White Paper

Applying a Zero Trust Approach to Security:

How Customer Data is Protected in Reltio Connected Data Platform

September 2021

Data loss. It's every organization's nightmare, especially when sensitive customer data has been breached by cybercriminals. The risk of a damaged reputation, decreased customer confidence, losing business to competitors, and hefty regulatory compliance fines keeps business and IT management up all night with the nagging question: How secure is our data, both on premise and in the cloud?

Cloud security is a responsibility that Reltio takes seriously. Security underlies everything we do, and we have structured our company to ensure best-in-class security practices as well as industry-leading performance. This white paper outlines Reltio's approach to security, our practices and controls, and our company's regulatory compliance and certifications. The bottom line: customer data in Reltio Connected Data Platform, stored in the public cloud, may well be safer than the data in your own data center.

Safeguarding the Data of Our Customers

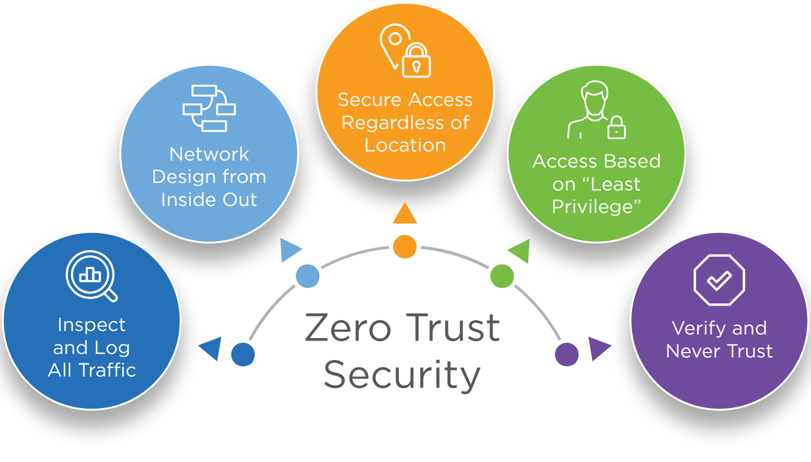
In 2019, there were 1,473 data breaches reported in the U.S. That represents an increase of 17 percent over 2018, according to the End-of-Year Data Breach Report for 2019 from the Identity Resource Center, a nationally recognized non-profit organization established to support victims of identity crime. The report found that the highest incidents of data breaches and the highest number of records exposed were due to cyberhacking. Unauthorized access to network systems was the second most common threat to data loss.

It has been proven many times over that cloud computing reduces the burden of managing the application infrastructure and operations, while still maintaining control over customer data. Still, Reltio understands that protection against data loss is the primary concern of all organizations. That's why we designed Reltio Connected Data Platform, a responsive data platform built on a cloud-native, big data architecture—and with security baked into it.

Reltio Connected Data Platform brings together data from internal, external, and third-party sources to create a single source of truth for all data domains. As this data may contain personally identifiable information (PII), sensitive PII, or HIPAA data, we put strong security measures in place to manage it with extreme care. Reltio is cloud native, and we use the best security systems from the leading public cloud providers (Amazon Web Services and Google Cloud Platform), as well as our own security practices, to deliver our services to clients.

Reltio's Zero Trust Approach

Reltio follows the Zero Trust security model. Our approach is centered on the belief that organizations should not automatically trust anything inside or outside their perimeters trying to connect to their IT systems. Instead, they must verify everything before granting access. Reltio bases its Zero Trust best practices on recommended security standards that support Amazon Web Services (AWS) and AWS Well Architected. Early on, we incorporated those standards into our Zero Trust model.


Inspect and Log All Traffic
Network Design from Inside Out
Secure Access Regardless of Location
Access Based on "Least Privilege"
Verify and Never Trust
Zero Trust Security

Tenets of the Zero Trust Model

Network Design from Inside Out

Reltio's Zero Trust approach takes a defensive view of the security threat landscape. This protects against common threats to our applications and our internal network, in part by minimizing vectors of attack. Another facet of Zero Trust is how we infuse security standards into our application design process from the earliest stages.

