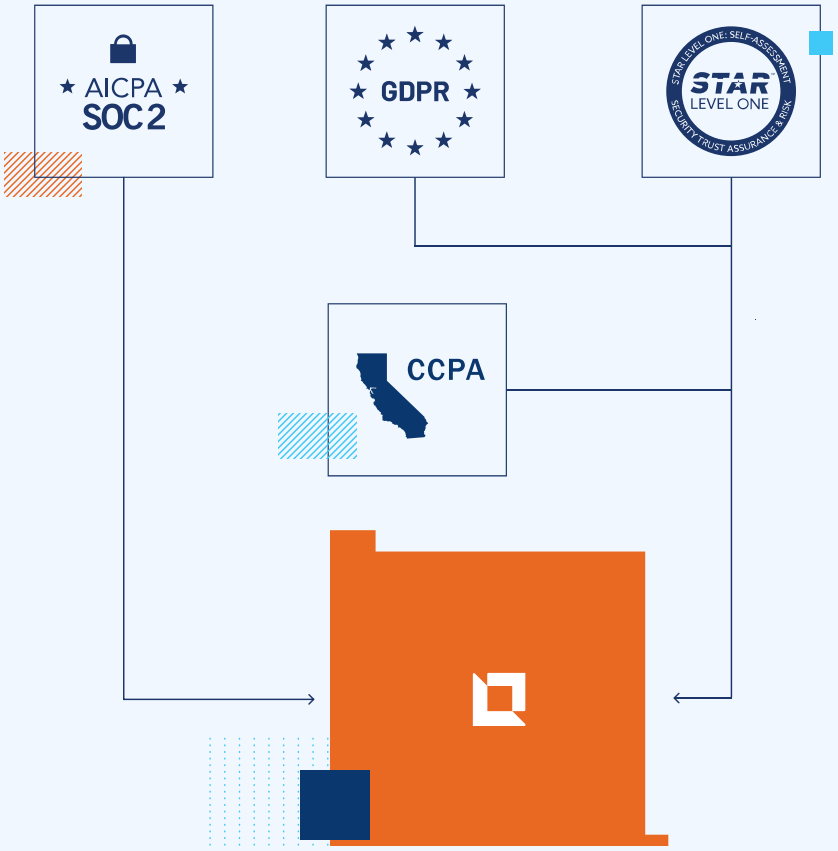
Regulatory compliance backed by industry certifications and accreditations

Ontic establishes a new benchmark by providing more than just adherence to critical regulations — delivering robust governance and in-depth audit capabilities. With Ontic at the core of security operations, organizations elevate beyond the manual processes and disparate tools (e.g., notebooks, emails, spreadsheets) that often impede visibility and accountability.

It's what we call Connected Intelligence.

Ontic supports organizations in adapting to the rapidly evolving data privacy and cybersecurity landscape by:

- Ensuring compliance with all relevant laws and regulations related to the collection, processing, and storage of personally identifiable information and other sensitive data.
- Proactively monitoring national and local legislation, restricting access to services or data when necessary to comply with state-specific laws and regulations.



Frequently asked questions

Where is client data stored?

As most of our clients are headquartered or based in the U.S., we store data solely in the U.S. by default. Not located in the U.S.? We work with our non-U.S. clients to store their data in a mutually agreeable alternative jurisdiction. See our Privacy Policy for more information.

How does Ontic ensure that the information security and privacy controls are operating effectively?

We engage internationally known independent firms to conduct information security and privacy audits and penetration tests, and independent researchers continually assess our systems. We ensure swift remediation of any risks associated with data confidentiality, integrity, availability, and privacy identified.

Do you provide detailed audit reports to your clients?

We perform an annual SOC 2 Type II attestation to prove that our system is designed to keep our clients' sensitive data safe and secure based on the Trust Service Principles of Security, Availability, and Confidentiality. A summary of the attestation report is provided to clients on request.

Which international information security and privacy standards do you comply with?

Our Information Security Management System (ISMS) and Privacy Information Management System (PIMS) are compliant with ISO/IEC 27001 and ISO/IEC 27701.

Do you perform independent penetration testing of your systems?

We perform regular penetration testing, a form of "ethical hacking" performed by third-party security experts, attempting to identify and exploit any vulnerabilities. The penetration test summary reports are provided to clients on request. We also have a bounty disclosure program. This allows the ethical hacking community to find and report vulnerabilities in our systems.

What privacy controls does Ontic have in place?

Ontic implements comprehensive privacy controls grounded in privacy-by-design principles to safeguard sensitive data across its lifecycle. Our practices align with leading global standards and incorporate rigorous access management, data minimization, and transparent compliance processes to consistently protect user privacy.

How does Ontic keep your data safe?

Our Information Security Management System (ISMS) and Personal Information Management System (PIMS) provide a systematic and structured approach to ensure that we manage the security and privacy of all of our client's data.

Does Ontic have a 24/7 cybersecurity operations center?

We partner with a managed service provider to provide 24×7×365 cybersecurity operations.

The cybersecurity operations team monitors, assesses, and prevents cyber threats against our systems, products, and services.

What security controls has Ontic implemented?

We implement administrative, technical, and physical security controls identified via the risk management framework. We carefully select the third-party service providers who support us with processing personal data and implement contractual clauses that hold them accountable to the same data protection and privacy standards we meet ourselves.

Administrative controls

- **Policies and procedures:** Aligned with recognized standards (e.g., ISO 27001, NIST 800-53)
- **Security awareness training:** Mandatory, ongoing education for all personnel
- **Risk management:** Regular evaluations of security posture, risk assessments, and ongoing risk management
- **Incident response and continuity plans:** Formalized protocols for incident handling, disaster recovery, and business continuity and annual IR and BC/DR testing.
- **Supplier risk management and due diligence:** Documented processes to evaluate, approve, and monitor suppliers and sub-processors

Technical controls

- **Encryption:** Data is encrypted at rest using AES 256 and in transit using TLS 1.2 or higher.
- **Network protection:** Web Application Firewall (WAF), network firewalls, virtual local area networks (VLAN), access control lists (ACLs), and intrusion detection systems are used to protect against internet-borne threats.
- **Authentication & access controls:** Multi-factor authentication (MFA) and least-privilege principles for system and data access
- **Logging, monitoring & alerting:** All security logs are forwarded to a Security Incident and Event Management (SIEM) system with 24/7 third-party and internal monitoring and log review.
- **Vulnerability management:** Regular scanning, penetration testing, patching, and remediation across the technology stack
- **Resilient cloud architecture:** High-availability infrastructure with redundancy across multiple availability zones (AZs), secure backups and regular backup/restore and disaster recovering testing.
- **Endpoint security:** Mobile Device Management (MDM), Anvit-Virus (AV), and Incident Detection & Response (IDR) are used to secure all physical and virtual endpoints.

Physical controls

- **Data center security:** Cloud service providers' facilities incorporate restricted access, security guards, environmental controls, and 24/7 surveillance
- **Office access controls:** Badge/key fob systems, visitor management, video surveillance, and facility assessments
- **Secure document and hardware disposal:** Strict protocols for the destruction of sensitive paperwork and decommissioned equipment
- **Asset management:** Tracking of asset lifecycles and secure storage for critical devices

ONTIC

Have more questions about Ontic's approach to security, privacy, and compliance?

Contact Us