RevSync Security Paper

MMS Version 12.0
Revision: 31.12.2024

TABLE OF CONTENTS

INTRODUCTION

The purpose of this document is to detail how Revcord security and privacy practices are applied to the RevSync cloud-based platform features and to provide security assurances to our customers.

REVSYNC PRODUCT DESCRIPTION

We offer RevSync to "virtualize" the logger. RevSync delivers the flexibility to remotely access recorded data on the Revcord MMS logger from outside of the internal network and provides live monitor functionality within a remote private tenancy. The recorded data is automatically synchronized from the remote tenant back to the local logger. RevSync also replaces expensive and unreliable onsite data storage and mitigates the risk of complete loss of recordings in the case of a catastrophe. RevSync is offered as the ultimate logging solution for the client: local and cloud-based access and redundancy.

As systems and threats evolve, no system can be protected against all vulnerabilities, and we consider our customers to be an essential partners in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention, and we will investigate them. Where appropriate, we will address the issue with product changes, technical bulletins, and/or responsible disclosures to our customers and regulators. Revcord continuously strives to improve security and privacy throughout the product life cycle.

KEY FEATURES OF REVSYNC

- Remote live monitoring of all channels
- Data Syncs both ways, i.e., changes done on the remote tenant syncs to the local logger
- Tier-4 Datacenter
- NFPA 110 Compliant
- Ability to troubleshoot the local logger without the need for access to the local server for various situations
- Securely access your mirrored system remotely from any location in the world
- Remote storage of all local logger recording data in case of a catastrophic disaster
- Five years of data storage
- HIPAA Compliant Access (Updated Quarterly)

- CJIS Compliant (Data Transmission and Data Storage)

SPECIFICATIONS

HARDWARE

- Minimum 8GB Ram
- Minimum Quad-Core Processor
- Minimum Windows 10 or Windows Server OS – 2019

NETWORK PORTS AND SERVICES

Port	Protocol	Service Name	Service	Description	Service	Encrypted	Open/C
1533	TCP	SQL	Outbound port	Websocket	Outbound port	Yes	Open
8441	TCP	RevSync	Outbound port	FTP	Outbound port	Yes	Open
443	TCP	RevSync	Outbound port	Websocket	Outbound port	Yes	Open
8431	TCP	RevSync	Outbound port	Livestream	Outbound port	Yes	Open