Reltio extends Zero Trust to vendor selection. We follow two main principles for vetting our vendors. First, the vendor's solution or service must meet our security requirements in line with Zero Trust. Second—and equally important—we select leading organizations whose names we recognize and trust, even if it requires a larger investment in their services. However, we are also open to working with lesser-known vendors if they have new technology that our team has vetted and that no else offers. Satisfying our security requirements and giving our customers confidence that we have selected vendors they can trust drive our vendor selection. The confidence factor is similarly important when choosing independent third-party auditors.

Beyond Zero Trust, Reltio applies the principle of Zero Trust verification. Reltio expects vulnerabilities, weaknesses, and misconfigurations to emerge—and doing nothing results in an erosion of our security model. Therefore, we verify the security of all operating environments on a continual basis by conducting offensive threat modeling using technology, automation, and human validation. This same approach is taken within Kubernetes environments where continual assessments occur in near real-time to proactively gain the perspective of an adversarial attacker and take actions quickly.

Reltio's Information Security Team: Who They Are and What They Do

Reltio has a dedicated information security team that reports to the CISO. This team is responsible for the development and maintenance of the company's security, availability, and confidentiality policies, performing routine updates to those policies as technology, industry, regulatory, and business requirements change. The information security team also defines and enforces security standards, policies, and processes. The information security team monitors the Reltio platform environment and works with development operations and product management to address security requirements arising from annual security reviews, reported incidents, and updates to security standards.

Reltio information security is highly focused on securing our customers' data and has direct control over access to the Reltio network and systems, limiting monitoring and access. To defend against threats from both outside and inside our professionals maintain and monitor security information and event management alerts (SIEM), intrusion detection systems (IDS), vulnerability scanning, enterprise mobility management (EMM), data leakage protection (DLP) as well as use identity management (IM) tools. The team conducts regular audits and works closely with Reltio's developers to ensure compliance with our own security standards as well as the top 10 standards of the Open Web Application Security Project (OWASP). Reltio scans its open source libraries for vulnerabilities too. It also monitors vendors and other third parties to ensure compliance with all other Reltio security standards.

Reltio information security is highly focused on securing customer data and has direct control over access to the Reltio network and systems.

We augment our security by partnering with a skilled managed security service provider (MSSP) to increase the scope of monitoring. Partnering with an MSSP helps us stay up to date with the most recent developments in the security space and provides another perspective on security approaches. In addition, Reltio monitors alerts from the United States Computer Emergency Readiness Team (US-CERT), news media, and online security resources for possible security issues affecting the Reltio architectural stack.

Customer-Managed Key (CMK) with Reltio Shield

With Reltio Connected Data Platform, you can generate your own keys (CMK) according to your organization's specific security policies and practices. Keys can be generated on demand with background re-encryption of data using the new keys or automatically, according to a schedule.

New keys are automatically distributed via secure automated processes without any manual involvement or handling by Reltio and with no service downtime.

Benefits include:

- Fine-grained access control
- Policy-driven, foolproof security management
- Self-service security through scheduled or on-demand generation of keys
- Zero down-time from automated keys distribution

Platform Security Overview

Reltio Connected Data Platform is delivered with enterprise-class security and granular, role-based visibility to records and attributes enabled. Every time a record is viewed, updated, merged, or used, it is tracked within Reltio's audit log framework. Patterns of usage can then be analyzed using data from the audit logs.

We perform regular validation (as required by FDA 21 CFR- 11, generally applicable to FDA-regulated industries) and penetration tests to ensure security and compliance. Reltio Connected Data Platform supports full security, Single Sign-On (SSO), as well as role-based and attribute visibility. We support integration with SSO and other identity management tools using SAML 2.0 or OAuth 2.0. This makes it easier for our customers to manage password policies and role-based security controls by linking their systems to Reltio's identity management applications via SAML.

A ticket and written authorization from the customer are always required when Reltio staff need to access customer cloud accounts for administrative or maintenance tasks. Access can be granted by Reltio support, a support manager, or information security. Staff members are added to a group based on their role and are narrowly granted access to only the tenant where work is required.

