Why Native Recording in Teams Is Not Enough

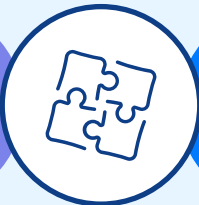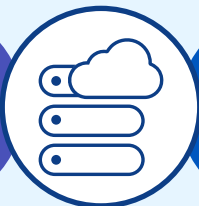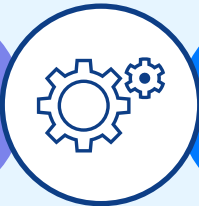| Native Recording in Teams	Compliance Recording
Teams users must manage manual **convenience recording** for Teams meetings and P2P calls	**Automated, always-on recording**, controlled by policies set up for a user or user group and covering all Teams interaction scenarios
Data can be stored in MS Stream only. Doesn't meet strict security standards to avoid data deletion or alteration during the retention period	**Multiple (on-prem or cloud) compliance storage and WORM archive integrations** with advancedregional data segregation
Basic search & playback without timeline view and advanced data tagging, not available for all communication modes	**Advanced search & playback** for compliance use cases – covers all communication modes, security, governance, discovery and user admin
Transcription only available in MS Stream. Lacks speaker identification and advanced analysis	**Open integration with advanced transcription engines** offering high accuracy, robust search and advanced analytic capabilities
Recording only available for MS Teams communications	**A single recording platform** for Teams, other leading UC, messaging, trading turret, mobile and IP telephony environments
Recording capability only available in the public cloud (MS Stream)	**Choice** of on-premises, hybrid and (public or private) cloud deployment models
Recording is not resilient to avoid service disruptions and unrecorded calls as a result	**Multiple resilience options** for undisrupted recording (load balancing, geo-resilient failover, redundant 2N recording)
Security features are not sufficient to keep the data safe and tamper-proof. Auditing capability limited to 90 days in O365	**Secure** access control, encryption, compliance workflows, full audit trail of all events with customizable retention periods

www.verint.com

VERINT.