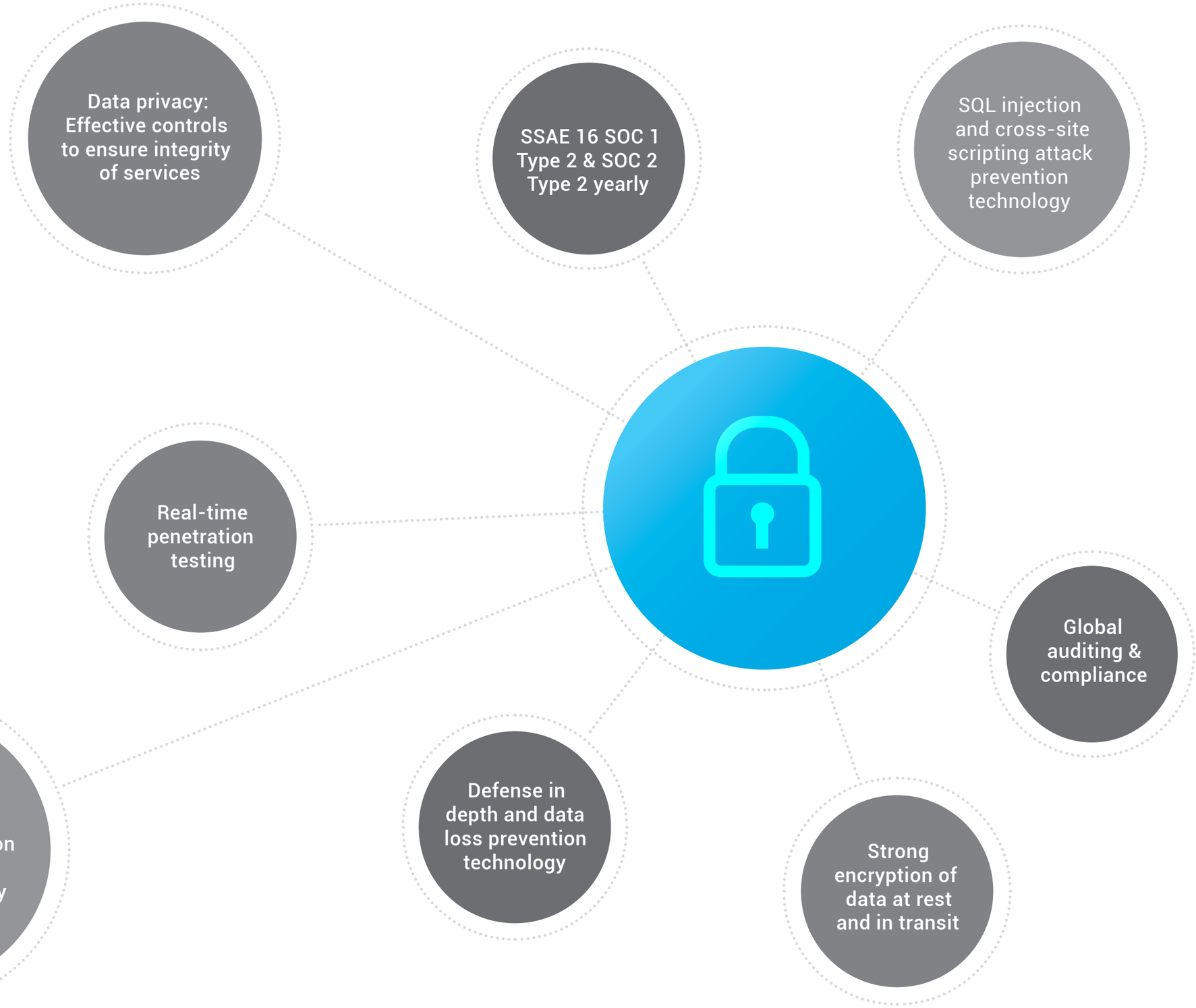
Keep your data
and applications

PRIVATE, SECURE, & COMPLIANT

in the cloud.

CallidusCloud®

You have your own business to worry about. Since cloud is our business, CallidusCloud protects your data with more security measures than you could ever adopt. We ensure compliance with all data privacy and data security regulations, employ third party specialists to routinely test our environments, undergo extensive security audits, and support multiple levels of access controls and data handling procedures that maintain data integrity and prevent misuse. Some of the world's largest customers entrust CallidusCloud with their data.