Customers typically manage access using their own SSO and business requirements for system access. Some clients integrate the onboarding process with security, which automates the creation of user accounts and assigns them to groups. Customers can create their own roles, groups, and users via the Reltio console, as well using SSO and SAML to control access. For everyone's security, customers should regularly patch their SSO versions to keep them up to date.

Reltio follows a three-tiered approach to data confidentiality, integrity, and accessibility. This ensures the highest level of data security and compliance in the cloud, all by using industry standards.

Three Tiers to Cloud Security

Confidentiality

- Encrypt at rest and in transit
- Privileged access MFA
- Least privilege
- Key management
- Host intrusion detection
- Security incident and event management
- Reltio security operating procedures
- Managed security service provider

Integrity

- Data replication across zones
- Penetration testing / bug bounty
- Business continuity and disaster Recovery
- Chef, Ansible, Terraform for server definition
- Tenant backup
- Security poster management
- Next gen WAF
- Enterprise mobility management

Availability

- Redundantly shared and replicated data
- Shared-nothing architecture
- Three-data center active-active deployment topology
- Minimum of 99.95% uptime and availability
- Resilient to a disaster scenario

Confidentiality

Reltio has controls governing confidentiality, including encryption of all data at rest and in transit over the internet. We also use intrusion detection, file monitoring, and a SIEM to log network and access activity. Meanwhile, our security engineers review the data, and additional reviews are provided by our MSSP.

Integrity

Reltio maintains data integrity by replicating application data across zones. By running our server on multiple zones, additional resilience is added to our applications. Moreover, access to our established firewall controls and public/private subnets is controlled via NAT Gateways, thereby creating a virtual DMZ. Server standards are enforced on virtual machine images using Chef, Ansible, and Terraform.

Availability

High availability, redundancy, backup, and recovery is built into Reltio Connected Data Platform. All data held in the Reltio platform is redundantly shared and replicated across a set of servers that operate on a shared-nothing architecture. This allows the Reltio platform to continue to run properly even if nodes on the overall cluster become unresponsive.

To ensure high availability, we deploy the necessary hardware redundantly in a three-data center “active-active” deployment topology. This enables our team to deliver service-level agreements (SLAs) with a minimum of 99.95% uptime and availability for mission-critical use of our multi-domain master data. Additionally, this cross-datacenter deployment makes the Reltio platform more resilient to a disaster scenario.

Security at Each Layer

Reltio’s approach to layered security is to combine defense and depth using a series of application layer tools that utilize the hosting vendor’s security offering. This provides another layer of security for both the hosting environment and the customer’s data. Key ingredients include:

Server Network
Reltio uses a well-regarded network penetration testing firm and test cases to detect OWASP top ten vulnerabilities. We run a next-gen web application firewall (WAF) to prevent these issues from arising in the first place and run source code vulnerability scanning tools on our software to look for any potential source code quality issues. We use hosting vendor capabilities for firewall rules, and our hosts have IDS built into the image.

Hosting Vendor: Amazon Web Services
Reltio validates that AWS security controls are acceptable by reviewing their respective SOC 2 Type 2 reports annually. Among the additional security controls we use to keep customer data secure are physical controls, infrastructure security, AWS Shield, CloudTrail, CloudWatch, AWS IAM, and AWS Trusted Advisor.

Hosting Vendor: Google Cloud Platform
Similarly, Reltio reviews GCP SOC 2 Type 2 reports and leverages additional security controls provided by Google. These include physical controls, infrastructure security, application layer transport security, Cloud IAM, Encryption at Rest, and Stackdriver logging.

Container Security
Reltio employs a model known as the “4 Cs,” which stands for cloud, cluster, container, and code. Utilizing a microservices architecture, we use Kubernetes for multi-cloud deployments in Amazon Elastic Kubernetes Service (Amazon EKS) and Google Kubernetes Engine (GKE) to support scalability, automation, and security.

