WHITE PAPER

Amber Road
Client Data and Network Security
Amber Road provides a cloud-based Software-as-a-Service (SaaS) platform that automates and streamlines global trade. By helping organizations to comply with country-specific trade regulations, as well as plan, execute and track global shipments, Amber Road enables goods to flow unimpeded across international borders in the most efficient, compliant and profitable way.

With more than 20 years of experience in delivering SaaS solutions, we consider security a core guiding principle for all aspects of our business. Amber Road’s solutions are specifically designed for enterprises and, as such, comply with the highest security standards.

While there are no truly bulletproof solutions, we continually review industry security developments and do our best to implement and follow best practices to keep service secure.
SECURITY ORGANIZATION AND PROGRAM

We strive to implement security processes and practices across all business units. To help with that, we have a dedicated team of professionals that manages Amber Road's security. Our practices are based on industry-leading standards, on which we are audited twice per year under the SOC framework.

The SOC framework audits policies and procedures, asset management, access management, physical security, people security, product security, cloud and network infrastructure security, third-party security, vulnerability management, as well as security monitoring and incident response.

Our information security policies and standards are approved by management and available to all Amber Road employees.
The people behind Amber Road products are an essential part in protecting the service, as the human factor has a key role in, and influence on, our organizational level of security. We put stringent controls in place for employees.

**Background Checks**
The screening process is based on personal interviews with recruitment/HR manager and a prospective employee’s direct manager. Where applicable, background checks include criminal record check, credit check, education check, references and identity. Additional checks may be performed in accordance with local law.

**Security Training**
New employees go through an extensive on-boarding process that include communication of security guidelines, expectations and code of conduct. In addition, all Amber Road employees undergo annual security awareness training.

**Continuous Communication**
The Amber Road security team provides continuous communication on emerging threats, performs phishing awareness campaigns and communicates with management regularly.
The Amber Road security development lifecycle (SDLC) standard helps ensure the delivery of a highly secure platform and activities. The following activities help us achieve this mission.

**Secure Development**
The development process strictly follows industry best practices (OWASP, SANS, NIST) that are continually tested using industry leading tools and third-party review.

**Penetration Testing**
Amber Road regularly performs testing for security vulnerabilities both in-house and by independent security assessment service providers. Penetration tests are performed on at least an annual basis by an independent third party.

**Change Management**
Amber Road follows a strict change management process. Changes are tracked, reviewed and approved to ensure operational changes are aligned with Amber Road’s business objectives and compliance requirements. A change is reviewed before being moved into a staging environment, where it is further tested before finally being deployed to production.

**Encryption in Transit**
Amber Road supports TLS1.1 or above with minimum key length of 128 bit to encrypt network traffic between the customer application and Amber Road.

**Encryption at Rest**
Amber Road offers customers the option to encrypt databases stored on Amber Road DB servers. The encryption is based on a 256-bit AES algorithm.

**Account Security**
Amber Road offers robust security controls that the customer can choose to enable in the application, such as an audit trail, log-in policy password complexity, and more. We encourage customers to work with their account managers and use these controls.
The security of our infrastructure and networks is critical. Creating a safe platform for Amber Road applications and customer innovation is the mission of our cloud security.

**Top-tier Infrastructure**
We use multi-layered controls to help protect our infrastructure, and are constantly monitoring and improving our applications, systems and processes to meet the growing demands and challenges of security.

**Asset Management and Ownership**
All assets are assigned with a defined owner and accountability.

**Access Control**
Access to production infrastructure is limited to the minimal number of employees based on least-privilege concept and need-to-work basis.

**Monitoring**
Amber Road utilizes a wide range of tools to monitor its environment across all data centers from the network, server and application level. Parameters are collected from devices on the network and aggregated to a central location for the sake of detecting indication(s) of compromise, intrusions, anomalies, trends, threshold crossing, etc.

In addition, logs are collected into a security information and event management (SIEM) platform that is monitored by a dedicated security operations center (SOC) to help ensure rapid detection and mitigation of risks.

**Distributed Denial-of-Service (DDoS) and Application Attack Prevention**
As part of the multi-layered protection approach, a dedicated application attack and DDoS mitigation ecosystem have been put in place. On a high level, this includes a minimum of four layers of protection, including multiple layers of firewalls, intrusion detection and prevention, SLB and DMZ protections (which includes specific configurations for DDoS mitigation), and application traffic reputation services for attack mitigation. On top of that, DDoS scrubbing center service is available.
Physical security of Amber Road facilities is an important part of our security strategy.

**Data Center Security**
Amber Road’s production environment is hosted in data centers across APAC, the United States and Europe. The facilities comply with the highest industry standards for physical, environmental and hosting controls.

For example, this includes 24/7 security officers, facility access, biometric hand reader, exterior security, interior security, annual audits, cages, alarm monitoring/intrusion protection, video imaging, CCTV, audio intercom and two-way radio subsystem, ID requirements, intrusion testing, security personnel hiring/training, security policies, asset tracking and video surveillance.
Amber Road maintains a full-scale, one-to-one ratio disaster recovery facility, which guarantees consistent service performance and minimal data loss in the event of a regional disaster.