What makes CallidusCloud security better?

CONTINUOUS TESTING
CallidusCloud routinely performs vulnerability assessments and penetration testing on its infrastructure and applications. CallidusCloud applications are scanned weekly against the Open Web Application Security Project (OWASP) top security flaws. Each quarter CallidusCloud employs third-party security experts to perform detailed vulnerability scans on different parts of the applications and manual penetration test yearly.

REGULAR, PUBLISHED AUDITS
CallidusCloud operates under SSAE 16 SOC 1 and SOC 2 certified controls framework, the second-generation data center audit standard that evaluates data center design and operational efficiency across multiple trust criteria. CallidusCloud completes the SSAE 16 SOC 1 and SOC 2 audit reports annually. We share the results of privacy and compliance audits with our customers upon request.

INTEGRATED COMPLIANCE FRAMEWORK
CallidusCloud has established strict procedures regarding all activities in our information processing environment. CallidusCloud has aligned itself with ISO 27001 for Information Security, US EU Safe Harbor / PIPEDA / UK ICO for Data Protection and Privacy, and ITIL for Service Delivery. Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence.

COMPLIANCE WITH IT SECURITY STANDARDS
CallidusCloud adheres to and complies with the following IT security standards: Authority to operate as a moderate risk Federal Information System by the Office of Personnel Management and Department of Homeland Security and EU Privacy Directive 95/46/EC for EU and non-EU customer data.

Partner with a TRUSTED cloud provider

Controlling who can — and who cannot — access your sensitive information is just as important as maintaining security at the physical and infrastructure layers. CallidusCloud has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to, all employees and contractors with access to CallidusCloud information assets. CallidusCloud uses a variety of methods to ensure that the right users have access to the right information, including:

SECURITY TRAINING
All new employees attend security awareness training, and the security team provides security awareness updates via email, blog posts, and through presentations during internal events.

BACKGROUND CHECKS
CallidusCloud performs background checks on all new employees in accordance with local laws. These checks are also required to be completed for contractors and cleaning crews. The background check includes criminal, education, and employment verification.

CONFIDENTIALITY AGREEMENTS
All new hires are screened through the hiring process and required to sign non-disclosure and confidentiality agreements.

We keep you PROTECTED

PHYSICAL SECURITY

CallidusCloud partners with localized world leaders in co-location hosting centers to provide environmentally controlled, secure facilities that use an integrated security management system. This includes electronic photo ID badging, cardholder access control, biometrics, recorded digital video surveillance, and alarm monitoring. All enterprise customers are hosted in data centers that are ANSI TIA/EIA-942 Tier III+ rated facilities. They provide continuous monitoring, 24-hour, year-round onsite security personnel, and intrusion detection alarm systems. In addition, the facilities include safeguards that:

1. **BLOCK ILLEGAL ENTRY** via biometric readers, and bulletproof walls,
2. **IMMEDIATELY ACT ON SECURITY BREACHES** through the use of silent alarms.
3. **AVOID DOWNTIME** with redundant power links to local utilities, backup batteries, and uninterruptible power supplies
4. **PROVIDE A SHIELD** against fire, natural disasters, and weather shifts with fire suppression systems; environment monitoring; and earthquake-safe designs
5. **PROVIDE ENHANCED BACKUP AND RESTORE** CallidusCloud runs full and incremental data backups daily or weekly and full archive logs backups daily, where applicable. Back up data is stored on an encrypted disk using AES 256-bit encryption. This data is available for rapid reimplementation and system restores if needed for any reason.

DATABASE SECURITY

Database environments used in cloud computing can vary significantly. CallidusCloud secures data while at rest, in transit, and in use, and implements strict measures for:

1. **ACCESS CONTROL** All access to information processing facilities and business processes are controlled according to business and security requirements.
2. **DATABASE AUDITS** Regular database audits allow CallidusCloud to maintain records demonstrating proof of origin.
3. **DATA ENCRYPTION** CallidusCloud solutions use a minimum of Advanced Encryption Standard (AES) 256-bit encryption to secure data at the block level of the storage systems.

