SECURITY AND PRIVACY WHITE PAPER

Poly Remote Managed Endpoint Services Overview

Part 3725-86319-001

Version 02

December 12, 2019

POLY REMOTE MANAGED ENDPOINT SERVICES OVERVIEW

INTRODUCTION

This white paper addresses security and privacy related information regarding Poly Remote Managed Services for Poly Unified Communications and Collaboration endpoints, which are never hosted by Poly. 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 the 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 managed services are discussed in this white paper:

REMOTE MONITORING AND MANAGEMENT SERVICES

- Remote monitoring and management for on-premises (RMM) video endpoints
- Remote management for on-premises audio endpoints

OVERVIEW OF REMOTE MANAGED SERVICES

There are two (2) options for this type of service as listed above. Each remote managed service is designed to provide a remote management and monitoring solution for Poly UC&C endpoints implemented in a non-Poly environment. The customer provides all network systems and supporting infrastructure, so security considerations will need to be configured in the customer's and/or service provider's environment.

Poly will provide a secured managed services environment consisting of the appropriate systems to provide the supporting services for the DMZ, user authentication, and secure customer connections.

Each solution is created using at least one logically separate DMZ to host the monitoring and management systems. IP addressing (RFC 1918) is provided by the customer making the DMZ a virtual extension of the customer's network. The customer must ensure that there are no IP conflicts on their network.

The monitoring and management systems consist of a jump server, a monitoring probe, and file storage dedicated to the engagement. This DMZ is external to the managed service environment and is connected to the customer via IPsec VPN.

VPN FOR REMOTE MONITORING AND MANAGEMENT SERVICE

An IPsec VPN across the Internet is used to connect the customer environment to the managed services DMZ for remote monitoring and management. The DMZ contains the monitoring and management servers and is external to the customer environment.

The IP address space used by the servers is typically provided by the customer for convenience in routing across customer's network. Customer should budget 50Mbps Internet bandwidth for this VPN. If multiple VPNs are used, each VPN is dedicated to access from a specific DMZ with a unique set of IP addresses. Redundant VPNs between one DMZ and the customer's infrastructure require custom development and are not part of the standard RMM service. On the Poly side, each VPN will terminate at the Poly core data center judged to provide connectivity with the least network latency.

At the customer's option the IPSec VPN may be terminated directly on customer's network equipment or on a VPN appliance provided by Poly. If the latter option is selected, the customer is responsible to provide public internet access, customer network access, power, cooling, and space for the VPN appliance. The VPN appliance requires a public IP

address for the VPN peer address. This address can be directly on the appliance or can be routed via 1-to-1 NAT to a private address on the appliance, whichever best fits the customer's network environment. 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 managed services environment, to generate alerts and dashboards for the Customer Management Center (CMC) technical support team.

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 customer and Poly.

REMOTE MONITORING AND MANAGEMENT FOR ON-PREMISES (RMM) VIDEO ENDPOINTS

For this service, the endpoints are owned by the customer and are physically located in the customer's space. Poly will only retain ownership of the products provided in support of the managed services. These endpoints are subject to the monitoring statements below.

REMOTE MANAGEMENT FOR ON-PREMISES AUDIO ENDPOINTS

For this service, the endpoints are owned by the customer and are physically located in the customer's space. Poly will only retain ownership of the products provided in support of the managed services.

SECURITY AT POLY

Security is a critical consideration in the deployment of any network-connected device, even more so for managed services.

Poly Remote Managed Services utilize the ITIL framework.

Poly's Information Security Management System (ISMS) aligns with ISO/IEC 27001:2013. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and a tangible measure by which existing and potential customers 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 for the implementation of specific security technologies—such as cryptographic controls related

to ciphers, protocols, storage, and web—are intended to provide our developers with industry approved methods for adhering to the Poly Product Security Standards.

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 while also enabling the data controller to create and improve security features.

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 to make sure that data controllers and processors can fulfill their data protection obligations.

