Poly Private Hosted Infrastructure Services Overview

Introduction

This white paper addresses security and privacy related information regarding the Poly Private Hosted Infrastructure Services, which are hosted by HP | Poly. This white paper describes the security features and access controls applied to HP | Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of these Managed Services, and the location and transfers of personal and other customer data. HP | Poly will use such data in a manner consistent with the HP Privacy Statement and this white paper (which may be updated from time to time). This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper is available on HP | Poly's website.

The following managed services are discussed in this white paper:

Managed Services: Poly Private Hosted Solutions
- Private Hosted for Business (PHfB)
- Private Hosted for Enterprise (PHfE)

Overview of Managed Services

There are two (2) options for these types of solutions: Private Hosted for Business and Private Hosted for Enterprise. The options are chosen based on size, location, and features required. These solutions all include RealPresence Platform (RPP) hardware, service, and maintenance as part of the service. HP | Poly retains ownership of all provided service components and data center engagements. If edge traversal functionality is included in the solution, endpoint access is provided over the internet. Network sizing is determined by concurrent users, call rate, signaling, and overhead. Customer can provide up to 4U and 350W of equipment in HP | Poly DC space for network termination. Customer handoff to Poly Service is via a HP | Poly provided switch and/or firewall.

HP | Poly will provide a secured managed services environment consisting of the appropriate systems to provide the supporting services for the DMZs, user authentication, and secure customer connections. The monitoring and management DMZ systems consist of a bespoke jump server, a monitoring probe, and file storage dedicated to the engagement. Each solution is created using multiple logically separate DMZs to host the monitoring and management, call platform, and internet facing systems. IP addressing (RFC 1918/24) is provided by the customer making the solution a virtual extension of the customer's network. The customer must ensure that there are no IP conflicts on their network.

For connectivity from internal corporate network, an MPLS or private line is required.

Private Hosted for Business (PHfB)

All servers required to run RPP applications are supplied, hardened, and accessed by HP | Poly only. HP | Poly will procure the public internet access for the service to use. This solution is currently only located in one (1) data center in Aurora Colorado, USA. HP | Poly will provide the network equipment required to integrate the solution within the data center.

Private Hosted for Enterprise (PHfE)

All servers required to run RPP applications are supplied and configured by HP | Poly. HP | Poly will procure the public internet access for the service to use. HP | Poly does not provide any back-bone network connections between regionally diverse implementations. The customer is required to provide the IP address space for the solution. It is therefore best that the routing between data centers be provided over the customers' network. HP | Poly will provide the network equipment required to integrate the solution within the DC space. Customer/service provider is required to bring their private network connection or MPLS to the HP | Poly DC space. If using a shared facility, then the customer can supply

a cross connect to the HP | Poly space. Customer network handoff to Poly Service is via a HP | Poly switch and firewall. The public internet access provided by HP | Poly is used for the following purposes:

- Poly Remote Monitoring and Management
- External users using H323/SIP endpoints to dial into solution
- Any optional integrations that are configured

Security at HP | Poly
Security is always a critical consideration for all HP | Poly products and services. HP | 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 HP | Poly has established and implemented best-practice information security processes.

Product security at HP | Poly is managed through the HP Cybersecurity team which oversees secure software development standards and guidelines.

The HP | 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 HP | Poly Product Security Standards.

Privacy by Design
HP | 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, HP | Poly considers the right to data protection with due regard.

Security by Design
HP | 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 HP | Poly uses – both on-premises and in the cloud as well as to the development, delivery, and support of HP | Poly products, cloud services and managed services.

The foundational principles which serve as the basis of HP | 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.

Change Management

Poly Private Hosted Infrastructure Services utilize the Information Technology Infrastructure Library (ITIL) framework. HP | 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 HP | 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.

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 HP | Poly for technical support are asked to provide contact information.

If someone is an individual user and the purchase of a HP | Poly managed 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

Information that is processed is used for enhancing the user experience, allowing configuration of settings required for proper delivery of services, and easy access to frequently used data.