CallidusCloud builds security into every layer of its solutions:

DATA CENTERS are physically protected from unauthorized access, damage, and interference.

DATABASE addresses heterogeneous data within the cloud.

APPLICATIONS are secured at the function, transaction, field, and data level.

MIDDLEWARE provides single sign-on and identity federation.

NETWORK AND COMMUNICATION security controls ensure complete confidentiality, integrity, and non-repudiation of data.

DEDICATED TEAM Our Security Team is on call 24/7 to respond to security alerts and events.

MIDDLEWARE SECURITY

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers. Therefore, it is important to understand the technologies the cloud provider uses to provision services and the implications they have on the security and privacy of the system throughout its lifecycle. CallidusCloud ensures that proper safeguards are in place to enforce authentication, authorization, and other identity- and access-management functions, including:

1. **MULTIFACTOR AUTHENTICATION**, which is required for administrators who manage the production environment
2. **SINGLE SIGN-ON AND IDENTITY FEDERATION**, which allows you to authenticate directly from your existing authorizing system, via Lightweight Directory Access Protocol (LDAP), tokens, or Security Assertion Markup Language (SAML 2.0)
3. **SAML 2.0 ASSERTION**, which allows you to authenticate users using your choice of identity provider and provides a standard mechanism to safely transmit the identity information to CallidusCloud
4. **SECURE SOCKET LAYER (SSL) TECHNOLOGY**, which protects application information accessed through a browser using server authentication and data encryption

APPLICATION SECURITY

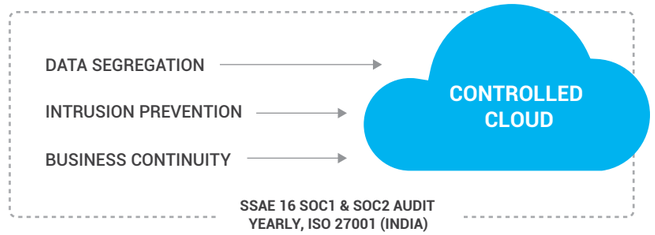
CallidusCloud applications employ extensive security measures to protect against the loss, misuse, and unauthorized alteration of data. CallidusCloud ensures security through continuous software testing to:

1. **PROTECT AGAINST IMPROPER LOGINS** by requiring user logins each time the application is opened, by using automatic logouts after thirty minutes and account locks after multiple failed logins.
2. **PROVIDE BEST PRACTICE SECURITY** at all levels (function, transaction, field, and data) by using role-based permissions (RBP).
3. **REPEL ATTACKS** in application-level firewalls to prevent SQL injection and cross-site scripting attacks and test applications using OWASP.

NETWORK SECURITY

CallidusCloud uses industry-leading routers, switches, and load balancers that are configured to provide secure, highly available access. Then, we ensure that every component of the IT network – from the point of entry to the place where information is stored – is meticulously configured, deployed, maintained, and continually tested for optimal performance. Finally, CallidusCloud takes extra steps to:

1. **REINFORCE SECURITY** with redundant connections to multiple Tier 1 Internet service providers (ISPs) for highly available network access. All network equipment is redundant, providing seamless failover between devices.
2. **PROTECT NETWORK AND APPLICATIONS** through Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), network vulnerability scanning, and third-Party penetration tests.
3. **MITIGATE AGAINST DENIAL OF SERVICE ATTACKS** by using a major third-party provider to deliver a scalable, fault-tolerant global Domain Name System (DNS) and Service Level Agreements (SLAs) with our Internet service providers (ISPs) for DoS response and mitigation support.



About CallidusCloud

Callidus Software Inc. (NASDAQ: CALD), doing business as CallidusCloud®, is the global leader in cloud-based sales, marketing, learning, and customer experience solutions. CallidusCloud enables organizations to accelerate and maximize their lead to money process with a complete suite of solutions that identify the right leads, ensure proper territory and quota distribution, enable sales forces, automate configure price quote, and streamline sales compensation — driving bigger deals, faster. More than 4,700 leading organizations, across all industries, rely on CallidusCloud to optimize the lead to money process to close more deals for more money in record time.

4140 Dublin Blvd, Suite 400 Dublin, CA 94568 / www.calliduscloud.com / 1 866 812 5244