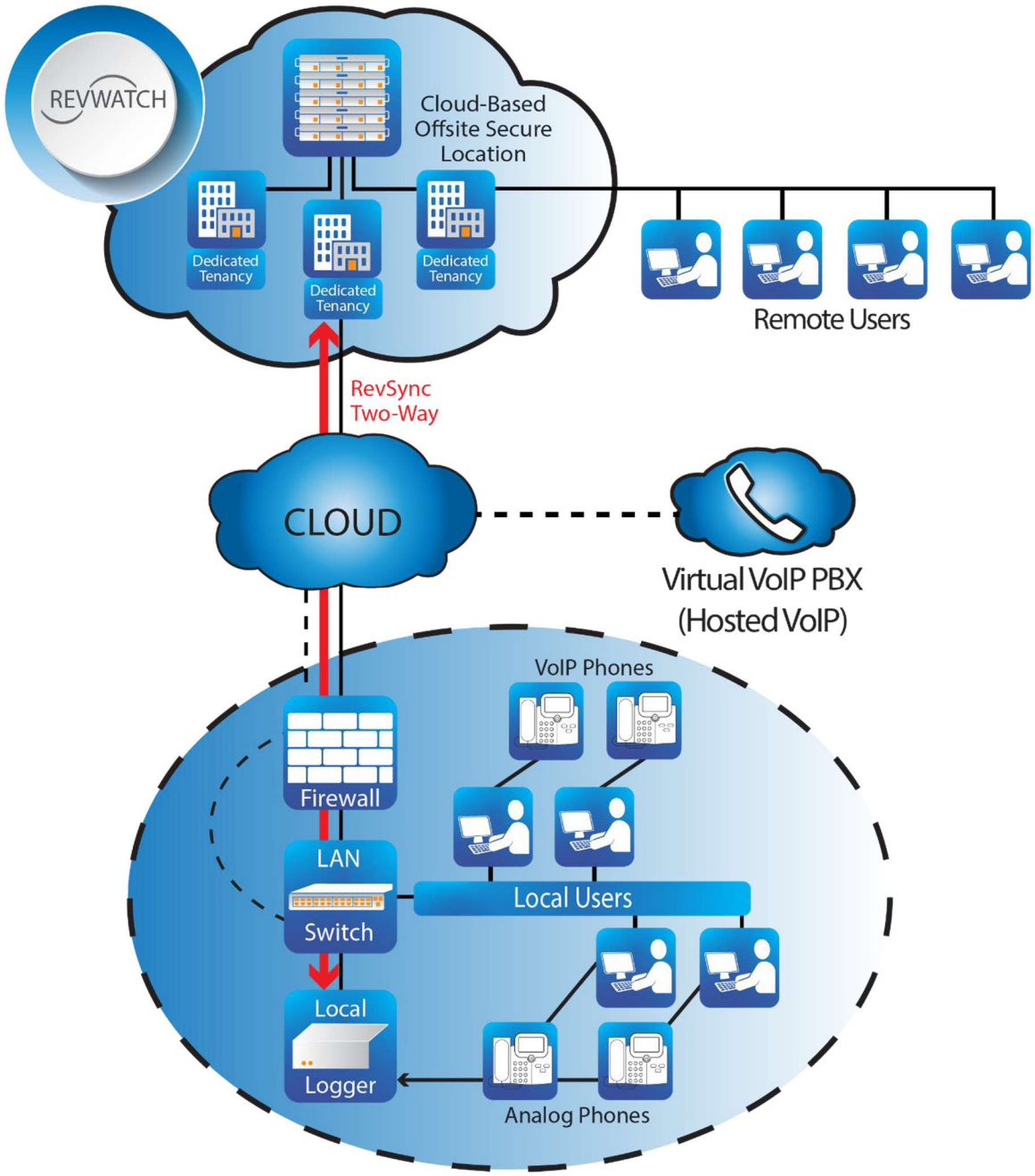
SECURE DATA TRANSMITTED AND STORED

- Data in transit meets CJIS encryption requirements (CJIS Security Policy 5.10.1.2.1)
- Data at rest in Revcord's Data Center meets CJIS and HIPAA compliance requirements (Data Center meets FIPS 140-2 requirements)
- Data at rest is stored as proprietary DSF audio files and optionally encrypted at the user's discretion. Audio format cannot be used outside of the Revcord environment.
- MMS Login account information

SECURITY OF TRANSMISSION AND STORAGE

- RevSync uses only outbound ports. There is no inbound traffic into the network.
- All communications are initiated from the local server.
- Windows and/or third-party firewall configurations are limited to ports 1533 and 8441 for outbound traffic only, which protects against possible network intrusions.
- All network traffic adheres to the TLS 1.2 standard using Secure Web Socket (WSS) as the protocol. Like HTTPS, WSS (WebSockets over SSL/TLS) is encrypted, protecting against man-in-the-middle attacks.
- RevSync stores all data in a proprietary format and can also store in an encrypted format.

NETWORK ARCHITECTURE AND DATA FLOW DIAGRAM



SECURE DATA STORAGE

RevSync customer data is stored at a Tier-4 data center in the Houston area. This ensures that in the unlikely event of a disaster at your facility, software and customer data can be back online in a matter of minutes. Tier-4 meets the CJIS definition of a physically secure location.

A Tier-4 data center is an enterprise-class data center tier with redundant and dual-powered servers, storage, network links, and power cooling equipment. It is the most advanced type of data center certification, which typically serves enterprise corporations and provides the following:

- 99.99% uptime per year (Tier 4 uptime).
- 2N+ 1 fully redundant infrastructure.
- 96-hour power outage protection.
- >26.3 minutes of annual downtime.

DATA CENTER PHYSICAL SECURITY

- Facility access is controlled with card control and auditable logs. The facility has alarms and monitoring for fire and unauthorized access as well as camera systems.
- Access to the facility is logged.
- Access is restricted to NETdepot personnel and Datacenter remote hands staff. Equipment is secured within a locked cage restricted to NETdepot authorized personnel and Datacenter Remote Hands.
- Background checks are performed for all personnel with access to Hosting Infrastructure.
- Media (hard drives) are secured at offsite locations in a SOCII facility within a locked cage, and the facility maintains access controls based on biometrics and card-based access.
- The offsite location is a SOCII facility within a locked cage, and the facility maintains access controls based on biometrics and card-based access. The backed-up data would be images of the Virtual Machines, which would be "turned up" in the remote location so the architecture would be identical to the production location.

DATA CENTER NETWORK SECURITY

- The public-facing web servers and application servers are on a separate layer 2 segments from the database servers, with strict firewall policies and logging monitoring cross-segment traffic.
- The supplier's Endpoint Devices are virtually separated into a "virtual datacenter" with its VXLAN overlay segments and a virtual firewall. There exists no routability to the

hosting infrastructure.

- Firewall logs are routinely monitored as well as set up for Email alerts to IT Director. The logs are monitored every hour for anomalies.
- There are host-based and network-based intrusion prevention systems and intrusion detection systems (IPS/IDS) installed on the Hosting Infrastructure

- IPS/IDS logs in the Hosting Infrastructure are monitored for anomalies on a 24 hour/365-day basis.
- IPS/IDS logs for the Hosting Infrastructure are retained for a period of one year.
- Network device logs for the Hosting Infrastructure are analyzed daily for anomalies.

DATA CENTER HOSTING INFRASTRUCTURE SECURITY

- Each server in the Hosting Infrastructure is protected by ESET Cyber Protect Cloud - Server Security with Dynamic Threat Defense.
- Data Center performs quarterly vulnerability scans on the Hosting Infrastructure.
- Data Center employs a third party to perform annual penetration testing on the Hosting Infrastructure.
- The Multi-Tenant system is virtually and logically separated from all other customers' equipment and data.

DISCLAIMER

The information contained in this document is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and Revcord or Revcord subsidiaries or affiliates (collectively, "Revcord"), including but not limited to our Warranty statement, our LaaS agreement, our Terms and Condition of sale, and our RevShield Service Level Agreement. Revcord does not make any promises or guarantees to the customer that any of the methods or suggestions described in this document will protect, restore or resolve any customer system issues.