SECURE DEPLOYMENT

Customer is responsible to procure and secure the public internet access and public IP addresses for the 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 the following 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 managed services network. Externally, all traffic to and from the customer will traverse the IPsec VPN. Internally, monitoring information is sent to the monitoring database, within the managed services environment, to generate alerts and dashboards for the Customer Management Center (CMC), technical support team.

Management is performed on a jump server. This serves as a bastion host for authorized users. No internet accessible Poly systems directly access customer systems, except for operating system updates through a proxy. Management traffic (e.g., HTTPS, SSH, Telnet, Ping, etc.) is generated from the customer specific DMZ to systems covered under the Remote Management and Monitoring Service. Support information (e.g., system logs, CDRs, network traces, etc.) is temporarily stored on the jump server. Support information is to be removed from the DMZ immediately upon being moved to support systems.

Poly uses its own change management policies and procedures, aligned with ITIL, to document and review changes for viability and necessity.

REMOTE MONITORING AND MANAGEMENT FOR ON-PREMISES (RMM) VIDEO ENDPOINTS

The customer is responsible for securely configuring the endpoint 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 through change management.

REMOTE MANAGEMENT FOR ON-PREMISES AUDIO ENDPOINTS

This service requires a RealPresence Resource Manager for provisioning. The customer is responsible for securely configuring the endpoint and 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 through change management.

USER 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 jump server using unique AD credentials. The managed services network has a separate active directory server for providing unique credentials and logging user activity on the jump 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.

Managed 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.

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 or redundant IPsec VPN connectivity to one or multiple sites. Each core DC has multiple routes to the internet. The monitoring solution leverages a distributed application to request and receive SNMP information. The monitoring application's core databases and app servers are virtualized on separate hardware. Management 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 or service level agreements designed around their specific solution design and documented in the service agreement.

CRYPTOGRAPHIC SECURITY

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

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)

DATA PROCESSING

Monitoring data continuously flows between sensor and internal database. This does not contain personally identifiable information.

System logs and call detail records are collected through the IPsec VPN for troubleshooting and reporting for the service. These may contain names, emails, IP addresses, locations.

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

If you are an individual user and the purchase of a Poly managed service has been made by your employer as the customer, all the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as controller of such personal data.

Personal Data Category	Type of Personal Data	Purpose of Processing
Support and reporting services	- Endpoint display name - User email address - User ID - User phone number - User address/location	- Troubleshooting and support remediation - Provide required reporting for managed services

PURPOSE OF PROCESSING

The primary purposes of processing information by the managed service are to provide support and reporting per agreement requirements and to provide recovery of system failure.

HOW CUSTOMER DATA IS STORED AND PROTECTED

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.

When Poly Managed Services needs to store customer or personal data to provide basic services, the data is processed as follows:

CATEGORY	WHERE IT STORED AND HOW PROTECTED	HOW LONG
Reporting data	Encrypted server in Poly IT environment	12 months or the conclusion of the engagement
Technical support	Stored in customer DMZ, stored in Poly CRMs, stored on sftp	Temporarily held until 90 days after ticket is closed

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 management servers created for the use of managed services follow hardened templates for deployment. Firewall ports are opened only as necessary and changes are documented through change management.

Backend and management servers that are the foundation for the Managed 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 bidirectional tunnel.

THIRD-PARTY PROVIDERS (SUB-PROCESSORS)

Poly shares customer information with service providers, contractors, or other third parties to assist in providing and improving the service. All sharing of information is consistent with the Poly Privacy Policy.

DATA DELETION AND RETENTION

Poly may retain customer data for as long as needed to provide that customer with the RMM managed service. When a customer makes a request for deletion, 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.

SECURITY INCIDENT RESPONSE

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may 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. https://support.polycom.com/content/support/security-center.html

ADDITIONAL RESOURCES

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

SECURITY INCIDENT RESPONSE

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may 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. https://support.polycom.com/content/support/security-center.html

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.