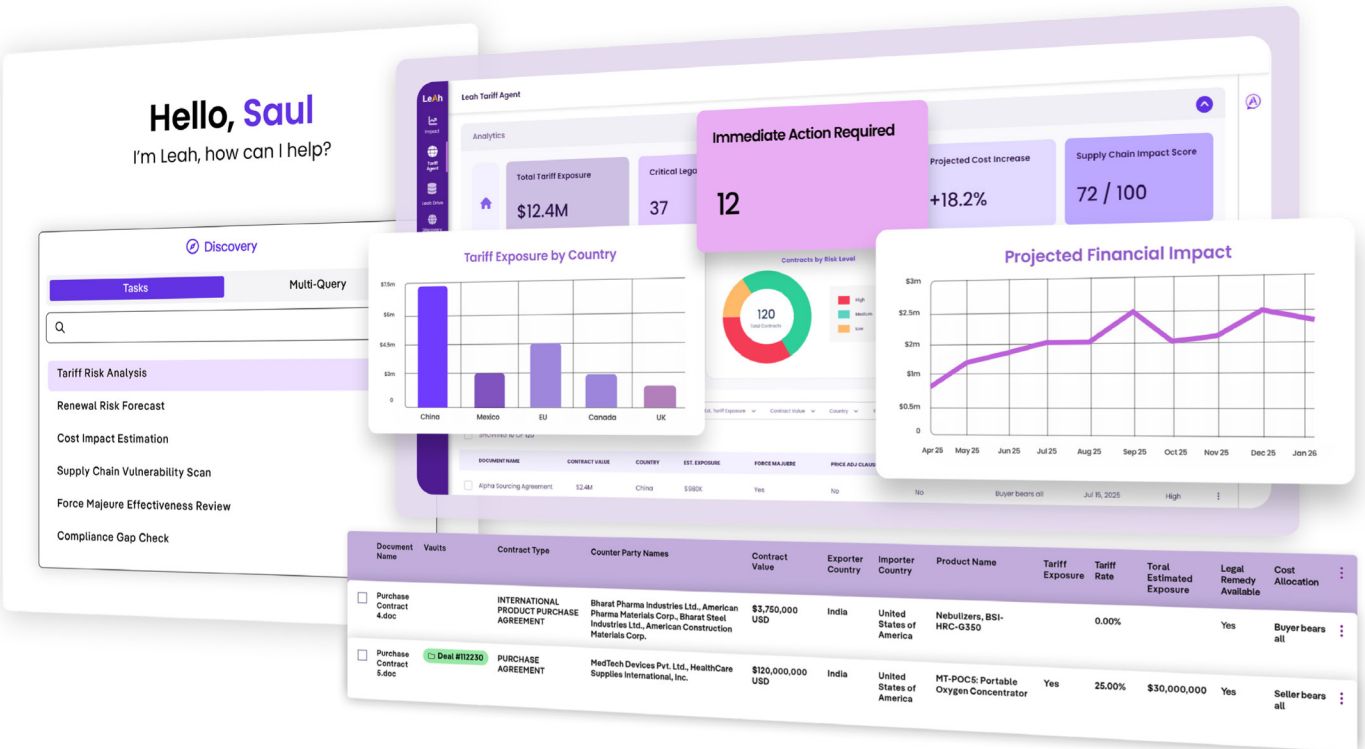
LEAH

Leah Architecture, Privacy, and Security



Leah Infrastructure

The Leah subscription software-as-a-service (formerly CPAi Service) is regionally hosted within Microsoft Azure Cloud (Azure) cloud datacenters, with available locations in the continental United States, continental Europe, or Australia. Each hosting location is mirrored across multiple, geographically dispersed data centers for fault tolerance and business continuity within the region the service is set to use. Clients may select specific regional processing locations upon implementation. The service provides clients with secure access to their mission-critical contract management system with a monthly uptime of 99.9% (excluding scheduled maintenance periods).

01 Encryption for External Connections	Transport Layer Security (TLS) encryption technology is utilized for data transfer between all parties involved in the process. TLS connections are negotiated for at least 256-bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. It is recommended that clients use the latest available browsers and consistently keep their browsers up to date because they are compatible with higher cipher strengths and have improved security.
02 Network Access Control	A limited number of Leah operations team members are granted access to the hosting environments, and then only after the completion of a successful background check, security awareness training, and acknowledgment of privacy and confidentiality agreements, and additional information security training. Access occurs through a multi-factor VPN (Virtual Private Network) or Private Proxy connection. Additional authentication, authorization, and accounting are implemented through standard security mechanisms. These measures are designed to ensure that only approved operations and support engineers have access to the systems. Remote access to the Azure environment is restricted to select operations staff and only available via two-factor authentication.
03 Network Bandwidth and Latency	Leah relies on the Azure network infrastructure to provide low latency network availability between the Leah Service and end users. The Azure infrastructure is built around regions and availability zones. A region is a physical location in the world where we have multiple availability zones. Availability zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, and housed in separate facilities. These availability zones offer you the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data center. Leah monitors applicable networks and addresses internal issues that may impact availability.
04 Anti-Virus and Anti-Malware Controls	Leah leverages best in class tools to monitor and block virus and malware behavior. This includes protection against emerging threats beyond traditional, signature-based solutions. Firewalls and intrusion prevention Leah utilizes firewalls as one component of a layered approach to application infrastructure security. To control access and allow only authorized traffic to Leah infrastructure, managed firewalls are used. In addition, Leah employs security policies to manage ingress and egress of data based upon protocol, port, source and destination within the environment. Any traffic not adhering to these strict access controls is discarded at the Internet boundary. Internally host-based intrusion prevention and monitoring systems are deployed at the server and network layers, respectively.

