Reltio

White Paper

Applying a Zero Trust Approach to Security:

How Customer Data is Protected in Reltio Connected Customer 360™

In Brief

Data loss. It's every organization's nightmare, especially when sensitive customer data has been breached by cyber criminals. 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, as well as our company's regulatory compliance and certifications. The bottom line: customer data in Reltio Connected Customer 360 that is stored in the public cloud may well be safer than the data in your own data center.

"Reltio is cloud native and we use the best security systems from the leading public cloud providers, as well as our own security practices, to deliver our services to clients."

Introduction: Safeguarding the Security of Our Clients

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 cyber hacking. Unauthorized access to network systems was the second most common threat to data loss.

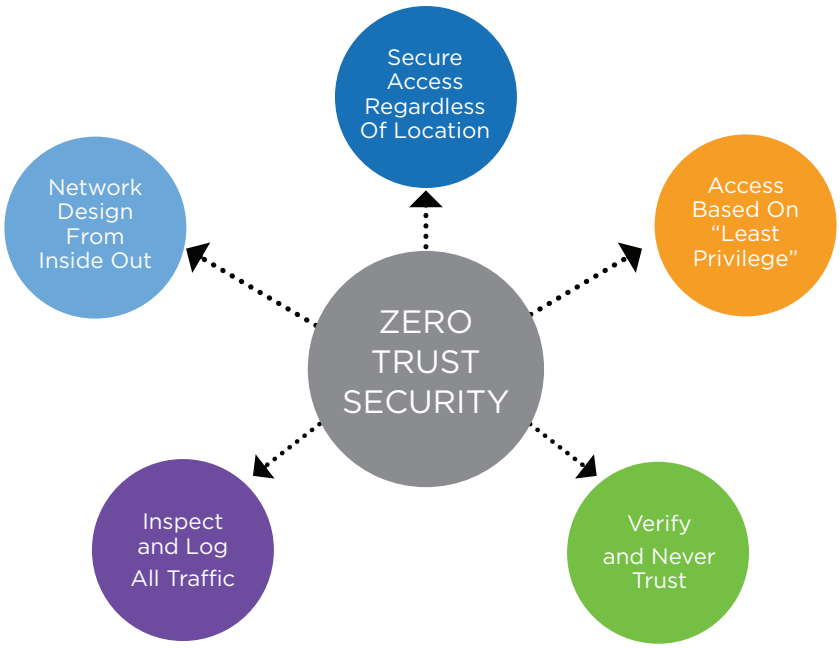
It has been proven many times over that cloud computing reduces the burden of managing the application infrastructure and operations, while still maintaining control over customer data. Still, Reltio understands that protection against data loss is the primary concern of all organizations. That's why we designed Reltio Connected Customer 360™, a responsive data platform built on a cloud-native, big data architecture—and with security baked into it.

Reltio Connected Customer 360 brings together data from internal, external and third-party sources to create a single customer view. 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 and AWS Well Architected. Early on, we incorporated those standards into the Zero Trust model.

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 look for leading organizations whose names we recognize and trust even if larger investment in their services are required. 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 third-party auditors, such as trusted names like KPMG.

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 makes significant investments to attract and retain the best talent for our Information Security team and to equip them with the tools and resources needed to excel. Compared to other cloud-based organizations of comparable size, our sizable security team, led by a Chief Information Security Officer (CISO) and a dedicated Global Head of Compliance, ensures that both customers' data and our own Reltio SaaS platform meet the highest security standards.

Reltio Information Security is highly focused on securing customer data and has direct control over access to the Reltio network and systems, limiting monitoring and access. To defend against threats—primarily external although insider threats are monitored as well—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.

Platform Security Overview

Reltio Connected Customer 360 ships 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) and penetrations tests to ensure security and compliance. Reltio Connected Customer 360 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.

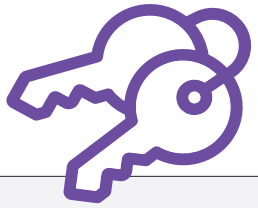
A ticket and written authorization from the customer are always required when Reltio staff need to access customer cloud accounts for administrative or maintenance tasks. Access can be granted by Reltio Support, a support manager or Information Security. Staff members are added to a group based on their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

Customers typically manage access using their own SSO and training requirements for system access. Some clients integrate the onboarding process with security, which automates the

BRING YOUR OWN KEY

Reltio offers a key management option that clients can use to generate their own keys in accordance with their 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, fool-proof security management
- Self-service security through scheduled or on-demand generation of keys
- Zero down-time from automated keys distribution



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, customer SSO versions should be patched and always kept 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

1. **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 with additional reviews provided by our MSSP.

2. **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.

3. **Availability.** High availability, redundancy, backup and recovery is built into Reltio Connected Customer 360. 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 percent 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 II 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 II reports and supports 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 Code1. 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.

1 Kubernetes, Overview of Cloud Native 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 CSF Certified.** Although geared to the healthcare industry, Reltio prefers HITRUST over similar security certifications as it encompasses a blend of requirements across many different standards. HITRUST includes all ISO 27001 standards, many NIST and COBIT 5 standards, Health Insurance Portability and Accountability Act (HIPAA) requirements, privacy requirements, as well as other state and federal regulations governing information security. Reltio has performed a risk assessment against HIPAA requirements which governs the confidentiality and privacy of protected health information (PHI). As a result of the assessment, we enable customers to comply with HIPAA requirements.

- **Other Certifications.** These include SOC 1 Type 2, SOC 2 Type 2, EU and Swiss Privacy Shield, APEC Certified and HIPAA Compliant. Reltio uses PCAOB registered third parties for its SOC and HIPAA reports (KPMG) and privacy experts for EU and Swiss Privacy Shield and APEC (TrustArc). Meanwhile, Reltio is both SOC1 and SOC2 certified in response to the financial reporting needs of our customers. We have been SOC certified since 2016 and continue to build on our experience.

Built-in Regulatory Compliance

Reltio Connected Customer 360 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). Other compliance standards we support include:

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

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

- **Integrated workflows** that manage consumer requests for data discovery. This includes changes and deletions with complete governance and traceability.

- **Data Erasure**. This supports "Right to Be Forgotten" purging profiles and historical activities while logging requests for audit purposes. Events and queues support cascade actions to be applied to originating downstream sources.

Reltio meets the EU Data Protection Directive by complying with EU and Swiss Privacy Shield regulations, as well as others. Contact us to request additional technical information on the full scope of our compliance and security activities.

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 cyber theft.