WHITEPAPER

Complying with the Hong Kong Personal Data (Privacy) Ordinance

How BeyondTrust PAM Solutions can help organisations meet "Principle 4 - Security of Personal Data"

BeyondTrust

Contents

Introduction

The Hong Kong Personal Data (Privacy) Ordinance has been in effect since 1996, but critical changes made in 2012 and 2018 drove a stronger focus to the regulation that affected, not only organisations in Hong Kong, but also contractors that supply services to those organisations.

The objective of the Personal Data (Privacy) Ordinance (Cap. 486) is to protect the privacy rights of a person in relation to personal data in Hong Kong. It's comprised of **6 main principles** that govern every aspect of the life cycle of a piece of personal data. Everyone who is responsible for handling data (Data User) should meet these six data protection principles:

- Principle 1— Purpose and Manner of Collection of Personal Data
- Principle 2—Accuracy and Duration of Retention of Personal Data
- Principle 3—Use of Personal Data
- Principle 4—Security of Personal Data
- Principle 5—Information to Be Generally Available
- Principle 6—Access to Personal Data

This white paper will focus on covering the specific elements of Principle 4, concerning the Security of Personal Data, and how a complete privileged access management program can help organisations meet the criteria entailed in this Principle.

The non-compliance with the Data Protection Principles does not constitute a criminal offence directly, however, contravention of an enforcement notice is an offence which could result in a maximum fine from HK$500,000 and imprisonment for up to 3 years, and heavier punishments may be applied to repeat offenders.

Privileged Access Management & Principle 4

"Principle 4" of the Hong Kong Personal Data (Privacy) Ordinance relates to the safeguarding of the personal data. In summary, any organisation that holds personal information from its clients' needs to take practicable steps to safeguard the personal data from unauthorised or accidental access, processing, erasure, loss, or use.

The following table maps out how a complete privileged access management (PAM) program can assist organisations in not only complying with the criteria in Principle 4, but also proving that they have exercised all due diligence to comply with this mandate.

Principle 4—Security of Personal Data

SUBSECTION 1

"All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to:"

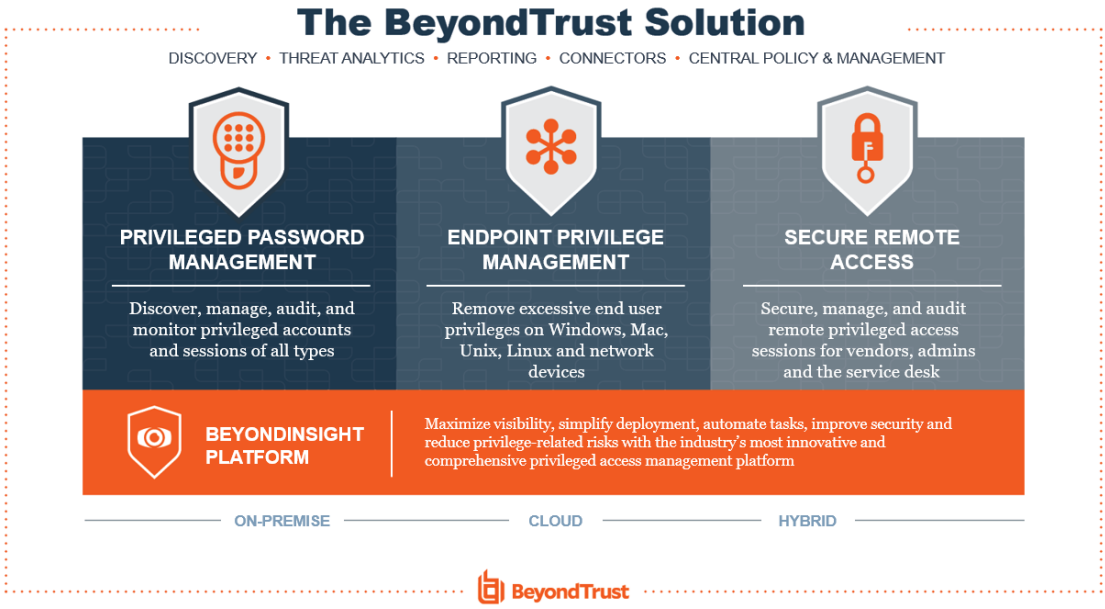
Criteria	How BeyondTrust can help
(a)the kind of data and the harm that could result if any of those things should occur;	BeyondTrust's Privileged Access Management solutions allow for the identification and tagging of sensitive data for classification and control access. While we no longer offer a vulnerability assessment engine, we recommend working with our strategic partner, Tenable. With their vulnerability management services, you can find sensitive information and classify it for the rest of our solutions.
(b)the physical location where the data is stored;	Not Applicable
(c)any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;	While we cannot detect security vulnerabilities, our Privileged Access Management solutions can secure key accounts that are used to access sensitive data to prevent privileged attack vectors at source.
(d)any measures taken for ensuring the integrity, prudence and competence of persons having access to the data;	BeyondTrust's Privileged Access Management solutions contain features like just-in-time access, challenge-response, two factor authentication, and workflow management to ensure integrity, prudence, and competence of individuals accessing data.
(e)any measures taken for ensuring the secure transmission of the data.	BeyondTrust's Privileged Access Management solution can monitor unsecure commands used for data transmission that may be in violation of the organisation's data privacy policies. In addition, our Secure Remote Access technology can be used to secure the transmission of data throughout almost any environment.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

BeyondTrust Solutions Overview

The BeyondTrust Privileged Access Management Platform includes the following individual best-of-breed products that are fully integrated into the platform itself.

Privileged Password Management	Discover, Manage, Audit, and Monitor Accounts with Privileged Password Management solutions. Password Safe lets you reduce the risk of privileged credential misuse through automated password and session management. Cloud Vault offers essential vaulting capabilities in the cloud. And DevOps Secrets Safe lets you secure and manage secrets used in DevOps environments.
Endpoint Privilege Management	BeyondTrust Endpoint Privilege Management enforces least privilege and eliminates admin rights across Windows, Unix, Linux, Mac, network, IoT, ICS, and SCADA devices. Organisations can remove admin rights from desktop users, and also tightly manage privileged access on servers (including eliminating root access), while empowering both IT and non-IT workers to securely do their jobs. The solution monitors and logs all privileged sessions in real-time, providing a thorough compliance trail. Endpoint Privilege Management can also centralise authentication for Unix, Linux, Mac, and Windows by extending AD's Kerberos authentication and single sign-on capabilities across platforms.
Secure Remote Access	With Remote Support, you can empower the service desk to support Windows, Mac, Linux, iOS, Android, network devices, and peripherals with one, secure tool. Privileged Remote Access allows you to secure, manage, and audit vendor and internal remote privileged access without a VPN.
Platform Capabilities	The BeyondTrust Privileged Access Management Platform is an integrated, extensible solution that provides visibility and control over all privileged accounts and users. By uniting the broadest set of privileged security capabilities, the platform simplifies deployments, reduces costs, improves usability, and reduces privilege risks. Common components centralised for all products in BeyondInsight include asset and account discovery, threat analytics, reporting and connectors to third-party systems, and central management and policy.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.