When configured to use an optional HP | Poly device management solution, the on-premises server or cloud service processes configuration files and their overrides to aid in the management of the devices in a given deployment. The server or cloud service may also process device network information, media statistics, and device asset information to aid in device analytics, which enables device performance validation and visibility into customer quality of experience and service performance.

How Customer Data Is Stored and Protected

Data backups are stored in the customer's encrypted DMZ on the customer's jump server for 61 days.

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

HP | Poly may change the location of the HP | 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 HP | Poly's website.

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

Source of Personal Data	Categories of PI Processed	Business Purpose for Processing	Disclosed to the following Service Providers
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	AWS, Azure
Configuration backups	• Display name • User email address • User ID • Phone number • Organization address/location	Ability to recover from system failure	AWS, Azure

Data Deletion and Retention

All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism. Nothing is transmitted outside of Poly Private Hosted Infrastructure Services. All data is self-contained in the database in the data center.

HP | Poly may retain customer data for as long as needed to provide the customer with any HP | Poly managed services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to HP's Chief Privacy and Data Protection Officer form, HP | Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. HP | Poly may "anonymize" personal data in lieu of deletion. In cases where anonymization occurs, the process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (e.g., name, site information and IP address) with randomly generated alphanumeric characters.

Secure Deployment

The RealPresence Platform (RPP) functionality and hardware are installed within HP | Poly's environment. Ownership and environment responsibility is retained by HP | Poly. HP | Poly 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 DMZs. The DMZs are encapsulated by firewall security zones. No unnecessary network ports are opened between zones. The DMZs have the following specific functionality to support the service:

Monitoring uses a collector in a customer specific 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 the customer will traverse customer provided MPLS or dedicated private line. 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 HP | 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. Configuration backups of managed devices are taken monthly for recovery. Backups and support information (e.g., system logs, CDRs, network traces, etc.) are temporarily stored on the jump server. Backup information on jump servers is encrypted. Support information is to be removed from the DMZ immediately upon being moved to support systems.

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

Server Access and Data Security
HP | Poly is responsible for physical and data security for all systems in their environment up to the customer connection at the edge of the network.

All 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. Only authorized staff members may access the facility with their badges. Access to the equipment for these systems is established via secure and bidirectional tunnel, or in the case of Private Cloud for Business, over direct internal network only.

Cryptographic Security for Managed Services Connections
- Certificates per HP | 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)

Authentication
HP | Poly personnel use certificates on HP | Poly managed assets for their software VPN connection to the HP | Poly Managed Services network. From the HP | Poly laptop, administrators access the specific jump server required 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. HP | Poly Managed Services personnel initially access the customer's managed devices using local administrator credentials provided during onboarding. These credentials are changed when Managed Services goes operational and are required to follow HP | Poly's own strong password configuration policy which complies with industry standard security practices.

Managed device credentials are stored in an encrypted password manager which is assigned, managed, and logged per user.

Customer user access is provided requiring unique identifiers and passwords which must be changed per HP | Poly policy. The Business Relationship Manager (BRM) can facilitate requests and will follow

up on password changes. All customer user traffic will stay within the customer's network. Customer will not be allowed administrative access to the managed solution.

Disaster Recovery and Business Continuity

Poly Private Hosted Infrastructure Services are architected to provide high reliability, resiliency, and security.

HP | Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. HP | Poly tests disaster recovery processes and procedures on an annual basis. We use the results of this testing process to evaluate our preparedness for disasters and to validate the completeness and accuracy of our policies and procedures.

Security Incident Response

The HP Cybersecurity team promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact them directly at informationsecurity@hp.com.

The HP Cybersecurity team works proactively with customers, independent security researchers, consultants, industry organizations and other suppliers to identify possible security issues with HP | Poly products and networks. HP | Poly security advisories and bulletins can be found on the HP Customer Support website.

Subprocessors

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

applicable data protection laws.

The subprocessor list here identifies HP | Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact HP's Chief Privacy and Data Protection Officer form.

Prior to engagement, suppliers that may process data on behalf of HP | 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 HP | 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 HP | Poly product. You may copy and use this paper for your internal reference purposes only. HP | 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 HP | POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.