Certifications and Compliance

To complete our security picture, customers can rest assured that Reltio has achieved the highest levels of certification and compliance, including:

HITRUST Common Security Framework
Reltio is certified for HITRUST Common Security Framework (CSF). HITRUST CSF unifies recognized standards and regulatory requirements from NIST, HIPAA/HITECH, ISO 27001, PCI DSS, FTC, and COBIT. Customers subject to an NDA with Reltio may obtain a copy of this report upon written request.

Service Organization Control Reports
Reltio is certified for SOC 1 type II and SOC 2 type II compliance for the Reltio Connected Data Platform. SOC 1 focuses on financial reporting controls as they relate to security of a system. The SOC 2 report focuses on a business's non-financial reporting controls, as they relate to security of a system. Customers subject to an NDA with Reltio may obtain a copy of these reports upon written request.

Privacy Certification
Reltio also maintains compliance with the myriad privacy rules across a number of jurisdictions. Reltio has obtained third-party certifications for EU and Swiss Privacy Shield as well as APEC certification. The Reltio Connected Data Platform supports both GDPR and CCPA, and Reltio maintains a privacy policy that complies with these laws. For more information on how Reltio maintains data privacy for its customers, see the Reltio Privacy Policy.

HIPAA Environment
Reltio maintains an environment on the platform configured to help customers meet HIPAA requirements. The HIPAA environment uses HIPAA-compliant services from its hosting vendors and complies with HIPAA requirements. Reltio maintains a Business Associate Agreement (BAA) with its hosting vendors. The platform encrypts customer data at rest and in-transit on the public internet, and it logs all access to the applications and supporting servers and network. Reltio maintains log data in its SIEM for one year.

Third-Party Security and Privacy Assessment
Reltio assesses third-party vendors prior to using vendor services as part of the Reltio Cloud Platform or for internal Reltio use. Reltio will assess the risk of the third party engagement and may review the vendor's SOC 2 type II report or the vendor's responses to a Reltio security assessment questionnaire. Reltio includes security and privacy obligations in its contractual agreements with such third-party vendors that are aligned with contractual obligations of Reltio's customers as well as Reltio's own security standards. Reltio conducts a reassessment of third-party vendors annually.

Built-in Regulatory Compliance

Reltio Connected Data Platform has integrated support for compliance regulations that are continually evolving, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). To do this, the Reltio platform provides:

- **Built-in capabilities** to support GDPR and CCPA requirements include classification of PII attributes, as well as a preference and a consent model to track requests and approvals for access to data.

- **Omnichannel consent management** captures and reconciles different consent types, including those via relationships such as parental consent, with exceptions supported at the country, brand, and product levels.

- **Integrated workflows** manage consumer requests for data changes and deletions with complete traceability.

- **Data erasure** supports the right to be forgotten, which enables purging profiles and historical activities while logging requests for audit purposes. Events and queues support cascade actions to be applied to the originating downstream sources.

Conclusion

Data breaches continue to be a grim reality in today's digital age, and data security remains critically important for any enterprise application and across all industries, regardless of the sensitivity of their data. With more data moving to the cloud, cloud data security must be as good as, or better than, on-premise based systems—whether it resides on public, private, or hybrid clouds.

Reltio recognizes the importance of cloud security and implements modern best practices and safeguards to secure the data of its clients. Rooted in our proven Zero Trust approach to data security, we will continue to invest in the resources, people, technology, and business partners that our customers can trust to protect their data from loss or cybertheft.

ABOUT RELTIO

Innovative Global 2000 companies trust Reltio to manage their mission-critical data for digital transformation. Reltio Connected Data Platform provides unified, reliable, and real-time data to fuel positive business outcomes, drive excellent customer experiences, and improve operational efficiency while simplifying management of risk and compliance.

The Reltio Connected Data Platform is a proven multi-tenant, multi-domain MDM platform that masters all data types in real-time and at-scale. To learn more, visit www.reltio.com.

Reltio

Let's Talk

US	+1 (855)	360-3282
UK	+44 (800)	368-7643

Start for Free
Reltio.com/Identity360

Connect with Us
@Reltio
facebook.com/ReltioHub
in linkedin.com/company/reltio-inc