Remote and Offshore Resources Overview

Verisma partners with a select group of long-standing offshore service providers located in the Philippines and India. All offshore team members supporting Verisma clients are fully vetted through background checks and onboarding processes equivalent to those for U.S.-based staff.

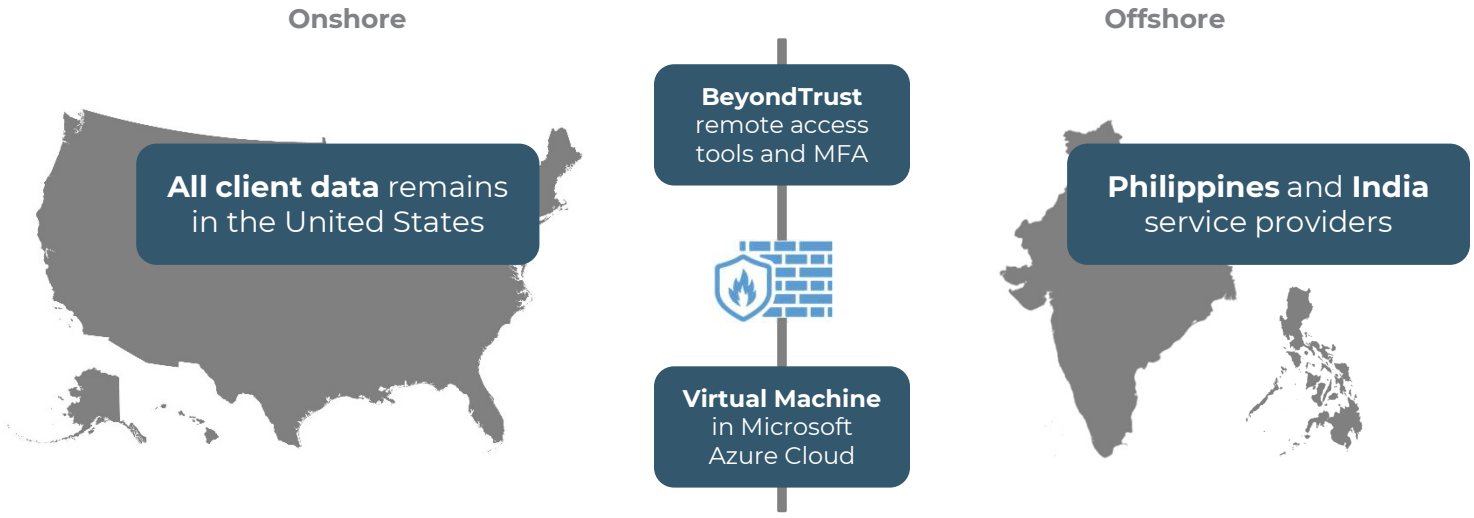
All client data is hosted within Microsoft Azure's U.S.-based data centers (primarily US East, with backup/disaster recovery in US West) and stored on encrypted physical media. No PHI is ever stored outside the United States.

Offshore team members access client environments using BeyondTrust remote access tools with multi-factor authentication (MFA) and conditional access policies managed through Microsoft 365. IP whitelisting is enforced to ensure access is only granted from secure, approved office locations.

Verisma does not permit offshore team members to work from home. All work must be performed from company-owned facilities that are included in the scope of applicable security audits. Any exceptions require approval from Verisma's Chief Information Security Officer (CISO) and must be technically enforced.

All offshore partners must maintain industry-recognized certifications (e.g., HITRUST, SOC 2 Type II, ISO-27001) covering HIPAA Security Rule controls and physical safeguards. These certifications are verified as part of Verisma's own HITRUST r2 compliance efforts. Contracts include Business Associate Agreements (BAAs) and clear Notice of Assignment (NOA) terms.

All activities are logged, monitored, and subject to regular audits. Annual physical office inspections are conducted.



Further information is available from Verisma's CISO, Jim Staley (jstaley@verisma.com) or our Third-Party Risk Management group (tprm@verisma.com).

Verisma Systems, Inc.
1750 Founders Pkwy
Ste 130.
Alpharetta, GA 30009