SECURITY AND PRIVACY WHITE PAPER

Poly Remote Monitoring & Partner Branded Remote Monitoring Services Overview

Part 3833-87257-001

Version 02

August 2021

Introduction

This white paper addresses security and privacy related information regarding Poly and Partner Branded Remote Monitoring (RM) Services for Poly approved room systems and Poly infrastructure devices. This white paper describes the security features and access controls applied to Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of these Poly Managed Services, and the location and transfers of personal and other customer data. Poly will use such data in a manner consistent with the Poly Privacy Policy and this white paper (which may be updated from time to time). This white paper is supplemental to the Poly Privacy Policy. The most current version of this white paper is available on Poly's website.

The following Poly Managed Services are discussed in this white paper:

Poly Remote Monitoring Services

- Poly Remote Monitoring Service
- Partner Branded Remote Monitoring Service

Overview of Poly Remote Monitoring Services

The Poly Remote Monitoring Service grants customers access to the Poly Monitoring System to monitor devices on their network. It also provides customer access to the dashboard that graphically displays the status of their devices and shows real time reports. Lastly, the service provides automated alerts and standard emailed monthly reports.

The basic operation of the service requires a collector to be deployed on the customer network where the devices reside. The devices provide data to the on-premises collector, which in turn relays that information back to the Poly Hosted Monitoring System. Using that data, the Monitoring System will monitor device health, and based on the configuration, update the real-time dashboard as well as send email alerts to the customer.

There are three (3) network connections to the service:

1. HTTPS://rmm.poly.com – dashboard
2. SSH application layer tunnel – device RM
3. (Optional) IPSEC VPN transport tunnel – device RM

Security at Poly

Security is always a critical consideration for all Poly products and services. Poly's Information Security Management System (ISMS) has achieved ISO 27001:2013 certification. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and you can be reassured that Poly has established and implemented best-practice information security processes.

Product security at Poly is managed through the Poly Security Office (PSO) which oversees secure software development standards and guidelines. The Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013, and OWASP for application security. Guidelines, standards, and policies are implemented to provide our developers with industry approved methods for adhering to the Poly Product Security Standards.

Secure Software Development Life Cycle

Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development process. Every phase of the development process ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing, and attack surface analysis are performed to verify the implementation.

The S-SDLC implemented by Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Poly products, a defense-in-depth model is systematically incorporated through layered defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation.

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

Privacy by Design
Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions, and processing of personal data and providing features which enable the data subject to exercise any rights they may have.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, Poly considers the right to data protection with due regard.

Security by Design
Poly follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems), and availability. These extend to all systems that Poly uses – both on-premises and in the cloud as well as to the development, delivery and support of Poly products, cloud services and managed services.

The foundational principles which serve as the basis of Poly's security practices include:

1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

Security Testing
Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams.

Patches are evaluated and applied in a timely fashion based on perceived risk as indicated by CVSSv3 scores.

HTTPS for Dashboard of Poly Remote Monitoring Service
Poly provides a URL to the customer which allows them to connect to the Dashboard and real-time reports. Customer web browser authentication is via Azure AD authentication, then local authentication is used to connect to the dashboard in the Presentation Layer DMZ in the Poly premises.

SSH for Poly Remote Monitoring Service
An SSH tunnel is used to connect the collector in the customer environment to the Poly Managed Services Public IP egress for the Remote Monitoring Service. The RM presentation, business logic, and database servers all reside in their own DMZs on Poly-owned hardware.

No unnecessary network ports are opened between zones. The customer will specify an IP address for the collector. The Poly specified IP address will be termed as "home" for the collector and the collector will phone home. All data flows will be initiated from

the collector to the Poly hosted service. All traffic traversing the VPN is protected by encryption.

Externally, all traffic between the Poly owned servers residing in the above-mentioned DMZs and the customer collector will traverse the SSH tunnel. Internally, monitoring information is sent to the monitoring database within the Poly Managed Services environment to generate alerts and dashboards.
The customer provides the compute resources to run the collector application.