05 System hardening and Monitoring	Leah employs an enterprise-class vulnerability management program to monitor and alert on any non- authorized changes or security configurations. Services undergo 3rd party penetration tests on at least an annual basis or prior to release of a material change.
06 Account Provisioning and Access Control	Identity management is used to provide authentication. Users must have a valid username and password to access the system. User profiles containing First and Last name, email address, login name, and password are associated with User Groups, User Security Roles, and Profile Rules using conditions and actions. Single Sign-On is also an option for ease of user administration and greater security controls. The Leah Service uses SAML (Security Assertion Markup Language) 2.0 for our SSO solution. Leah employee access to the service is limited to only that access required for support and maintenance purposes. Employee access is contingent on a successful background check, confidentiality agreements, and documented authorization by an appropriate member of management. Access is strictly controlled via VPN and other authentication mechanisms, as specified above.
07 Data Management and Protection	Leah subscribers own the files and data that reside in the service. Each subscriber has their own unique, credentialed and named database instance. These database instances are encrypted at rest for an additional level of data security. Subscriber data is never commingled with data from other subscribers.
08 Incident Response	Leah has a rigorous incident management process for security events that may affect confidentiality, integrity, and/or availability of systems or data. If an incident involves customer data, Leah will inform the customer and support investigative efforts via our Customer Service team. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. To help ensure the swift resolution of security incidents, the Leah security team is available 24/7 to all employees. If an incident involves customer data, Leah will inform the customer and support investigative efforts via our security team.
09 Physical Security	Processing occurs within Azure data centers that are housed in nondescript facilities. Professional security staff strictly control physical access, both at the perimeter and at building ingress points. Video surveillance and intrusion detection systems are in place at a minimum of all ingress and egress points. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification, are signed in, and are continually escorted by authorized staff.

10 Scalability	Leah is architected to be both horizontally and vertically scalable; additional services can be added to increase the performance of clusters and new clusters can be added to provide service for new clients.
11 Availability and Disaster Recovery	Leah maintains geographically diverse data centers and leverages the near seamless failover technologies from Azure. The people, processes, and technology necessary to conduct our business are distributed among these sites, with critical business operations conducted at multiple globally diverse locations. If activity at any one of these sites is disrupted, our systems are designed to continue operating at the other locations without serious interruption for clients. Available data centers are built in clusters in various regions. All data centers are online and serving clients. No data center is "cold." In the case of failure, automated processes move customer data traffic away from the affected area. Each availability zone is designed as an independent failure zone. Information stored in the Leah Service is backed up using Azure-provided facilities. For short term recoverability, the Azure point-in-time restore capability is enabled. Using a combination of daily snapshots and transaction log backups, a recovery can be performed to any instant in the prior 30 days. For longer term recoverability, Azure snapshots are taken nightly. For Azure Blob Storage, the Azure Backup Service snapshot functionality will be used to snapshot the blob storage daily. Both the database and file backups will be encrypted and retained for one year.
12 Office Disruptions	Leah maintains a globally diverse operations staff in the event core offices have any significant disruption. Additionally, all Leah employees have laptops and a secure process to access necessary resources to support infrastructure and clients.
13 Leah Audits and Certifications	Leah is committed to achieving and maintaining the trust and confidence of our clients. Integral to this mission is Leah's dedicated, in-house security team. This team is tasked with enabling Leah clients to meet a multitude of compliance, data protection, and regulatory obligations from around the globe. Leah's trust and assurance activities include: · Service Organization Control (SOC) reports: Leah's information security control environment undergoes an independent evaluation annually. Leah's most recent SOC 2, Type II report covering security, availability, and confidentiality is available upon request. Data Processing Addendums or Agreements including the Standard Contractual Clauses as approved by the European Commission and incorporating stringent requirements of Article 28 of the EU General Data Protection Regulation 2016/679. Penetration testing conducted by industry-recognized 3rd party on material environment changes or annually. HIPAA (Health Insurance Portability and Accountability Act): Leah signs Business Associate Agreements (BAAs) to meet client needs.

14

Security Related Maintenance

The Leah operations and development teams, in conjunction with our Information Security department, performs security-related change management and maintenance. In most cases, these are invisible to the client via new system builds at the data centers. Patches and updates are installed during the scheduled maintenance window so as to minimize any downtime.

LEAH