**Recovery Planning**
Amber Road maintains formal business continuity and disaster recovery plans that are regularly reviewed and updated.

**Global Resiliency**
Amber Road operates out of two data centers in the US, serving mainly US-based customers - one in Florida and one in New Jersey. Within Europe, it also operates out of two data centers serving its European-based customers - one in Germany and one in Ireland.

Amber Road additionally has two data centers in Shanghai, China, and two data centers in Hong Kong.

Amber Road has established a business continuity plan (BCP) that enables it to respond quickly and remain resilient in the event of most failure modes, including natural disasters and system failures.

**Customer Data Backups**
Amber Road conducts full daily and weekly incremental backups, providing up-to-the-minute recovery from archive logs. Backups are performed to disk within the data center and replicated, via a secure private connection, to the backup data center. All the artifacts required to restore service are backed up, including DBs, file systems and virtual servers.
With the exception of our data center providers, Amber Road directly manages our SaaS solution. Amber Road has implemented the following procedures.

**Vetting Process**
Third-party vendors used by Amber Road are checked before employment to validate that prospective third parties meet Amber Road’s security standards. Customer data will not be accessible to third parties or subcontractors.

**Ongoing Monitoring**
Once a relationship has been established, the Amber Road security team will conduct an annual review of these vendors. The annual review can be done by Amber Road’s security team or via a third-party report (e.g., SSAE 16 SOC2 report, ISO 27001).

The procedure takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data and legal/regulatory requirements.

Amber Road is committed to mitigating risk and ensuring its services meet regulatory and security compliance requirements.
Regulatory Environment
Amber Road complies with applicable legal, industry and regulatory requirements as well as industry best practices, including AT101 SOC2.

Amber Road has obtained SOC2 certification, which validates the strength of our security controls, shows confidence in our security program, and demonstrates our maturity within the information security space. Security is a top priority for Amber Road and this achievement demonstrates our commitment to information security, data protection and continuous improvement.

EU-US (and Swiss-US) Privacy Shield Framework
Amber Road has been working in the European Union for many years. Our operations are certified under the EU privacy regulations through the Privacy Shield Framework provisions as a part of our commitment to comply with EU data protection requirements in case of a need to process or store EU data outside of the EU.

General Data Protection Regulation (GDPR)
As mentioned, Amber Road has been active in the EU for a significant number of years and has maintained compliance with the ever-changing EU privacy requirements. As such, Amber Road is, and will actively remain, compliant with the new GDPR regulations.
CONTINUOUS MONITORING AND VULNERABILITY TESTS

At Amber Road, the security and resiliency of our products and infrastructure is a top priority. As part of the ongoing work of the security team, continuous monitoring is being done as part of the compliance and regulation program and the risk assessment. The vulnerability tests establish how we identify, respond to, and triage vulnerabilities against the Amber Road platform. To ensure security of our platform, Amber Road continues to mature the following capabilities:

**Continuous Monitoring Program**
Our security team uses a centralized SIEM system to collect logs from different security tools, identify current or historical vulnerabilities, and track incidents and threats that Amber Road must respond to and mitigate accordingly.

**Distributed Denial-of-Service (DDoS) and Application Attack Prevention**
Amber Road infrastructure is protected with multiple layers of defense systems, including a dedicated, real-time, best-of-breed application attack and DDoS mitigation technology. Amber Road’s multiple layers of firewalls, intrusion detection systems, load balancers and DMZ servers contain dynamic mitigation and NAT to deny attack traffic. This includes advanced protection controls such as Forward and Reverse Proxies. In addition, Amber Road uses private ranges of IPs that deny direct access to internal networks, further reducing DDoS and application attacks. Amber Road is using the services of a scrubbing center in case of DDoS attack.
As a leading SaaS provider with more than 20 years of experience in the industry, we realize that working in a cloud-based environment may raise concerns related to the protection of confidential and personal information. Security mechanisms to protect physical, network and application components of the platform, coupled with transparency about our security policies and processes, allow many of the Fortune 500 to trust us with their most confidential data, while leveraging the benefits of our SaaS solution.

For further details and steps to secure your Amber Road account, or if you have questions or need more detailed answers, feel free to get in touch with our Security Team via your Account Manager.

About Amber Road
Amber Road’s (NYSE: AMBR) mission is to dramatically transform the way companies conduct global trade. As a leading provider of cloud-based global trade management (GTM) software, trade content and training, we help companies all over the world create value through their global supply chain by improving margins, achieving greater agility and lowering risk. We do this by creating a digital model of the global supply chain that enables collaboration between buyers, sellers and logistics companies. We replace manual and outdated processes with comprehensive automation for global trade activities, including sourcing, supplier management, production tracking, transportation management, supply chain visibility, import and export compliance, and duty management. We provide rich data analytics to uncover areas for optimization and deliver a platform that is responsive and flexible to adapt to the ever-changing nature of global trade.