SSH Tunnel Parameters

- Port 7705
- X509 certificates with RSA 2048 encryption
- 2048-bit RSA key for certificate verification
- SSH v1 – disabled
- SSH v2
- TLS v1.2 connection protocol
- DHE-RSA-AES256-SHA cipher for OpenSSL
- AES-256
- SHA-2 message digests

VPN For Poly Managed Service for Remote Monitoring

An IPsec VPN across the Internet may be used to connect the customer environment to the Poly Managed Service for Remote Monitoring. The VPN is an additional layer of security that may be wrapped around the earlier mentioned SSH tunnel.

The IP address space used by the servers is typically provided by the customer for convenience in routing across the customer's network. If multiple VPNs are used, each VPN has dedicated access from a specific DMZ with a unique set of IP addresses. Redundant VPNs between one DMZ and the customer's collector require custom development and are not part of the standard RM service. On the Poly side, each VPN will terminate at a Poly core data center to provide connectivity with the least network latency.

Typically, the IPSec VPN will be terminated directly on customer's network equipment. All traffic traversing the VPN is protected by encryption. The DMZ is encapsulated by firewall security zones. No unnecessary network ports are opened between zones. Externally, all traffic between the DMZ and the customer will traverse the IPsec VPN. Internally, monitoring information is sent to the monitoring database within the Poly Managed Services environment, to generate alerts and dashboards.

Poly's preferred IPSec VPN parameters are shown in this table:

IKE/ISAKMP Parameters (Phase I)	Values
Mode	Main
IKE Version	1
IKE Encryption / Encryption Algorithm:	AES-256
Pre-Shared Key:	TBD
Authentication Algorithm:	SHA-2 (256)
DH-Group:	Group 2
Security Association Lifetime (Seconds):	86400

IPSEC Parameters (Phase II)	Values
Protocol	ESP
IPSEC Encryption Algorithm:	AES-256
Authentication Algorithm:	SHA-2 (256/128)
Perfect-Forward Secrecy (PFS):	Yes
PFS Keys DH-Group:	Group 2
Security Association Lifetime (Seconds):	7200

These are the parameters that will be used if the VPN terminates on an appliance provided by Poly. If the customer elects to terminate the VPN on its own network equipment, parameter values will be negotiated between Poly and the customer. But the above are strongly recommended for the security of both the customer and Poly.

Source of Personal Data	Categories of PI Processed	Business Purpose of Processing	Disclosed to the following Service Providers
Support and reporting services	• Endpoint display name • IP address • User email address • User ID • User phone number • User address/location	• Troubleshooting and support remediation • Provide required reporting for monitoring services	None

Data Processing

Monitoring data continuously flows between the sensor and the internal database. This may contain the IP addresses and DNS names of monitored systems. SNMP data records are collected through the VPN for monitoring and reporting for the service. These may contain names, emails, IP addresses, and locations.

Customers who contact Poly for technical support are asked to provide contact information.

If someone is an individual user and the purchase of a Poly Remote Monitoring Service has been made by their employer as the customer, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data.

Purpose of Processing

The primary purposes of processing information by the Poly Remote Monitoring Service are to provide monitoring, dashboards, and reporting per agreement requirements.

How Customer Data Is Stored and Protected

Reporting data is stored in an encrypted server in the Poly IT environment for 2 months or the conclusion of the engagement, whichever comes first. Technical support details are stored in Poly CRMs and on SFTP (temporarily held until 90 days after ticket is closed).

Poly may change the location of the Poly Managed Service database server and details of any such change shall be set forth in the latest copy of this white paper available on Poly's website.

For transferring personal data of EU customers to the US, Poly uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

Data Deletion and Retention

Poly may retain customer data for as long as needed to provide the customer with the Poly Managed Service and/or Poly Remote Monitoring Service. When a customer makes a request for deletion to privacy@poly.com, Poly will delete the requested data within 30 days, unless the data is required to be retained for Poly's legitimate business purposes or if needed to provide the service to customer. Poly may "anonymize" personal data in lieu of deletion. The anonymization process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (such as name, site information, and IP address) with randomly generated alphanumeric characters.

Secure Deployment

The customer is responsible to procure and secure the public internet access and public IP addresses for the IPSec service to use. Poly will be responsible to procure and secure the public IP addresses for the SSH service to use.

Customer information obtained during onboarding is used to create the DMZ. Customer is able to monitor Poly network traffic as it will only enter the customer's network using the subnet assigned.

The DMZ has specific functionality to support the service. Monitoring uses a collector in each DMZ allowing for gathering of alert information (e.g., SNMP, API, Ping, etc.) from the customer and

isolation of the internal Poly Managed Services network. Externally, all traffic to and from the customer will traverse the SSH or IPsec VPN. Internally, monitoring information is sent to the monitoring database, within the Poly Managed Services environment, to generate alerts and dashboards.

Poly Remote Monitoring for On-Premises (RM) Video Endpoints and Infrastructure Devices

The customer is responsible for securely configuring the endpoint devices and/or provisioning setup, whether on their own or working with Poly Professional Services. Poly is responsible for securely configuring the DMZ and connections to the customer, as well as keeping provisioning profiles current throughout change management.

Server Access and Data Security

The customer or their Service Provider (depending on the agreement) is responsible for physical and data security for all systems in their environment up to the Poly VPN connection at the edge of the network.

All backend and monitoring servers created for the use of Poly Remote Monitoring Services follow hardened templates for deployment. Firewall ports are opened only as necessary, and changes are documented through change management.

Backend and monitoring servers that are the foundation for the Monitoring Services network and DMZs are in secure data centers, with only authorized staff members having badged access. The access to the equipment for these systems is via secure and bi-directional tunnel.

Cryptographic Security

Poly Managed Services Connections

- Certificates per Poly asset used for administrative access
    - Encryption algorithm: SHA-256
    - Authentication Algorithm: RSA
- IPsec VPN connection minimums
    - Encryption algorithm: AES-256
    - Authentication algorithm: SHA-2

Poly Managed Services Data Storage Encryption

- Password storage
    - Encryption algorithm: AES-256
    - Local authentication: SHA-512
- Support ticket information
    - Encryption algorithm: AES-256
- Reporting server (BRMs)
    - Encryption algorithm: SHA-256
- Backup server (application backup data)
    - Encrypted by individual application (please see individual application Security White Paper for details)

Authentication

Poly personnel use certificates on Poly managed assets for their software VPN connection to the Poly Managed Services network. From their Poly device, administrators access the specific proxy server using unique AD credentials. The Poly Managed Services network has a separate Active Directory server for providing unique credentials and logging user activity on the proxy server dedicated to the customer.

Poly Managed Services personnel initially access the customer's managed devices using local administrator credentials provided during onboarding. These credentials are changed when Poly Managed Services goes operational.

Monitored device credentials are stored in an encrypted password manager which is assigned, managed, and logged per user. All customer user traffic will stay within the customer's network.

Change Management
Poly Remote Monitoring Services utilize the Information Technology Infrastructure Library (ITIL) framework. Poly uses its own change management policies and procedures, aligned with ITIL, to document and review changes for viability and necessity.

A formal change management process is followed by all teams at Poly to minimize any impact on the services provided to the customers. All changes implemented go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing). Only after final approval from stakeholders, changes are implemented in production. While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to applying any changes in production.

Disaster Recovery and Business Continuity
The solution's core network leverages hardware redundancy on all routers, switches, and firewalls. Depending on the chosen customer solution, connectivity to the customer can be single SSH or IPsec VPN connectivity to one or multiple sites. Each core DC has multiple routes to the internet. The monitoring solution leverages distributed applications to request and receive SNMP information. The monitoring application's core databases and app servers are virtualized on separate hardware. Monitoring tools are also virtualized, baselined using snapshots, and backed up on a regular and recurring basis using standard virtualization toolsets.

Solutions for each customer will have Service Level Objectives (SLO) or Service Level Agreements (SLA) designed around their specific solution design and documented in the service agreement.

Security Incident Response
The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. Please contact the PSO directly at informationsecurity@poly.com

The PSO team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with Poly products and networks. Poly security advisories and bulletins can be found on the Poly Security Center.

Subprocessors
Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third-party data processor who, on behalf of Poly, processes customer data. Prior to engaging a subprocessor, Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact privacy@poly.com.

Prior to engagement, suppliers that may process data on behalf of Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk. Suppliers that cannot meet the security requirements are disqualified.

Additional Resources
To learn more about Poly Managed Services, please visit our website.

Disclaimer
This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Poly product.

You may copy and use this paper for your internal reference purposes only. POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED "AS IS" AND MAY BE UPDATED BY POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.